

VMware vSphere 4: Install, Configure, Manage

Student Manual – Volume 1
VMware ESX 4.0 and vCenter 4.0



VMware® Education Services
VMware, Inc.
education@vmware.com

VMware vSphere 4:
Install, Configure, Manage
VMware ESX 4.0 and vCenter 4.0
Part Number EDU-ENG-A-ICM4-LEC1-STU
Student Manual – Volume 1
Revision A

Copyright/Trademark

Copyright © 2009 VMware, Inc. All rights reserved. This manual and its accompanying materials are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The training material is provided “as is,” and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This training material is designed to support an instructor-led training course and is intended to be used for reference purposes in conjunction with the instructor-led training course. The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended.

These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted or modified without the express written approval of VMware, Inc.

TABLE OF CONTENTS

MODULE 1	Course Introduction	1
	Importance	2
	Objectives	3
	Goals of This Course	4
	What Is VMware vSphere?	5
	Objectives for the Learner	6
	Course Outline	7
	VCP on vSphere 4 Certification	8
	vSphere Curriculum	9
	VMware Online Resources	10
	Course Map	11
	Key Points	12
 MODULE 2	 Introduction to VMware Virtualization	 13
	You Are Here	14
	Importance	15
	Lesson Objectives	16
	What Is Virtualization?	17
	How Does Virtualization Work?	18
	Host Operating System-Based Virtualization	19
	Virtualization Using a Bare-Metal Hypervisor	20
	What Is a Virtual Machine?	21
	Why Use Virtual Machines?	22
	vSphere Components	23
	Using vSphere in a Datacenter	24
	Using VMware View with vSphere	25
	Using VMware Lab Manager with vSphere	26
	Key Points	27
 MODULE 3	 Configuring ESX/ESXi	 29
	You Are Here	30
	Importance	31
	Module Lessons	32
	Lesson 1: Overview of ESX/ESXi	33
	Lesson Objectives	34
	ESX/ESXi: Virtualization Platform	35
	ESX/ESXi Features	36
	ESX, ESXi Installable, and ESXi Embedded	37
	ESXi Architecture	38
	ESX Architecture	39
	Lesson Summary	40
	Lesson 2: Configuring ESX/ESXi	41
	Lesson Objectives	42

Installing ESX/ESXi	43
Configuring ESXi	44
Configuring ESXi: root Access	45
Configuring ESXi: Management Network	46
Configuring ESXi: Other Settings	47
Using the vSphere Client	48
Logging In to ESX/ESXi	49
vSphere Client: Configuration Tab	50
Viewing Processor and Memory Configuration	51
ESX/ESXi Licensing	52
License Assignment Procedure	53
Synchronizing Host Time Using NTP	54
ESX/ESXi as an NTP Client	55
Configuring ESX/ESXi as an NTP Client	56
Network Settings: DNS and Routing	57
ESX Service Console Firewall	58
ESX/ESXi User Account Best Practices	59
Viewing ESX/ESXi System Logs	60
Lab 1 and eLearning Activity	61
Lesson Summary	62
Key Points	63

MODULE 4

VMware vCenter Server	65
You Are Here	66
Importance	67
Module Lessons	68
Lesson 1: Installing vCenter Server	69
Lesson Objectives	70
vCenter Server: Management Platform	71
vCenter Architecture	72
vCenter Server Components	74
vCenter Server Modules	75
vCenter Server: Physical or Virtual Machine	76
vCenter Server Hardware/Software Requirements	77
vCenter Database Requirements	78
Calculating the Database Size	79
Steps Before Installing vCenter Server	80
vCenter Server Installation Procedure	81
vCenter Server Installation Information	82
Configuring Access to the Database	83
vCenter Server Account Considerations	84
Standalone Instance or Linked Mode Group	85
Ports Used by vCenter Server	86

Configuring Ports Used by vCenter Server	87
vCenter Server Services	88
vSphere Client Installation Procedure	89
Logging In to the vSphere Client	90
Installing vCenter Additional Modules and Plug-Ins	91
Lab 2	92
Lesson Summary	93
Lesson 2: Using vCenter Server	94
Lesson Objectives	95
vSphere Client Home Page	96
Navigating the vSphere Client	97
vCenter Inventory Objects	98
Organizing Inventory Objects into Folders	99
Managing Multiple Datacenters	100
vCenter Views: Hosts, Clusters, VMs, Templates	101
vCenter Views: Datastores and Networks	102
Adding Host to vCenter Server Inventory	103
ESX/ESXi and vCenter Communication	104
vCenter License Overview	105
Adding License Keys	106
vCenter Server Events	107
vCenter Server System Logs	108
Creating a vCenter Server Administrator	109
Lab 3	110
Lesson Summary	111
Key Points	112

MODULE 5

Networking	113
You Are Here	114
Importance	115
Module Lessons	116
Lesson 1: vNetwork Standard Switches	117
Lesson Objectives	118
What Is vNetwork?	119
vNetwork Standard Switch	120
vNetwork Standard Switch Components	121
vSwitch Ports	122
vSwitch Examples	123
Adding a Network: Connection Type	124
Adding a Network: Network Adapters	125
Adding a Network: Connection Settings	126
vSwitch Configuration	127
Physical Network Considerations	128

Lesson Summary	129
Lesson 2: vNetwork Distributed Switches	130
Lesson Objectives	131
vNetwork Distributed Switch	132
Benefits of Distributed Switches	133
vNetwork Distributed Switch Architecture	134
Distributed Switch Example	136
Creating a Distributed Switch	137
Viewing Distributed Switches	138
Connecting a Virtual Machine to a Port Group	139
Adding a Host to a Distributed Switch	140
VMkernel and Service Console Connections	141
Managing Physical Adapters (Uplinks)	142
Third-Party Distributed Switches	143
Lab 4	144
Lesson Summary	145
Lesson 3: Modifying Virtual Switch Properties	146
Lesson Objectives	147
Editing General Switch Properties	148
Editing Advanced Switch Properties	149
Editing Distributed Port Group Settings	151
Editing Port Group Policies	152
Security Policy	153
Traffic-Shaping Policy	155
Configuring Traffic Shaping	156
VLANs	157
VLAN Policy	158
Private VLAN Architecture	159
Configuring and Assigning PVLANS	161
Advanced Settings	162
Lab 5	163
Lesson Summary	164
Key Points	165

MODULE 6

Storage	167
You Are Here	168
Importance	169
Module Lessons	170
Lesson 1: Storage Concepts	171
Lesson Objectives	172
Storage Overview	173
Storage Technology Overview	174
Datastores	175

VMFS	176
NFS	178
Raw Device Mapping (RDM)	179
Local versus Shared Storage	180
Storage Device Naming Conventions	181
Physical Storage Considerations	182
Lesson Summary	183
Lesson 2: Fibre Channel SAN Storage	184
Lesson Objectives	185
Using Fibre Channel with ESX/ESXi	186
Fibre Channel SAN Components	187
Fibre Channel Addressing and Access Control	189
Accessing Fibre Channel Storage	190
Viewing Fibre Channel Storage Information	191
Viewing Fibre Channel Storage Maps	192
Lesson Summary	193
Lesson 3: iSCSI Storage	194
Lesson Objectives	195
Using iSCSI with ESX/ESXi	196
iSCSI Components	197
iSCSI Addressing	198
iSCSI Initiators	199
Steps to Configure Software iSCSI	200
Configuring Network for Software iSCSI	201
Enabling the iSCSI Software Adapter	202
iSCSI Target-Discovery Methods	203
Configuring iSCSI Target Addresses	204
iSCSI Security: CHAP	205
Configuring iSCSI Security: CHAP	206
Steps to Configure Hardware iSCSI	207
Viewing iSCSI Information	208
Lab 6	209
Lesson Summary	210
Lesson 4: VMFS Datastores	211
Lesson Objectives	212
Using a VMFS with ESX/ESXi	213
Creating a VMFS	214
Viewing VMFS Datastores	215
Browsing Datastore Contents	216
Growing a VMFS	217
Volume Grow versus Extent Grow	218
Before Growing a VMFS	220
Using Volume Grow: Increase Capacity	221

Using Volume Grow: View Disk Layout	222
Using Volume Grow: Specify Capacity	223
Using Extent Grow: Select LUN	224
Deleting a VMFS	225
Lab 7	226
Lesson Summary	227
Lesson 5: NAS/NFS Datastores	228
Lesson Objectives	229
Using NAS/NFS with ESX/ESXi	230
NFS Components	231
Addressing and Access Control with NFS	232
Configuring Networking for NFS Access	233
Creating an NFS Datastore	234
Viewing NFS Datastore: Storage Tab	235
Viewing NFS Datastore: Storage Views Tab	236
Unmounting an NFS Datastore	237
Lab 8	238
Lesson Summary	239
Key Points	240

MODULE 7

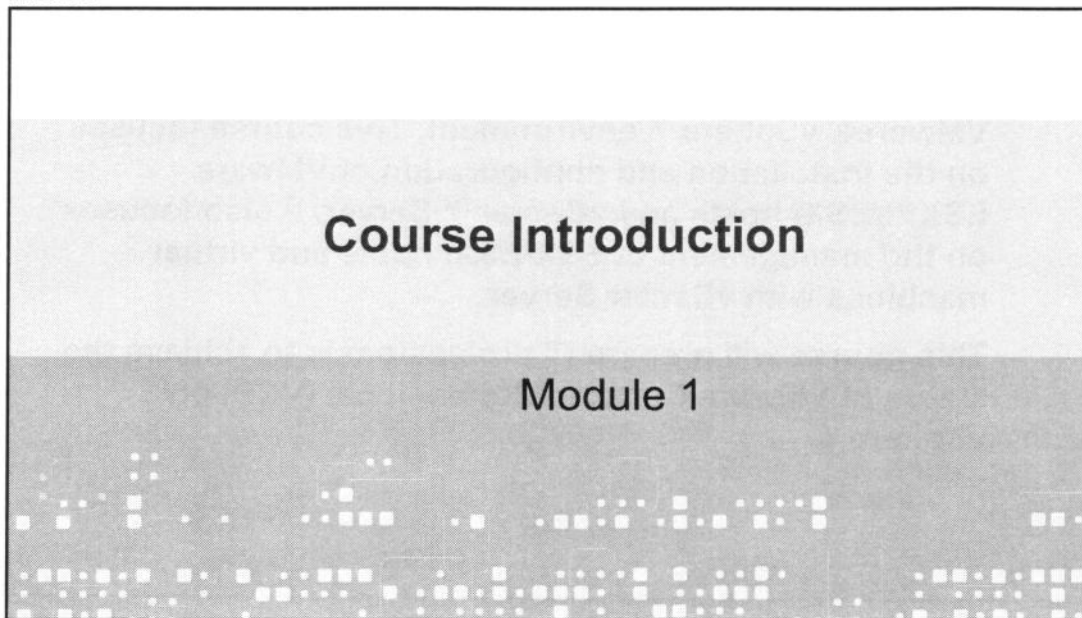
Virtual Machines	241
You Are Here	242
Importance	243
Module Lessons	244
Lesson 1: Virtual Machine Concepts	245
Lesson Objectives	246
What Is a Virtual Machine?	247
What Files Make Up a Virtual Machine?	248
Displaying a Virtual Machine's Files	250
Displaying Files Using the Storage Views Tab	251
Virtual Machine Hardware	252
CPU and Memory	253
Virtual Disk	254
Virtual NIC	255
Other Devices	257
Virtual Machine Console	258
VMware Tools	259
Provisioning a Virtual Machine	260
VMware Products for Provisioning Virtual Machines	261
Lesson Summary	262
Lesson 2: Creating a Virtual Machine	263
Lesson Objectives	264
Creating a Virtual Machine: Launch Wizard	265

Choosing the Typical Configuration	266
Choosing the Custom Configuration	267
Installing the Guest Operating System	268
Installing VMware Tools	269
Virtual Appliances	270
Deploy OVF Template	271
Lab 9	272
Lesson Summary	273
Lesson 3: Creating Templates and Clones	274
Lesson Objectives	275
What Is a Template?	276
Creating a Template	277
Viewing Templates	278
Updating a Template	279
Deploying a Virtual Machine from Template	280
Cloning a Virtual Machine	281
Customizing the Guest Operating System	282
Deploying Virtual Machines Across Datacenters	283
Lab 10	284
Lesson Summary	285
Lesson 4: VMware vCenter Converter	286
Lesson Objectives	287
vCenter Converter Capabilities	288
vCenter Converter Components	289
vCenter Converter Requirements	290
Importing a Physical System	291
Remote Hot Cloning of a Physical Machine	292
Local Cold Cloning of a Physical Machine	293
Importing a Physical System	294
Cloning Modes: Disk-Based and Volume-Based	295
Changes to Virtual Hardware	297
Lab 11 and eLearning Activity	298
Lesson Summary	299
Lesson 5: vCenter Guided Consolidation	300
Lesson Objectives	301
Guided Consolidation	302
Guided Consolidation Architecture	303
Guided Consolidation Prerequisites	304
Finding Physical Systems to Consolidate	305
Analyzing Potential Candidates	306
Consolidating Candidates	307
Capacity Planning with vCenter CapacityIQ	308
eLearning Activity	309

Lesson Summary	310
Lesson 6: Modifying Virtual Machines	311
Lesson Objectives	312
Modifying Virtual Machine Settings	313
Hot-Pluggable Devices	314
Increasing Virtual Disk Size: Hot Extend Feature	315
Hot Extend Example	316
Creating a Raw Device Mapping	317
Virtual Machine Options	318
Options: General Options	319
Options: VMware Tools	320
Options: Power Management	322
Advanced: Boot Options	323
Advanced: Paravirtualization	324
Swap File Location	326
Lab 12	327
Lesson Summary	328
Lesson 7: Managing Virtual Machines	329
Lesson Objectives	330
Virtual Machine Snapshots	331
Taking a Snapshot	332
Managing Snapshots	333
Virtual Machine Snapshot Files	334
Managing Virtual Machines Using vApp	335
Removing a Virtual Machine	336
Migrating Virtual Machines	337
Comparison of Migration Types	338
Benefits of Storage VMotion	339
Storage Type Independency	340
Storage VMotion In Action	341
Migrating Using Storage VMotion	343
Storage VMotion Guidelines and Limitations	344
Lab 13	345
Lesson Summary	346
Key Points	347

Course Introduction

Slide 1-1



Importance

Slide 1-2

This course will equip administrators with the knowledge, skills, and abilities to build and run a VMware® vSphere™ environment. This course focuses on the installation and configuration of VMware ESX™/ESXi hosts and vCenter™ Server. It also focuses on the management of ESX/ESXi hosts and virtual machines with vCenter Server.

This course will prepare IT professionals to achieve the status of VMware Certified Professional (VCP) on vSphere 4.

Objectives

Slide 1-3

- Understand the course goals
- Understand the course objectives
- Get familiar with the course outline

Goals of This Course

Slide 1-4

- > To prepare you to install, manage, and configure your vSphere environment
- > To prepare you to achieve the status of VMware Certified Professional (VCP) on vSphere 4

This course teaches you how to administer VMware ESX™/ESXi hosts and the virtual machines that run on them. It also teaches you how to administer VMware vCenter™ Server and take advantage of its capabilities to manage ESX/ESXi hosts and their virtual machines.

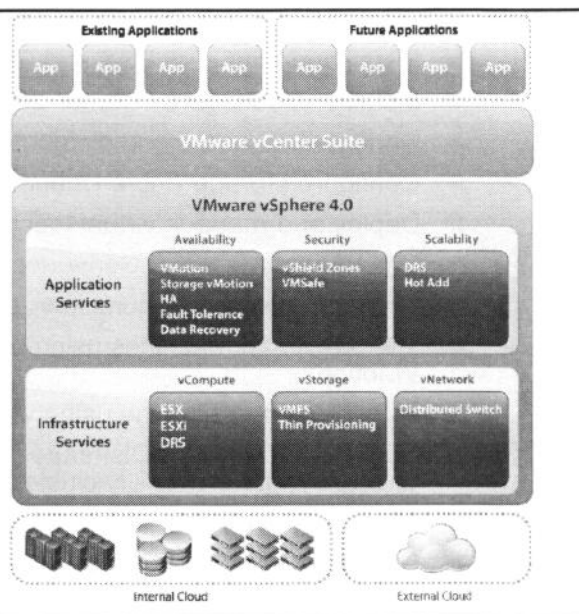
This course is required to achieve the status of VMware Certified Professional (VCP) on vSphere.

What Is VMware vSphere?

Slide 1-5

An infrastructure virtualization suite that:

- > Provides virtualization, management, resource optimization, application availability, and operational automation capabilities
- > Aggregates physical hardware resources and provides virtual resources to the datacenter



VMware® vSphere™ is an infrastructure virtualization suite that provides virtualization, management, resource optimization, application availability, and operational automation capabilities in an integrated package.

vSphere virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the datacenter.

In addition, vSphere provides a set of distributed services that enable detailed, policy-driven resource allocation, high availability, and consolidated backup of the entire virtual datacenter.

Objectives for the Learner

Slide 1-6

- > Install and configure ESX and ESXi
- > Install and configure vCenter Server
- > Configure standard and distributed networking
- > Configure storage (Fibre Channel, iSCSI, NAS/NFS, VMFS)
- > Deploy and manage virtual machines using templates
- > Use VMware vCenter Converter and Guided Consolidation
- > Manage user permissions in vCenter Server
- > Migrate virtual machines using VMware VMotion™ and Storage VMotion
- > Monitor resource usage using vCenter Server
- > Configure a VMware Distributed Resource Scheduler (DRS) and VMware High Availability cluster
- > Back up and recover a virtual machine using VMware Data Recovery
- > Configure VMware vCenter Update Manager

This course discusses and demonstrates the following:

- Guidelines for installing and configuring ESX/ESXi and vCenter Server
- Tasks that can be performed to create, manage, and migrate virtual machines
- Ways to monitor virtual machine and ESX/ESXi activity
- Components that make up the vSphere environment, such as VMware Distributed Resource Scheduler (DRS), VMware High Availability, vCenter Converter, Guided Consolidation, vCenter Update Manager, VMware Data Recovery, and VMware Consolidated Backup.

Course Outline

Slide 1-7

- Module 1: Course Introduction**
- Module 2: Introduction to VMware Virtualization**
- Module 3: Configuring VMware ESX and ESXi**
- Module 4: Installing and Using VMware vCenter Server**
- Module 5: Networking**
- Module 6: Storage**
- Module 7: Virtual Machines**
- Module 8: Access Control**
- Module 9: Resource Monitoring**
- Module 10: Scalability**
- Module 11: High Availability and Data Protection**
- Module 12: Configuration Management**
- Module 13: Installing VMware ESX and ESXi**

These are the modules presented in the course, They are usually presented in this sequence. The daily schedule of topics will be covered by your instructor.

VCP on vSphere 4 Certification

Slide 1-8

VMware Certified Professional (VCP) program

- For technical individuals who want to demonstrate their vSphere expertise and advance their career

Three steps to becoming a VCP

1. Participate in a VMware-authorized course.
2. Gain hands-on experience with VMware vSphere.
3. Enroll and pass the certification exam.

For more information on how to become a VCP on vSphere 4, or on how to upgrade your existing certification, see

- <http://mylearn.vmware.com/portals/certification>

The VMware Certified Professional (VCP) program is designed for any technical individuals—partners, end users, resellers, and consultants—who want to demonstrate their expertise in virtual infrastructure and increase their potential for career advancement.

Becoming a VCP is a straightforward, three-step process:

1. Participate in a VMware-authorized, instructor-led course to learn best practices and gain hands-on experience. If you are a current VCP, there are no course prerequisites.
2. Gain hands-on experience with VMware vSphere. Individuals who do not have hands-on experience find it very difficult to pass the exam.
3. Enroll and pass the certification exam. To register to take the VCP examination, contact Pearson VUE, a third-party testing center, at <http://www.pearsonvue.com/vmware>.

This course will give you most of the information you need for the exam. But it will not give you *everything*. To best prepare for this exam, use the exam blueprint as a study guide. The blueprint includes the list of topics covered in the exam as well as references for these topics, such as the VMware product documentation and the VMware Web site. Hands-on experience is also a key component to passing the exam. The blueprint is available on the VMware Certification Web page at <http://mylearn1.vmware.com/portals/certification>.

To view the curriculum roadmap for vSphere, go to the VMware Web site:

<http://www.vmware.com/education/vsphere>

To view the vSphere curriculum roadmap, go to <http://www.vmware.com/education/vsphere>.

The VMware vSphere 4: Install, Configure, Manage course provides the foundation for most of the other courses offered by VMware.

VMware Online Resources

Slide 1-10

VMware communities:

<http://communities.vmware.com>

- > Start a discussion.
- > Access the knowledge base.
- > Access documentation, technical papers, and compatibility guides.
- > Access communities.
- > Access user groups.

VMware support:

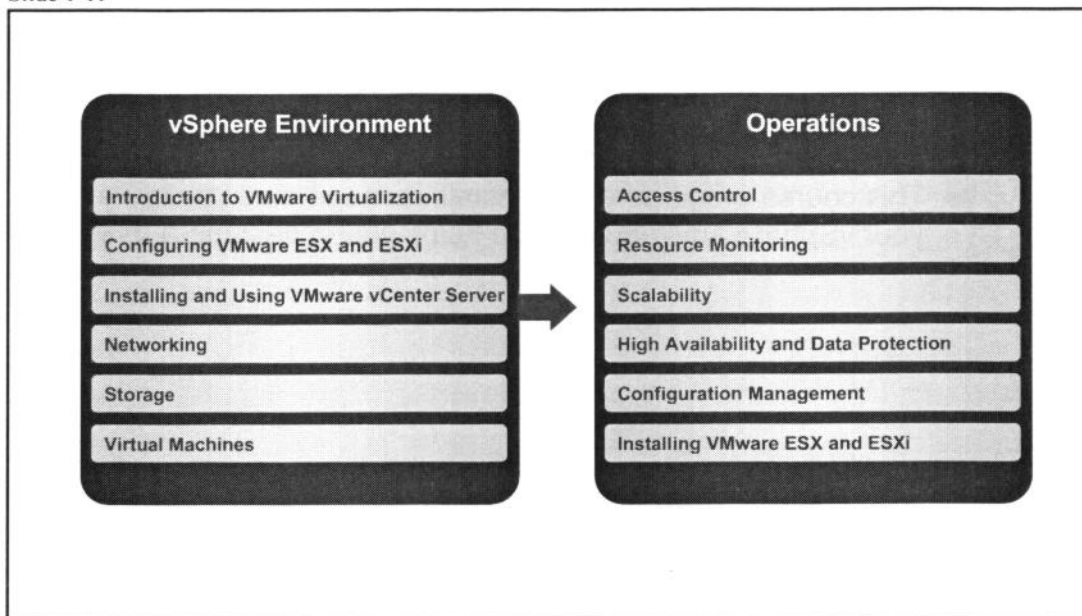
<http://www.vmware.com/support>

Making full use of VMware technical resources will save you time and money. The first place to look for support is VMware's extensive Web-based resources. The VMware Communities Web page provides tools and knowledge to help users maximize their investment in VMware products. VMware Communities provides information about virtualization technology through technical papers, documentation, a knowledge base, discussion forums, user groups, and technical newsletters.

The VMware Support page provides a central point from which you can view support offerings, create a support request, and download products, updates, drivers/tools, and patches.

Course Map

Slide 1-11



This course's modules fall into two categories:

- Modules in the vSphere Environment category discuss system-wide technologies.
- Modules in the Operations category are concerned with features related to day-to-day management of a vSphere environment, with the exception of the ESX/ESXi installation module, which covers a procedure that is typically done just once.
- Each module contains one or more lessons. All lessons have a lecture component, and most of them have a laboratory exercise.

This course map will be used throughout the course to indicate our progress.

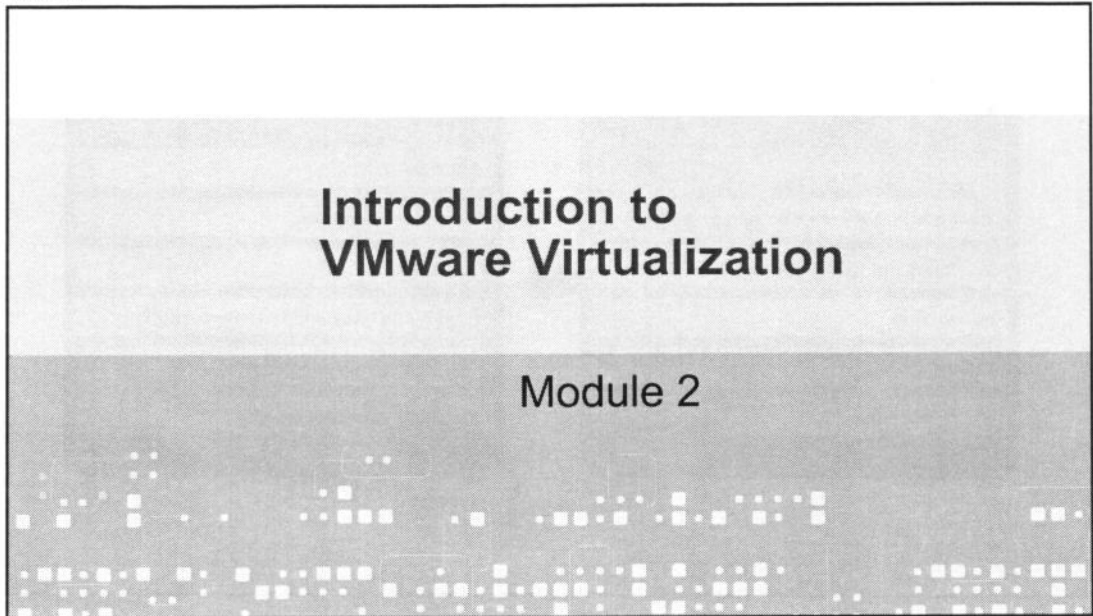
Key Points

Slide 1-12

- This course teaches you about such vSphere components as ESX/ESXi, vCenter Server, VMware HA, DRS, Update Manager, and Data Recovery.
- This course prepares you to install, manage, and configure your vSphere environment and helps you to become a VCP.

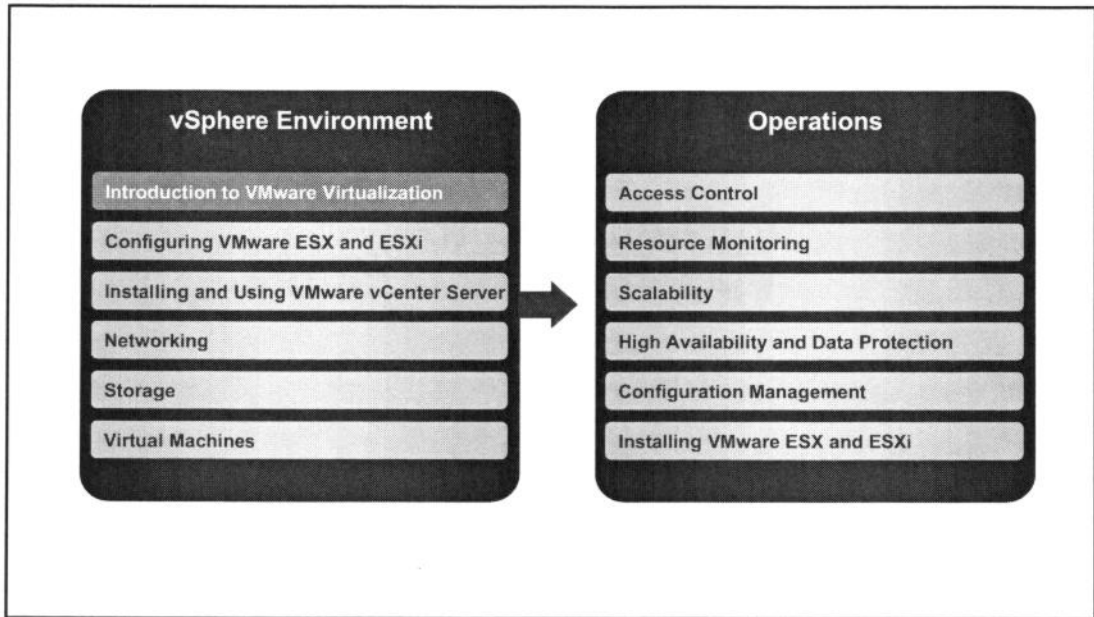
Introduction to VMware Virtualization

Slide 2-1



You Are Here

Slide 2-2



Importance

Slide 2-3

- VMware® vSphere™ is based on many components that, as a vSphere administrator, you should be familiar with. This module describes the basic concept of virtualization, the types of virtualization available from VMware, and the virtual machine. This module then shows you the fundamental components of vSphere and provides some examples of how vSphere can be used in your environment.

Lesson Objectives

Slide 2-4

- > Understand the concept of virtualization
- > Identify the benefits of using a virtual machine
- > Describe vSphere components
- > Describe scenarios for using virtualization

What Is Virtualization?

Slide 2-5

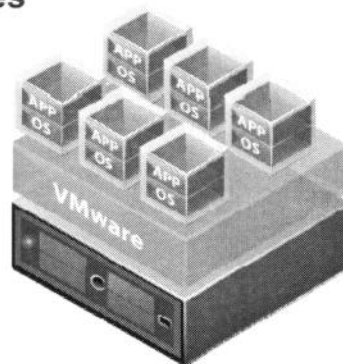
Virtualization is a technology that transforms hardware into software.

Virtualization allows you to run multiple operating systems as virtual machines on a single computer.

- Each copy of an operating system is installed into a *virtual machine*.

Virtualization is *not*:

- Simulation
- Emulation



As desktop and server processing capacity has consistently increased year after year, virtualization has proved to be a powerful technology to simplify software development and testing, to enable server consolidation, and to enhance datacenter agility and business continuity. Fully abstracting the operating system and applications from the hardware and encapsulating them into portable virtual machines has enabled virtual infrastructure features simply not possible with hardware alone. For example, servers can now run in extremely fault-tolerant configurations on virtual infrastructure 24 hours per day, 7 days per week, 365 days per year, with no downtime needed for backups or hardware maintenance.

Virtualization is an architecture that allows you to run multiple operating systems simultaneously on a single computer. Each copy of an operating system is installed on its own virtual machine.

Virtualization is often confused with simulation and emulation. It is neither of these things.

Simulation is something that looks like something else. A flight simulator is a well-known example: it is a machine (or a computer program) that can make it look like you are flying a plane.

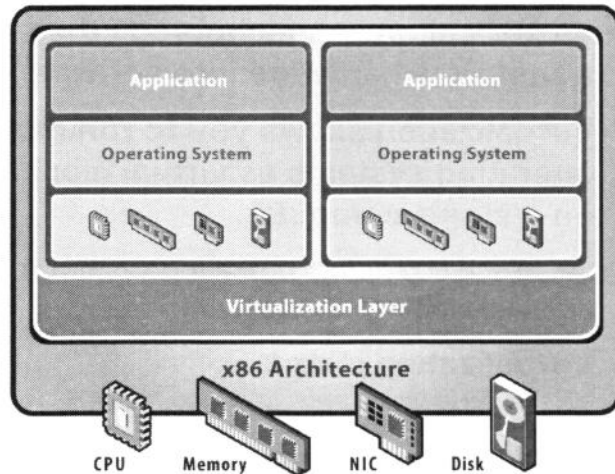
Virtualization is not simulation. The real operating system is installed on the virtualized hardware.

Emulations require software to translate commands for the emulated hardware into commands the physical hardware can understand. This translation process is slow and usually causes software packages running inside an emulator to run slowly. Also, emulation packages can fail to translate correctly some of the machine-language commands. Virtualization is not emulation. No command translations take place when you use VMware virtualization products.

How Does Virtualization Work?

Slide 2-6

A virtualization layer is installed. It uses either a hosted or hypervisor architecture.

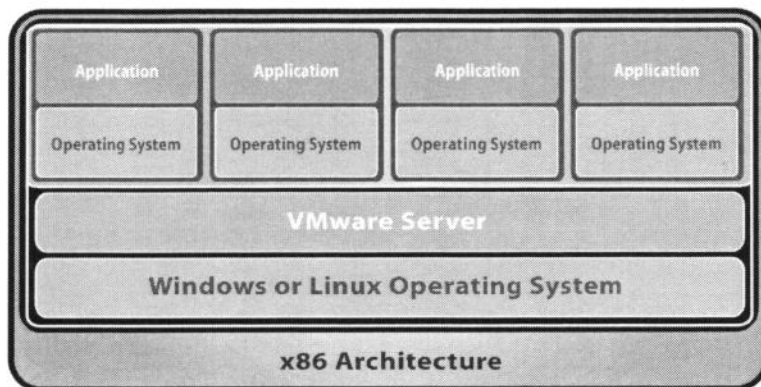


The term virtualization broadly describes the separation of a service request from the underlying physical delivery of that service. With x86 computer virtualization, a virtualization layer is installed between the hardware and the operating system. This virtualization layer allows multiple operating system instances to run concurrently within virtual machines on a single computer, dynamically partitioning and sharing the available physical resources, such as CPU, storage, memory, and I/O devices.

For industry-standard x86 systems, virtualization approaches use either a hosted or a hypervisor architecture.

Host Operating System-Based Virtualization

Slide 2-7



A host-based virtualization system requires an operating system (such as Windows or Linux) to be installed on the computer.

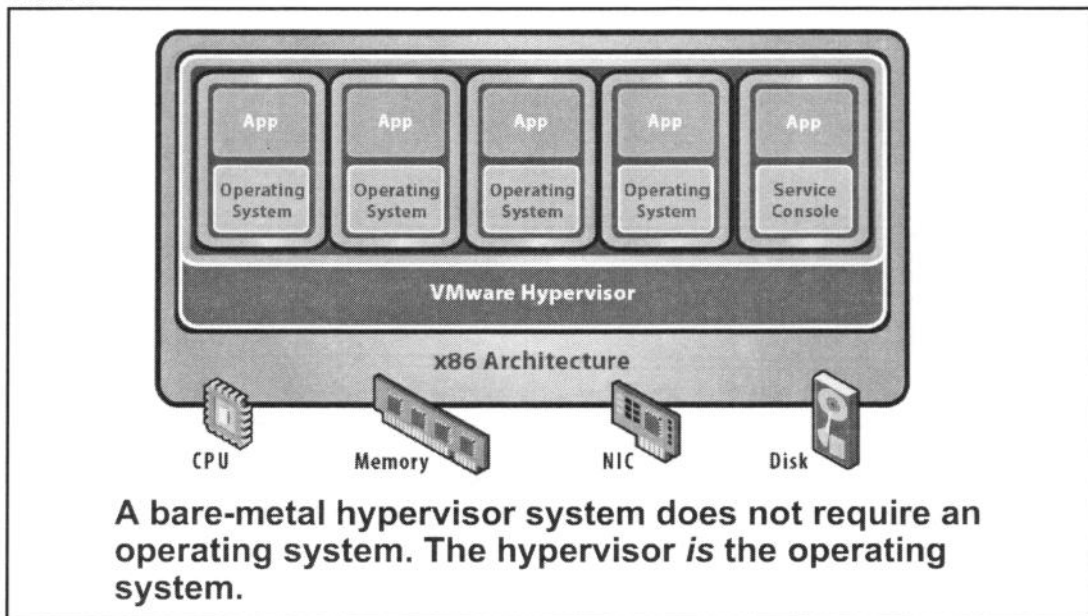
Host operating system-based virtualization—also called host-based virtualization—installs and runs the virtualization layer as an application on top of an operating system and supports the broadest range of hardware configurations.

For example, VMware Server is a free application that can be installed on a supported Windows or Linux system and that provides host-based virtualization. Once VMware Server is installed, virtual machines can be created and employed.

Other VMware applications that employ a hosted architecture are VMware Player, ACE, and Workstation.

Virtualization Using a Bare-Metal Hypervisor

Slide 2-8



In contrast, a hypervisor (or, bare-metal) architecture installs the virtualization layer directly on a clean x86-based system. Because it has direct access to the hardware resources, rather than going through an operating system, a hypervisor is more efficient than a hosted architecture and delivers greater scalability, robustness, and performance.

A hypervisor is the primary component of virtualization that enables basic computer system partitioning (that is, simple partitioning of CPU, memory, and I/O). VMware ESX™/ESXi employs a hypervisor architecture on certified hardware for datacenter-class performance.

For a very good discussion on virtualization, see the white paper “Understanding Full Virtualization, Paravirtualization, and Hardware Assist” at http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf.

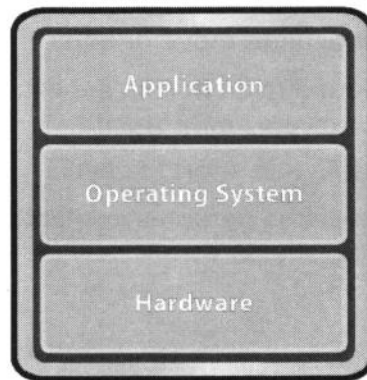
What Is a Virtual Machine?

Slide 2-9

From the user's perspective, it is a software platform that, like a physical computer, runs an operating system and applications.

From the hypervisor's perspective, it is a discrete set of files. These are the main files:

- > Configuration file
- > Virtual disk file
- > NVRAM settings file
- > Log file



Virtual Machine



From the user's perspective, a virtual machine is a software platform that, like a physical computer, runs an operating system and applications. An operating system that has been virtualized is called a *guest operating system*. One supported guest operating system runs in each virtual machine that is created. Each virtual machine is completely independent and can have its own applications and its own security.

From the perspective of the hypervisor, a virtual machine is a discrete set of files, including a configuration file, virtual disk files, a NVRAM settings file, and a log file. Virtual machines are portable. They can easily be backed up and cloned. They are just an encapsulated set of files.

Virtual machines will be discussed in detail in a later module.

Why Use Virtual Machines?

Slide 2-10

Physical Machine	Virtual Machine
Difficult to move or copy	Easy to move and copy
Bound to a specific set of hardware components	<ul style="list-style-type: none">> Encapsulated into files> Independent of physical hardware
Often has short life cycle	Easy to manage
Requires personal contact to upgrade hardware	<ul style="list-style-type: none">> Isolated from other virtual machines running on the same physical hardware> Insulated from physical hardware changes
	

In a physical machine, the operating system (Windows, UNIX, Linux, and so forth) is installed directly on the hardware. This requires specific device drivers to support specific hardware. If the computer is upgraded with new hardware, new device drivers are required. Hardware upgrades also require direct hands-on contact by technical support personnel.

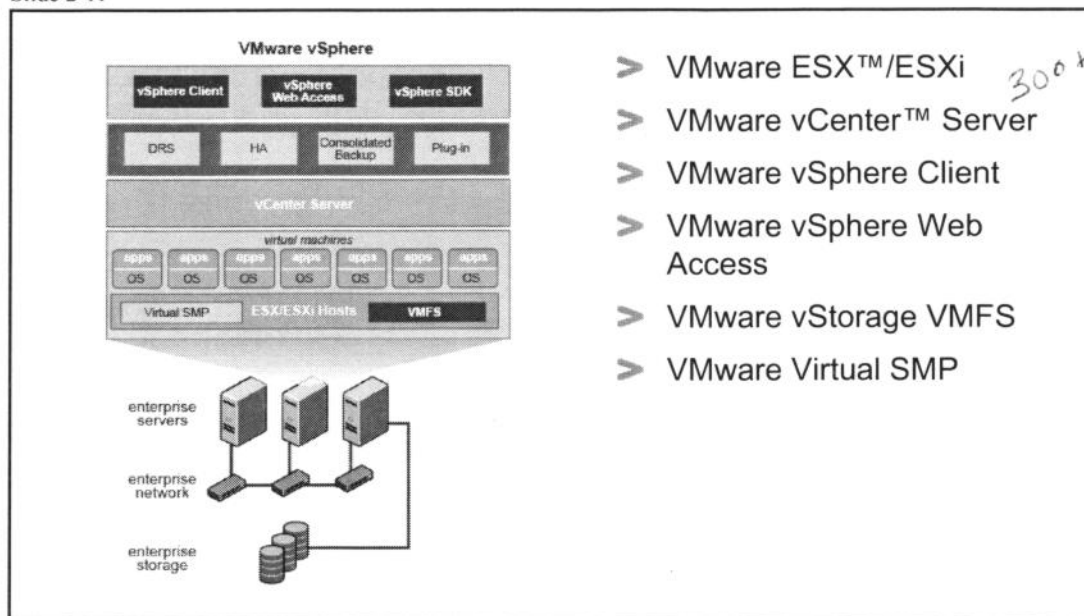
Virtual machines are 100 percent software. The virtual machine is nothing more than a set of files. This includes files known as virtual disks, which replace hard disk storage. All the files for a single virtual machine are located in one directory. Because it uses standardized virtual device drivers, the hardware can be upgraded without any change to the virtual machine.

Multiple virtual machines are isolated from one another. So now you can have your database server and your email server running on the same physical computer. The isolation between the virtual machines means that software-dependency conflicts and performance-tuning conflicts are not a problem.

Because a virtual machine is just a set of files, it is simple to move the entire virtual machine to a new server to perform hardware upgrades. This also makes disaster recovery planning and testing much easier.

vSphere Components

Slide 2-11



- > VMware ESX™/ESXi
- > VMware vCenter™ Server
- > VMware vSphere Client
- > VMware vSphere Web Access
- > VMware vStorage VMFS
- > VMware Virtual SMP

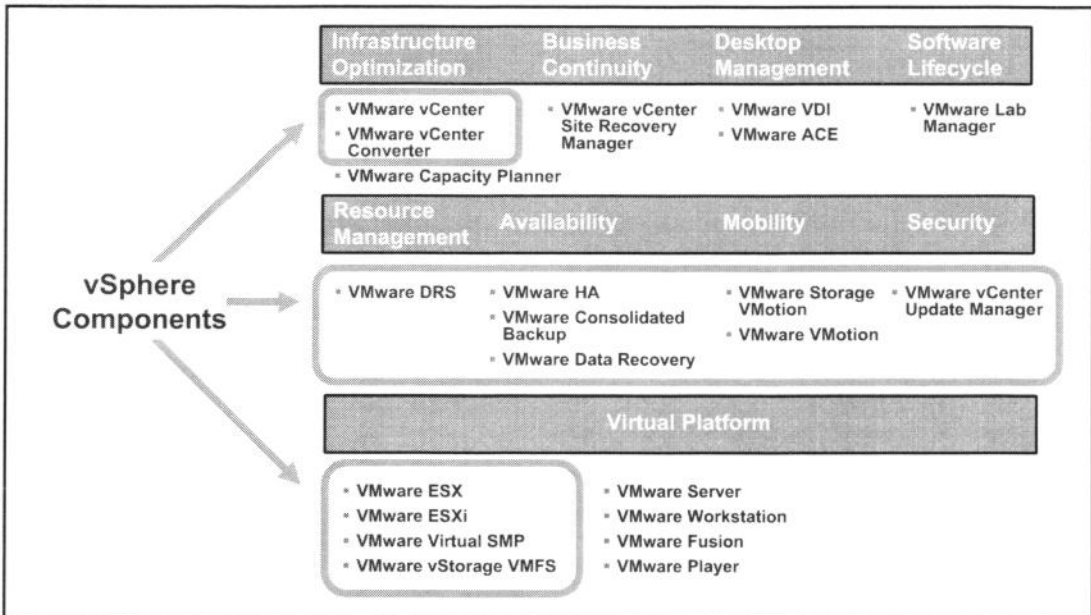
VMware vSphere™ consists of the following components:

- VMware ESX/ESXi – The virtualization platform for vSphere
- VMware vCenter™ Server – The central point for configuring, provisioning, and managing virtualized IT environments
- VMware vSphere Client – An interface that allows users to connect remotely to vCenter Server or ESX/ESXi from any Windows PC.
- VMware vSphere Web Access – A Web interface that allows virtual machine management and access to remote consoles
- VMware vStorage VMFS – A high-performance cluster file system for ESX/ESXi virtual machines
- VMware Virtual SMP – A feature that enables a single virtual machine to use multiple physical processors simultaneously

vSphere also provides functionality for resource management such as VMware Distributed Resource Scheduler (DRS), for availability such as VMware High Availability, and for data protection such as VMware Consolidated Backup and VMware Data Recovery.

Using vSphere in a Datacenter

Slide 2-12



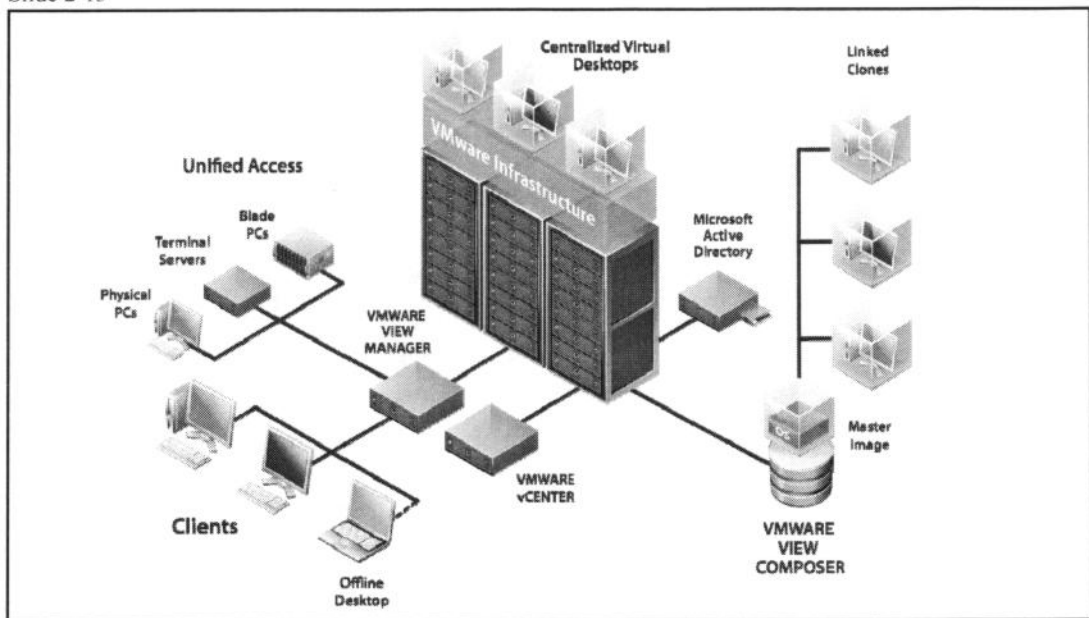
vSphere is most commonly used for creating a responsive datacenter with a virtualized IT infrastructure.

Datacenter administrators use vSphere for the following:

- Solving the problems of server proliferation (lack of space, power, and cooling in server rooms) by replacing single-application servers with virtual machines consolidated onto a much smaller number of physical hosts
- Making better use of server hardware by deploying new servers in virtual machines to avoid adding more underutilized servers to the datacenter
- Provisioning new servers in virtual machines, which takes minutes rather than the days or weeks necessary for provisioning a physical server

Using VMware View with vSphere

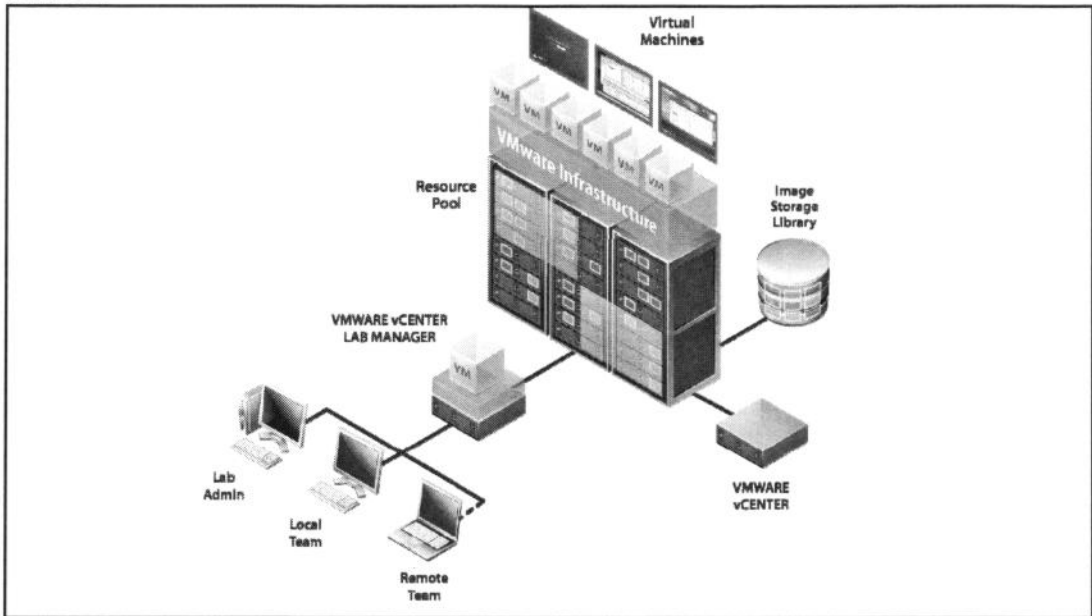
Slide 2-13



vSphere is the foundation for VMware View™. With View, companies can host individual desktops inside virtual machines that are running in their datacenter. Users access these desktops remotely from a PC or a thin client using a remote display protocol. Because applications are managed centrally at the corporate datacenter, organizations gain better control over their desktops. Installations, upgrades, patches, and backups can be done with more confidence and without user intervention.

Using VMware Lab Manager with vSphere

Slide 2-14



vSphere can be used with VMware Lab Manager to support the software life-cycle process.

Lab Manager provides the ability to do the following:

- Allocate resources as needed, instead of maintaining multiple static systems that are used only sporadically. Resources can be pooled and shared between development and test teams for maximum utilization.
- Provision new machines nearly instantly. Software developers and QA engineers can fulfill their own provisioning needs, instead of IT doing it for them.
- Quickly reproduce software defects and resolve them earlier in the software life cycle and ensure higher-quality software and systems.

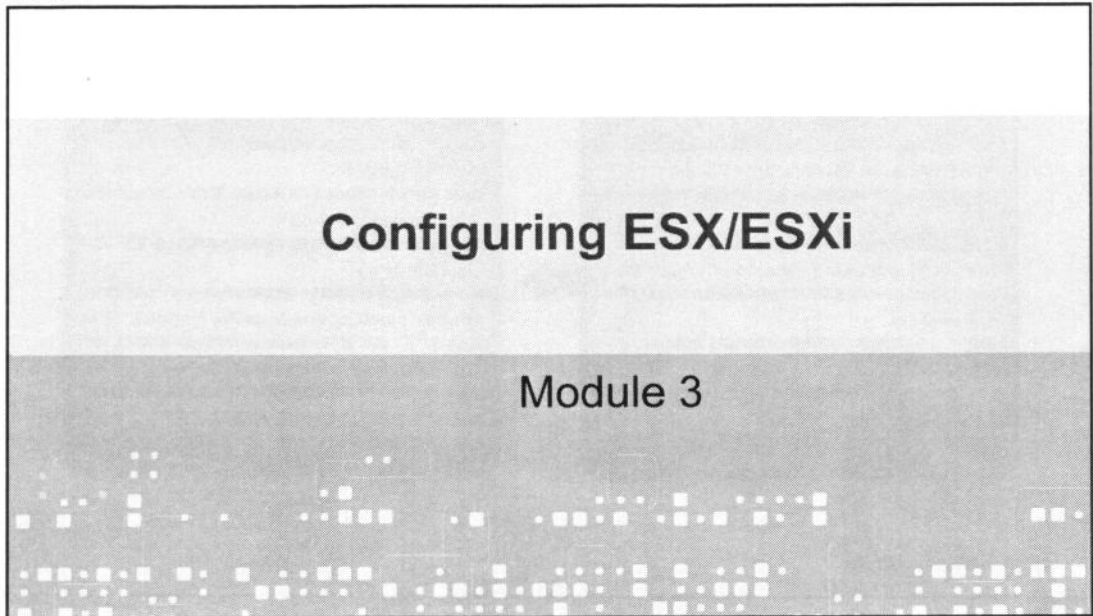
Key Points

Slide 2-15

- ESX/ESXi uses virtualization layers based on the hypervisor architecture.
- Virtual machines are encapsulated into files and independent of physical hardware, making them easy to move and copy between hosts.
- vSphere is commonly used for datacenter consolidation. It is also the foundation for other VMware products, such as View™ and Lab Manager.

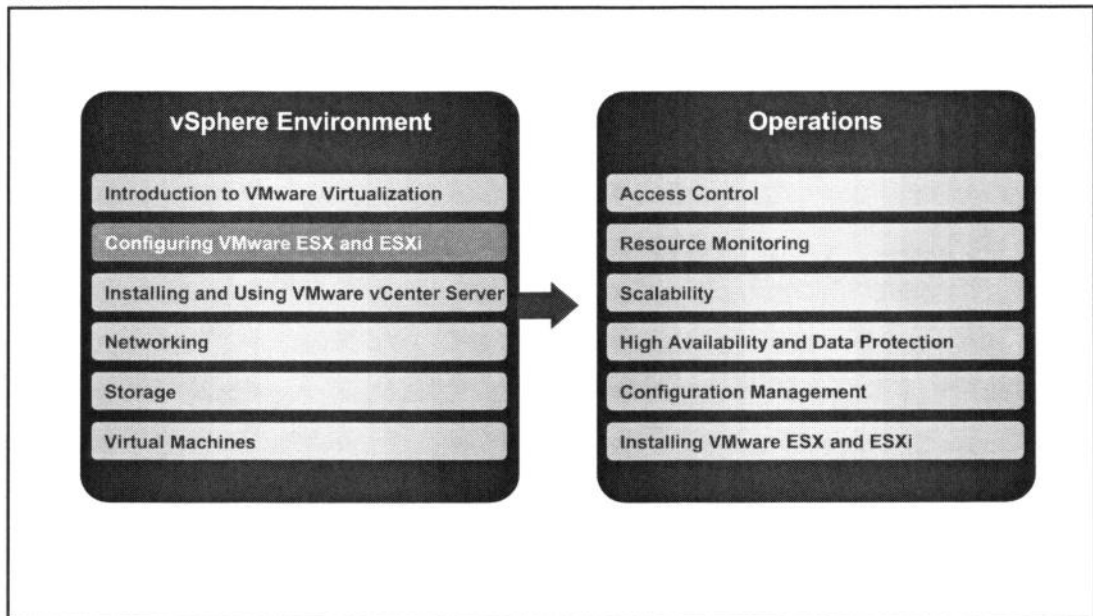
Configuring ESX/ESXi

Slide 3-1



You Are Here

Slide 3-2



Importance

Slide 3-3

- > VMware® ESX™/ESXi hosts provide the physical resources used to run virtual machines. Failure to properly install and configure ESX/ESXi hosts can negatively affect the performance, operation, and administration of all virtual machines located on these hosts.

Module Lessons

Slide 3-4

Lesson 1: Overview of ESX/ESXi

Lesson 2: Configuring ESX/ESXi

Lesson 1: Overview of ESX/ESXi

Slide 3-5

Lesson 1: Overview of ESX/ESXi

3

Configuring ESX/ESXi

Lesson Objectives

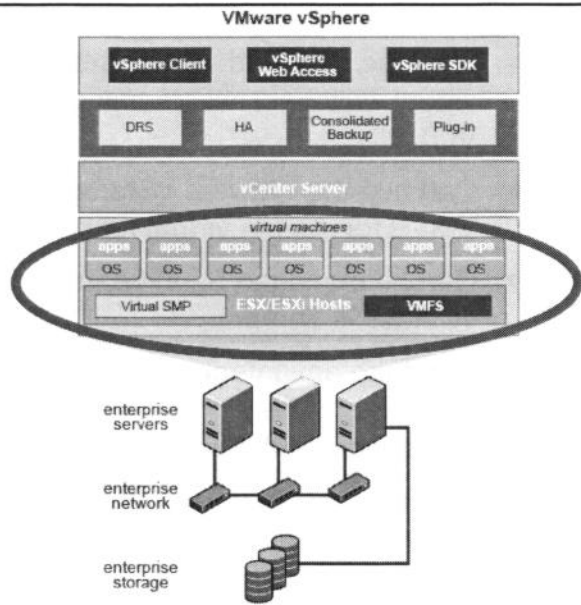
Slide 3-6

- > Describe the features of ESX/ESXi
- > Identify the different versions of ESX
- > Describe the architecture of ESX/ESXi

ESX/ESXi: Virtualization Platform

Slide 3-7

- ESX and ESXi are bare-metal, efficient, and reliable hypervisors running directly on server.
- ESX and ESXi abstract CPU, memory, storage, and networking into multiple virtual machines.

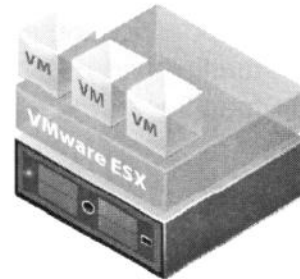
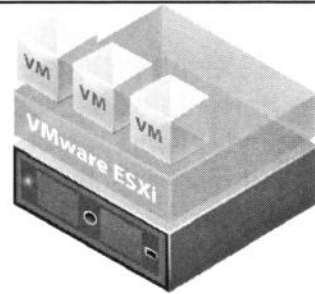


VMware® ESX™ and ESXi provide a virtualization layer that abstracts the processor, memory, storage, and networking resources of the physical host into multiple virtual machines. ESX and ESXi are hypervisors that create the foundation for a dynamic and automated datacenter.

ESX/ESXi Features

Slide 3-8

- > Can use standard and distributed virtual switches, NIC teaming, and VLANs
- > Can use the VMware vStorage VMFS for storing virtual machines
- > Can be managed by VMware vCenter™ Server
- > Can take advantage of various VMware vSphere™ features, such as VMware VMotion™
- > Can be accessed using the VMware vSphere Client



ESX/ESXi allows you to network virtual machines as you would physical machines, using standard and networking virtual switches, NIC teaming, and VLANs.

ESX/ESXi provides a few options for storing virtual machines. The most common way is using the VMware vStorage Virtual Machine File System (VMFS), a high-performance cluster file system that can be used to centralize virtual machine file storage for greater manageability, flexibility, and availability.

Multiple ESX/ESXi hosts can be centrally managed by VMware vCenter™ Server. vCenter Server can be used to provision, monitor, and manage the virtual machines located on these hosts.

ESX/ESXi can take advantage of the various features and components of VMware vSphere™, such as VMware VMotion™, Storage VMotion, VMware High Availability, Distributed Resource Scheduler (DRS), Distributed Power Management, Consolidated Backup, and vCenter Update Manager.

ESX/ESXi hosts can be accessed with the VMware vSphere Client. The vSphere Client is a graphical user interface that acts as a console to operate virtual machines and as an administration interface to ESX/ESXi hosts and vCenter Server.

ESX, ESXi Installable, and ESXi Embedded

Slide 3-9

ESX comes in two main versions:

> ESX

- Managed with a built-in service console or the vSphere Command-Line Interface (vCLI)
- Available as an installable CD-ROM boot image

> ESXi

- Managed with a BIOS-like direct console or vCLI
- A high-security, 32MB footprint
- ESXi Installable – Available as an installable CD-ROM boot image
- ESXi Embedded – ESX image preinstalled as firmware or burned onto an external USB key by the hardware vendor

*The better
way to go
The Future*

Two main versions of ESX are available:

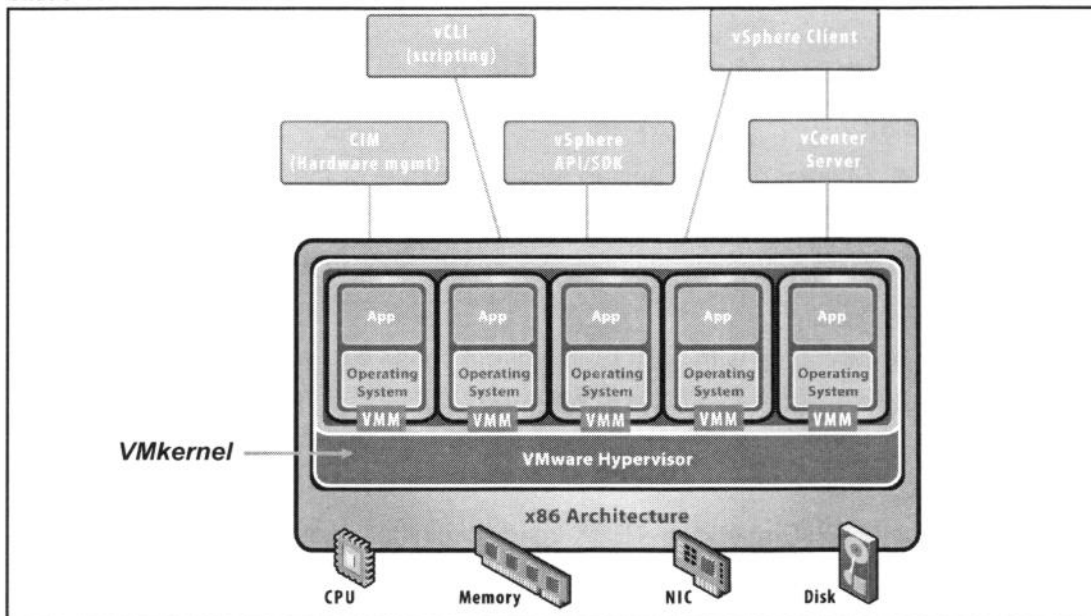
- ESX is a virtualization platform that contains a built-in service console used to manage the ESX host. It is available as an installable CD-ROM boot image.
- ESXi is a virtualization platform that does not contain a service console. It has a compact, 32MB footprint for increased security and reliability. It is available in two forms: ESXi Embedded and ESXi Installable.

ESXi Embedded is software that is preinstalled as firmware that is built into a server's physical hardware or burned onto an external USB key by the hardware vendor. Moving ESXi Embedded USB keys from one server to another is not supported.

ESXi Installable is software that is available as an installable CD-ROM boot image. You install the ESXi 4.0 Installable software onto a server's hard drive.

ESXi Architecture

Slide 3-10



ESXi is an enterprise-class hypervisor with a thin 32MB footprint for added security and reliability.

An ESXi host can be accessed using a number of interfaces, such as the vSphere Client (connected directly to the host or to vCenter Server), the vSphere Command-Line Interface (vCLI), the vSphere API/SDK, and CIM (Common Information Model). CIM is a management standard promoted by the Distributed Management Task Force. Much of the information that you can find using the CIM interface is also available through the vSphere API. However, there is some information that can be found only through CIM; most important, the health status of the hardware hosting ESXi.

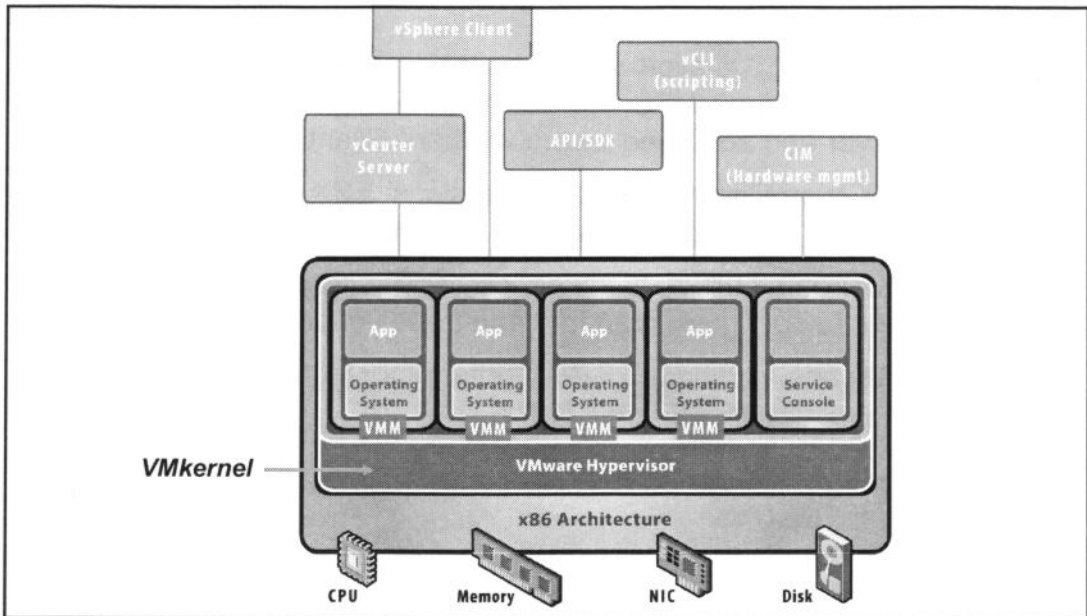
Under ESXi, applications running within virtual machines access CPU, memory, disk, and network interfaces without direct access to the underlying hardware. The ESX hypervisor is known as the VMkernel. The VMkernel intercepts virtual machines' requests for resources and presents them to the physical hardware.

ESXi is supported on Intel processors, Xeon and above, or AMD Opteron (32-bit-mode) processors. ESXi includes a 64-bit VMkernel. As a result, servers with 32-bit-only processors are not supported. ESXi offers support for a number of 64-bit guest operating systems.

For the complete list of supported systems for ESXi, see the compatibility guide at <http://vmware.com/resources/guides.html>.

ESX Architecture

Slide 3-11



Under ESX, applications running within virtual machines access CPU, memory, disk, and network interfaces without direct access to the underlying hardware. Like ESXi, the ESX hypervisor is also known as the VMkernel.

An ESX host can be accessed via a number of interfaces, such as the vSphere Client, the vCLI, and the vSphere API/SDK. An ESX host can also be managed by vCenter Server.

The ESX service console uses a 64-bit, 2.6-based Linux kernel compatible with Red Hat Enterprise Linux Server (RHEL) 5.2, CentOS 5.2, and equivalent Linux systems. The service console provides an execution environment to monitor and administer the entire ESX host. For example, the service console can monitor the health of the host's hardware.

ESX is supported on Intel processors, Xeon and above, or AMD Opteron (32-bit-mode) processors. Like ESXi, ESX also includes a 64-bit VMkernel. As a result, servers with 32-bit-only processors are not supported. ESX offers support for a number of 64-bit guest operating systems.

For the complete list of supported systems for ESX, see the compatibility guide at <http://vmware.com/resources/guides.html>.

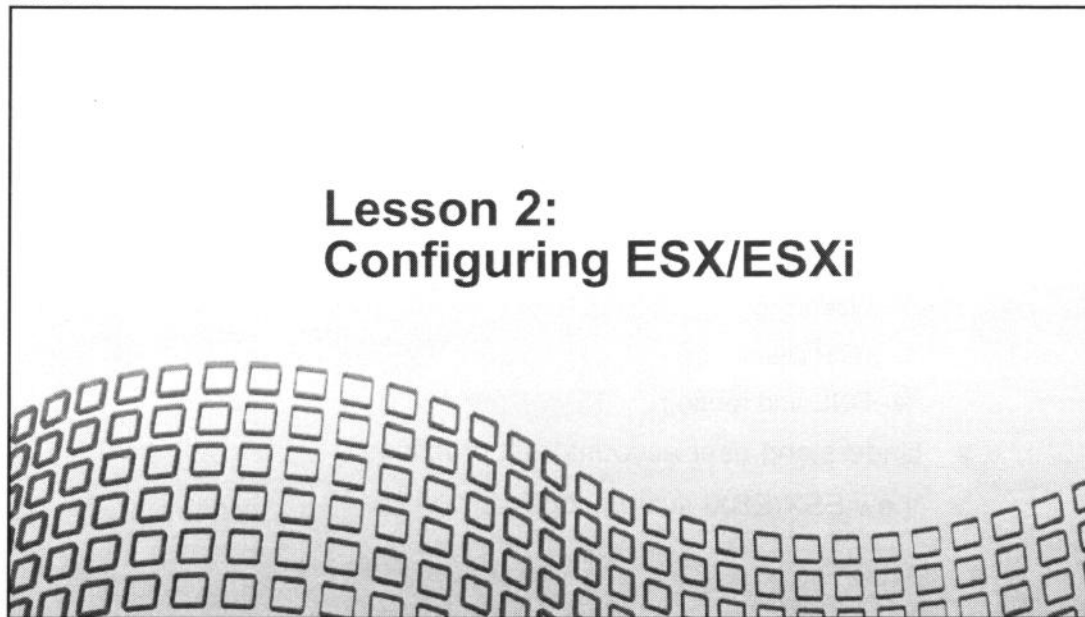
Lesson Summary

Slide 3-12

- > ESX and ESXi allow virtual machine networking and shared storage using VMFS. They can be managed by vCenter Server and accessed by the vSphere Client.
- > ESX is available in two main versions: ESX and ESXi (which includes ESXi Embedded and ESXi Installable).
- > ESX has a built-in, Linux-based service console that can be used to configure, manage, and troubleshoot the ESX host.
- > ESXi has a compact, 32MB footprint for increased security and reliability.

Lesson 2: Configuring ESX/ESXi

Slide 3-13



Lesson Objectives

Slide 3-14

- > Understand how to access the ESXi direct console user interface
- > Access an ESX/ESXi host using the vSphere Client
- > View or configure ESX/ESXi settings:
 - Processor and memory configuration
 - Licensing
 - NTP client
 - DNS and routing
- > Understand user account best practices
- > View ESX/ESXi system logs

Installing ESX/ESXi

Slide 3-15

- ESX must first be installed on supported hardware.
- ESXi Installable must first be installed on supported hardware.
- ESXi Embedded is preinstalled in the firmware of a supported vendor's hardware.
- In all cases, ESX or ESXi must be configured.

*This lesson assumes that ESX/ESXi
has already been installed.
(Installation is covered in a later module.)*

Whether you have to install ESX, depends on which version of the software you have. If you have ESX or ESXi Installable, you must install ESX. If you have ESXi Embedded, it is not necessary to install ESXi because the software is preinstalled for you by the hardware vendor.

During the ESX installation procedure, you can configure some aspects of the host, such as its host name and IP settings. You can also choose the disk device on which to install the software.

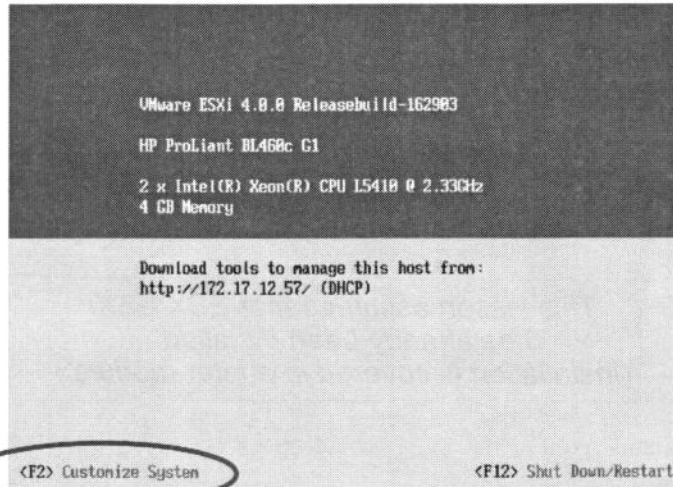
During the ESXi Installable procedure, you can choose the disk device on which to install the software.

Further configuration is usually necessary for all versions of ESX.

Configuring ESXi

Slide 3-16

- The direct console user interface is similar to the BIOS of a computer with a keyboard-only user interface.



The direct console user interface is used to configure certain settings for ESXi Embedded and ESXi Installable. The direct console is similar to the BIOS of a computer in that it has a keyboard-only user interface.

The direct console can be accessed from the ESX console. To start customizing system settings, press F2.

Configuring ESXi: root Access

Slide 3-17

The screenshot shows the ESXi System Customization menu. The 'Configure Password' option is highlighted with a black oval. The menu is divided into two columns. The left column lists various configuration options, and the right column shows the 'Configure Password' sub-menu with the 'Set' option selected. A text box overlay explains the direct console access options.

System Customization	Configure Password
Configure Password Configure Lockdown Mode	Set To prevent unauthorized access to this system, set the password for the user.
Configure Management Network Restart Management Network Test Management Network Disable Management Network Restore Standard Switch	
Configure Keyboard View Support Information View System Logs	
Restart Management Agents	
Reset System Configuration Remove Custom Extensions	
<Up/Down> Select	<Enter> Change <Esc> Log Out

The direct console allows an administrator to:

- > Set a root password (complex passwords only)
- > Enable or disable lockdown mode (to prevent user access to host as root)

The administrative user name for the ESXi host is root. By default, the administrative password is null. If you do not set a root password, you will be unable to log in to the ESXi host with the vSphere Client. To set the root password, select **Configure Root Password**, then press Enter. If you receive an error when setting the root password, it is likely that the password you chose is not complex enough. In general, choose a password that is more than six characters long and that has at least one uppercase character, one lowercase character, and one digit.

When enabled, lockdown mode prevents remote personnel from logging in to the ESXi host with the root login name. By default, lockdown mode is disabled. Users can still access the host through the direct console or through an authorized centralized management application, such as vCenter Server.

When lockdown mode is enabled, you can create a user with administrator privileges to connect to a standalone host. But do not use this approach in environments with numerous hosts, because maintaining separate user password databases for each host might be difficult to manage.

To enable or disable lockdown mode, select **Configure Lockdown Mode**, then press Enter. Choose to either enable or disable.

Configuring ESXi: Management Network

Slide 3-18

The screenshot shows the 'System Customization' menu in ESXi. The 'Configure Management Network' option is highlighted with a black oval. The right pane shows the configuration details for the management network.

System Customization	Configure Management Network
Configure Password	Hostname: sc-goose07
Configure Lockdown Mode	IP Address: 172.17.12.57
Configure Management Network	Network identity acquired from DHCP server 192.168.2.30
Restart Management Network	To view or modify this host's management network settings in detail, press <Enter>.
Test Management Network	
Disable Management Network	
Restore Standard Switch	
Configure Keyboard	
View Support Information	
View System Logs	

The direct console allows you to modify network settings like the host name, IP configuration (IP address, subnet mask, default gateway), and DNS servers.

<Up/Down> Select <Enter> More <Esc> Log Out

You must set up your IP address before your ESXi host is operational. By default, a DHCP-assigned address is configured for the ESXi host. To change or configure basic network settings, use the direct console or the vSphere Client.

From the direct console, you can change the host name, IP settings (such as IP address, subnet mask, default gateway), and DNS servers. You can also modify the network adapter used for the management network, configure VLAN settings, use an IPv6 configuration, and set custom DNS suffixes.

You can also restart the management network (without having to reboot the system), test the management network (using ping requests), and disable a management network.

Configuring ESXi: Other Settings

Slide 3-19

The screenshot shows the 'System Customization' menu in the ESXi direct console. The 'Configure Keyboard' option is highlighted with a black bar and circled in red. A callout box titled 'The direct console allows an administrator:' lists three functions: configuring keyboard layout, viewing support information, and viewing system logs. The background menu includes options like 'Configure Password', 'Configure Lockdown Mode', 'Configure Management Network', 'Restart Management Network', 'Test Management Network', 'Disable Management Network', 'Restore Standard Switch', 'Restart Management Agents', 'Reset System Configuration', and 'Remove Custom Extensions'. Navigation instructions at the bottom indicate '<Up/Down> Select', '<Enter> More', and '<Esc> Log Out'.

System Customization	Configure Keyboard
Configure Password	Default
Configure Lockdown Mode	To select the layout type for the keyboard of this host, press <Enter>.
Configure Management Network	The direct console allows an administrator: <ul style="list-style-type: none">> To configure the keyboard layout (default is English)> To view support information> To view system logs
Restart Management Network	
Test Management Network	
Disable Management Network	
Restore Standard Switch	
Configure Keyboard	
View Support Information	
View System Logs	
Restart Management Agents	
Reset System Configuration	
Remove Custom Extensions	
<Up/Down> Select	<Enter> More <Esc> Log Out

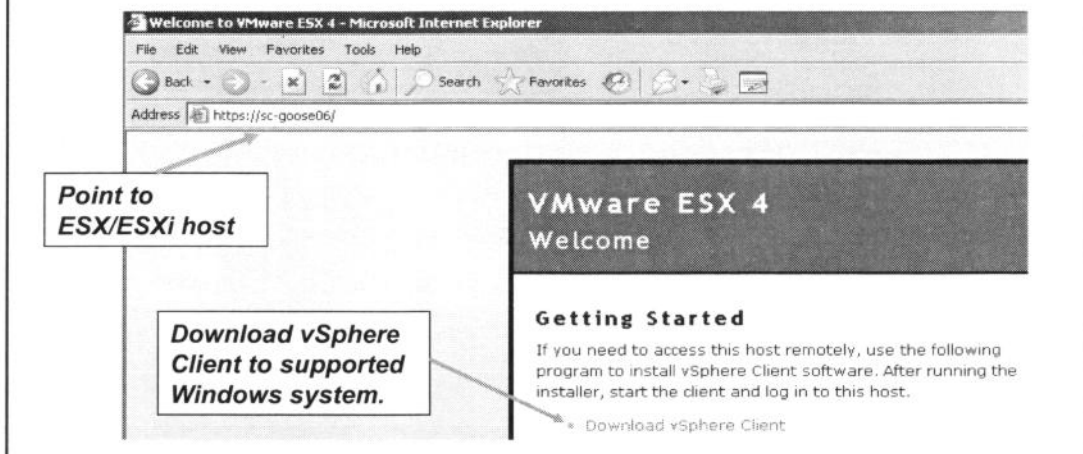
Finally, the direct console allows you to change the keyboard layout (the default is English), view support information, and view system logs.

You can also restart management agents, reset the system configuration, and remove custom extensions.

Using the vSphere Client

Slide 3-20

- > The vSphere Client is an interface used to connect remotely to ESX/ESXi or vCenter Server from any Windows PC.
- > Download software from the main page of ESX/ESXi.



The vSphere Client is the primary interface for managing all aspects of the vSphere environment. It is the interface to the vCenter Server and hosts. It also provides console access to virtual machines.

After ESX or ESXi is installed, a Welcome page is displayed, from which you can download the vSphere Client.

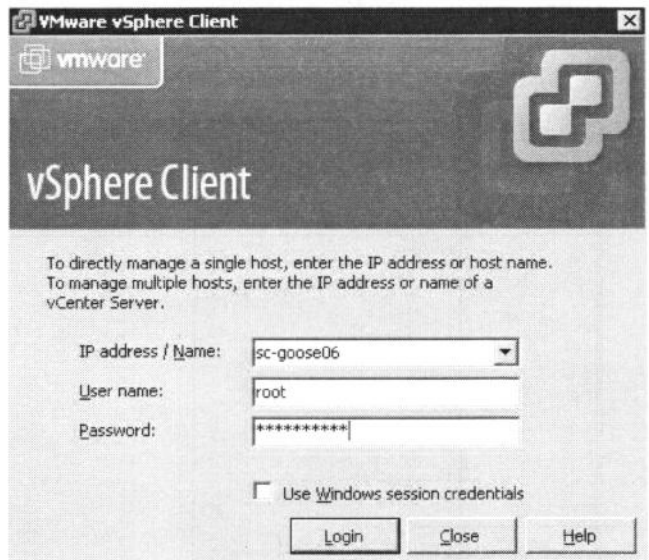
For the list of versions of ESX and ESXi hosts that the vSphere Client is compatible with, see the installation guide at <http://vmware.com/resources/guides.html>.

Logging In to ESX/ESXi

Slide 3-21

At the vSphere Client login screen, enter:

- > Host name or IP address of ESX/ESXi host
- > User name **root**
- > Password for user **root**

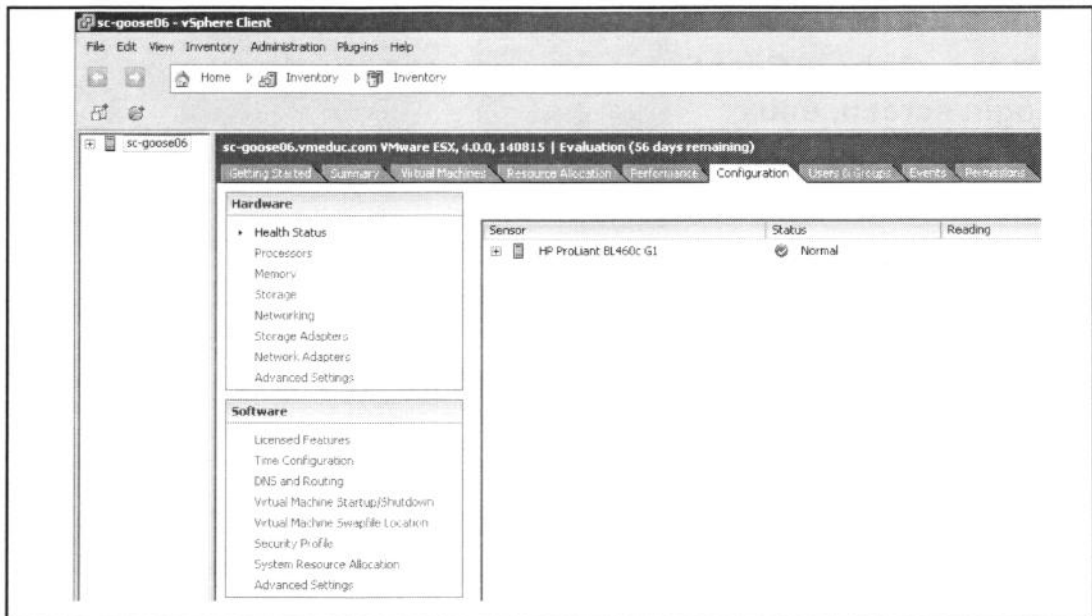


The vSphere Client provides direct access to an ESX/ESXi host. To log in to an ESX/ESXi host, provide the host name, a user account, and a password. In most cases, you will log in to the ESX/ESXi host as user root.

The **Use Windows session credentials** check box applies only when using the vSphere Client to log in to a vCenter Server system.

vSphere Client: Configuration Tab

Slide 3-22



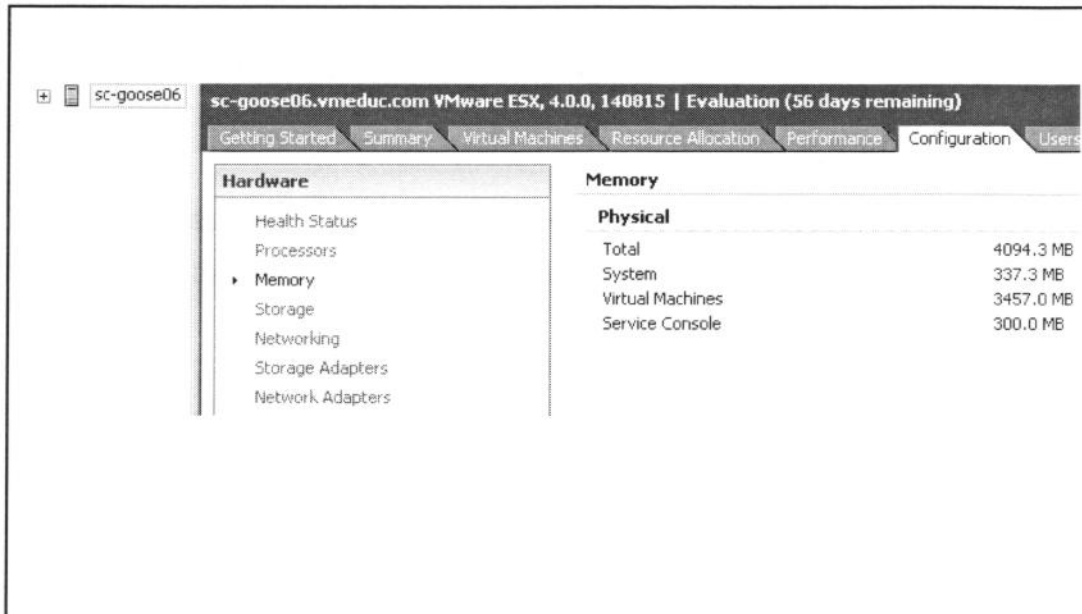
After you log in, the vSphere Client shows the ESX/ESXi host in the left pane. Click the **Configuration** tab to view or configure the host's hardware and software settings.

On the **Configuration** tab, you can view the health of your host's hardware, view the host's processor and memory configuration, add license keys, and configure a host's networking and storage. The vSphere Client also allows you to add a host's license key, configure the host as an Network Time Protocol (NTP) client, configure or modify the primary and secondary DNS servers, and modify the ESX service console's firewall.

You will use the **Configuration** tab to configure storage and networking in a later module.

Viewing Processor and Memory Configuration

Slide 3-23



In the **Hardware** section of the **Configuration** tab, the **Processors** link allows you to view information about your host's CPUs, such as model, processor speed, and the number of sockets, cores, and logical processors.

The **Memory** link (shown above) allows you to view information about the physical memory, such as total size and the amount of memory currently used for system overhead, virtual machines, and the service console (if viewing an ESX host).

On an ESX host, you can change the memory size of the service console if necessary. The change takes effect on the next system reboot. Increase the size of service console memory if you are going to run one or more management agents (such as a backup agent or system management agent) on the service console. The amount of additional memory necessary for the service console depends on the agent software to be run.

Before purchasing and activating licenses, you can install ESX/ESXi in evaluation mode.

Evaluation mode

- > Is intended for demonstration and evaluation purposes
- > Allows software to be completely operational immediately after installation
- > Does not require any licensing configuration
- > Provides full functionality of ESX/ESXi for 60 days from the time you install it
- > Allows the software to notify you of the time remaining in the evaluation period

Before purchasing and activating licenses for ESX/ESXi, you can install the software and run it in evaluation mode. Evaluation mode is intended for demonstrating the software or evaluating its features. During the evaluation period, the software is completely operational: you can use VMotion, DRS, VMware HA, and other useful features.

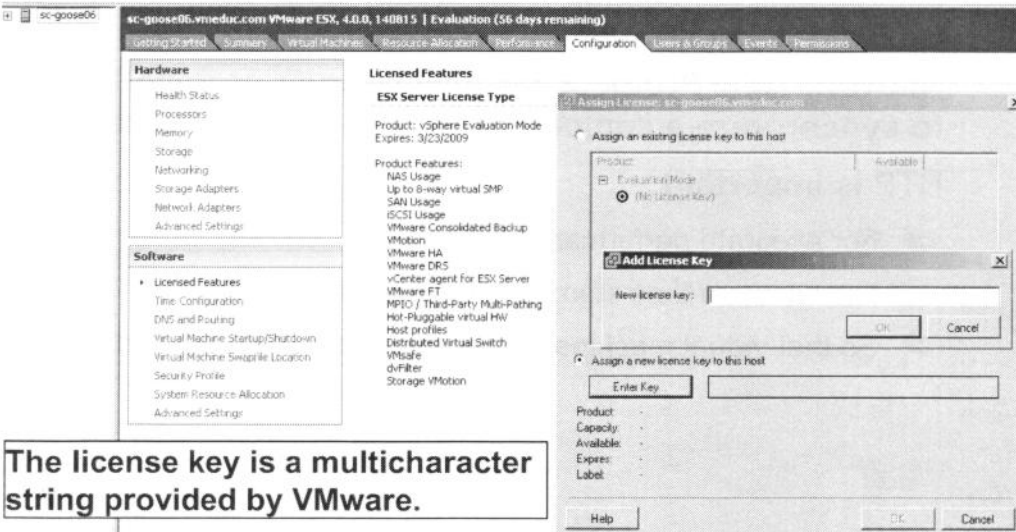
The evaluation period is 60 days from the time you install ESX/ESXi. During this period, the software notifies you of the time remaining until expiration. The 60-day evaluation period cannot be paused and it cannot be restarted.

After the 60-day evaluation period expires, you are no longer able to perform some operations in vCenter Server and ESX/ESXi. If you want to continue to have full use of ESX/ESXi and vCenter Server operations, you must acquire a license.

Without a license, you are able to perform some operations, but you cannot power on or reset your virtual machines. All hosts are disconnected from the vCenter Server if the evaluation period expires before you assign a license to the vCenter Server. Any single ESX/ESXi host is disconnected from the vCenter Server if the ESX/ESXi evaluation period expires before you assign a license to the host.

License Assignment Procedure

Slide 3-25



The screenshot displays the VMware ESX/ESXi configuration interface. The top navigation bar includes tabs for Getting Started, Summary, Virtual Machines, Resource Allocation, Performance, Configuration, Users & Groups, Events, and Permissions. The left sidebar shows the Hardware and Software sections. The main pane is divided into 'Licensed Features' and 'ESX Server License Type'. The 'Assigned License' dialog box is open, showing the 'Assign an existing license key to this host' option. The 'Add License Key' sub-dialog box is also visible, with a text field for the 'New license key:' and buttons for 'OK' and 'Cancel'. A text box at the bottom of the screenshot states: 'The license key is a multicharacter string provided by VMware.'

The license key is a multicharacter string provided by VMware.

To assign a valid license key to your ESX/ESXi host, click the **Licensed Features** link. The **Licensed Features** pane shows what type of license and what product features you currently have. In the example above, the host is running in evaluation mode. Click the **Edit** link to the right of the license type (not shown in the example). The Assign License dialog box enables you to assign a new license key to the host by entering the key, a multicharacter string provided by VMware.

Synchronizing Host Time Using NTP

Slide 3-26

Network Time Protocol is a client-server protocol used to synchronize a computer's clock to a time reference.

NTP is important:

- > For accurate performance graphs
- > For accurate time stamps in log messages
- > So that virtual machines have a source to synchronize with

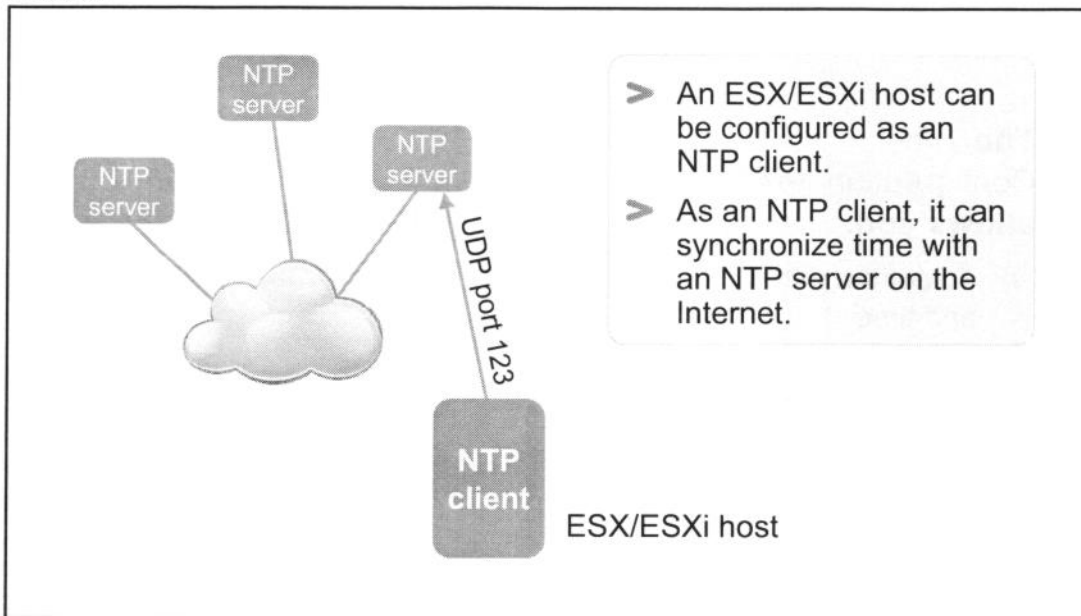
The Network Time Protocol (NTP) is an Internet standard protocol used to synchronize computer clock times in a network. There are several benefits to synchronizing an ESX/ESXi host's time:

- Performance data can be displayed and interpreted properly.
- Accurate time stamps appear in log messages (which make audit logs meaningful).
- Virtual machines can synchronize their time with the ESX/ESXi host. This is also beneficial to applications, such as database applications, running on the virtual machines.

For more information on NTP, see <http://www.ntp.org>.

ESX/ESXi as an NTP Client

Slide 3-27



NTP is a client-server protocol. When you configure the ESX/ESXi host to be an NTP client, the host synchronizes its time with an NTP server, which could be a server on the Internet.

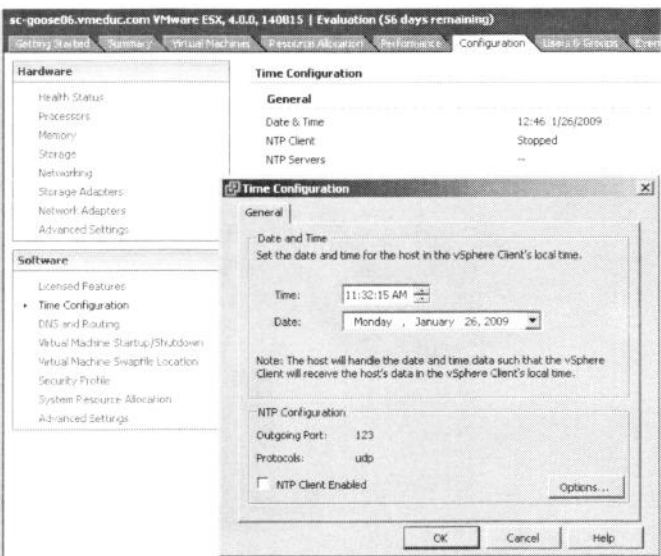
The system depends on multiple “strata” (layers) of time servers. Stratum 1 devices are connected directly to extremely sophisticated clock devices like atomic clocks to ensure that they have absolutely perfect time. Stratum 1 time servers are supposed to have time accurate to within 200 microseconds (1/5000th of a second). Stratum 2 time servers get their time from stratum 1. Time is requested and delivered via TCP/IP UDP port 123. There may be up to four strata in the hierarchy, and time within the lower levels is still supposed to be accurate to within 1/100th of a second.

Configuring ESX/ESXi as an NTP Client

Slide 3-28

The Time Configuration link allows you:

- > To set the date and time
- > To configure your host as an NTP client



The screenshot shows the VMware ESX/ESXi Configuration console. The left sidebar lists various configuration categories: Hardware, Software, and Time Configuration. The 'Time Configuration' link is highlighted. The main pane displays the 'Time Configuration' dialog box. The 'General' tab is active, showing the 'Date and Time' section with fields for 'Time' (11:32:15 AM) and 'Date' (Monday, January 26, 2009). Below this is a note: 'Note: The host will handle the date and time data such that the vSphere Client will receive the host's data in the vSphere Client's local time.' The 'NTP Configuration' section shows 'Outgoing Port' set to 123, 'Protocols' set to 'udp', and a checkbox for 'NTP Client Enabled' which is currently unchecked. An 'Options...' button is located next to the checkbox. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

To configure your ESX/ESXi host to be an NTP client, click the host's **Configuration** tab, then click the **Time Configuration** link. This displays the Time Configuration dialog box, shown above.

Here, you can enable the NTP client software and specify one or more NTP servers to synchronize with. You can also specify one or more NTP servers with which the ESX/ESXi host (the NTP client) can synchronize time.

Network Settings: DNS and Routing

Slide 3-29

The DNS and Routing link allows you to change:

- > Host name and domain
- > DNS server addresses and search domains
- > Service console and VMkernel gateways

DNS and Routing	
Host Identification	
Name	sc-geese07
Domain	vmeduc.com
DNS Servers	
Method	Static
Preferred DNS Server	192.168.2.30
Alternate DNS Server	192.168.100.30
Search Domains	
vmeduc.com	
Default Gateways	
Service Console	172.17.12.1
VMkernel	

The host's **DNS and Routing** link allows you to change the host name and domain, the primary and secondary DNS servers, as well as the service console gateway and VMkernel gateway.

To configure these settings, click the host's **Configuration** tab, then click the **DNS and Routing** link to display the information as shown above.

ESX Service Console Firewall

Slide 3-30

The ESX service console has a firewall through which you can enable or disable incoming or outgoing connections for a range of services.

The screenshot shows the 'Security Profile' window with the 'Firewall' tab selected. It lists incoming and outgoing connections. Below, the 'Firewall Properties' section includes a 'Remote Access' note and a table of services with checkboxes to enable or disable access.

Label	Incoming Ports	Outgoing Ports	Protocols	Daemon
Required Services				
Secure Shell				
<input checked="" type="checkbox"/> SSH Server	22		TCP	Running
<input type="checkbox"/> SSH Client		22	TCP	N/A
Simple Network Management Protocol				
<input type="checkbox"/> SNMP Server	161	162	UDP	N/A
Ungrouped				
<input type="checkbox"/> Software iSCSI Client		3260	TCP	N/A
<input checked="" type="checkbox"/> VMware vCenter Agent		902	UDP	N/A
<input type="checkbox"/> NTP Client		123	UDP	Stopped

ESX includes a firewall between the service console and the network. To ensure the integrity of the service console, there are very few firewall ports that are open by default. To provide or prevent access to certain services or clients, you must modify the firewall properties.

To modify the firewall properties, click the host's **Configuration** tab, then click the **Security Profile** link. In the **Security Profile** pane, click the **Properties** link (not shown above). The Firewall Properties dialog box appears (shown above).

To provide access to a service or client, select the appropriate check box. To prevent access, deselect the appropriate check box.

For example, if you want to use the iSCSI software initiator, you must provide access to the iSCSI software client by selecting its check box.

ESX/ESXi User Account Best Practices

Slide 3-31

- Strictly control root privileges to the ESX/ESXi host.
- Use the vSphere Client to manage the ESX/ESXi host.
- Ideally, use vCenter Server – and thus vCenter Server user accounts – to manage hosts.

On an ESX or ESXi host, the root user account is the most powerful user account on the system. The user root has access to all files and all commands. This user has almost unlimited capabilities. Therefore, securing this account is the most important step you can take to secure the ESX/ESXi host.

As a guideline, always use the vSphere Client to log in to your ESX/ESXi host. It is possible to log in to your ESX host from the service console. Likewise, it is possible to log in to your ESXi host through the vCLI.

Furthermore, once your host is managed by a vCenter Server, use the vSphere Client to log in to the vCenter Server and manage your host from there. Use the vSphere Client to connect directly to the ESX/ESXi host in unusual circumstances; for example, when the vCenter Server is down.

When you log in to the vCenter Server, you will use vCenter Server user accounts. These user accounts can be either local or domain accounts.

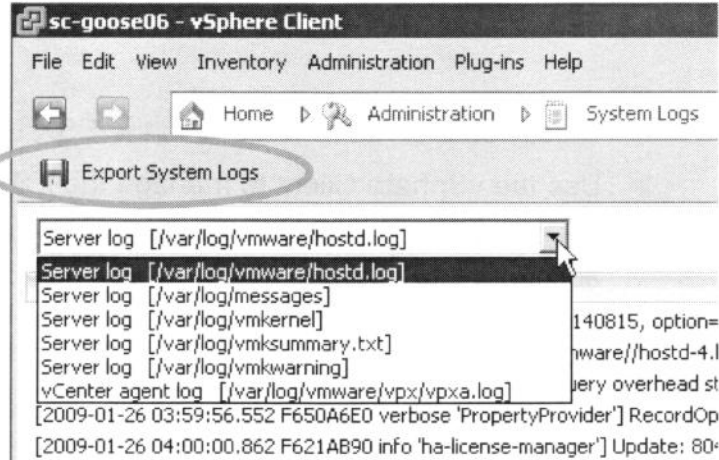
Viewing ESX/ESXi System Logs

Slide 3-32

View using the vSphere Client.

Export system logs to an archive file.

- Send in to VMware Support.



To view ESX/ESXi system logs, in the vSphere Client menu bar, click **View > Administration > System Logs**.

ESX and ESXi have the log files `hostd.log` and `messages`. These log files contain entries made during the bootup sequence and while the system is up and running.

ESX has the additional log files `vmkernel`, `vmksummary.txt`, and `vmkwarning`. These log files track service console availability; VMkernel alerts, warnings, and messages; and ESX host availability (including uptime and downtime).

The log file contents are especially useful to VMware Support. When working on a problem with VMware Support, you will need to provide them with your host's log files. The vSphere Client allows you to export system logs to a compressed archive file that you can send to VMware Support for further troubleshooting.

Lab 1 and eLearning Activity

Slide 3-33

In this lab, you will work configure an ESX host.

1. Log in to the ESX host using the vSphere Client.
2. View information about your host's hardware.
3. View information about your virtual machine.
4. Configure the ESX host as an NTP client.
5. Add DNS server and default gateway information to an ESX host.
6. Export the host's system logs.

In this eLearning activity, you will view a self-paced demonstration on how to install and configure an ESXi host.

➤ <http://mylearn.vmware.com/register.cfm?course=38258>

Lesson Summary

Slide 3-34

- > ESXi Installable and ESXi Embedded have a direct console user interface from which you can configure a few settings.
- > Use the vSphere Client to configure most of an ESX/ESXi host's settings.
- > Instead of accessing a host directly, whenever possible, manage and configure your ESX/ESXi hosts using vCenter Server.

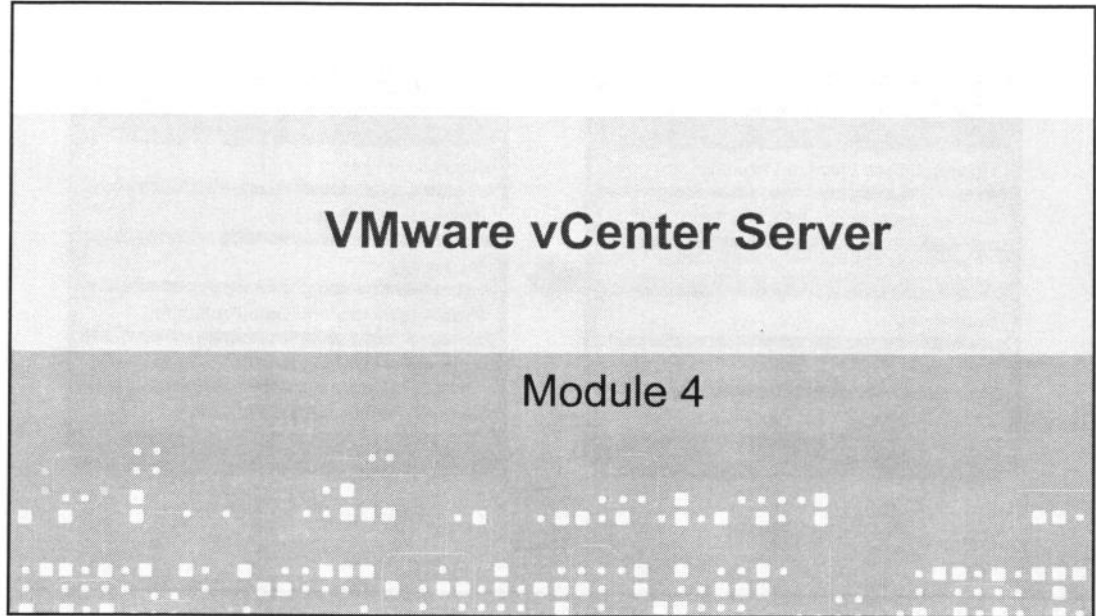
Key Points

Slide 3-35

- There are two main versions of ESX available: ESX and ESXi (which includes ESXi Installable and ESXi Embedded).
- ESXi hosts have a direct console user interface to configure items like the host name, IP settings, and keyboard layout.
- The vSphere Client is used to configure ESX/ESXi hosts.

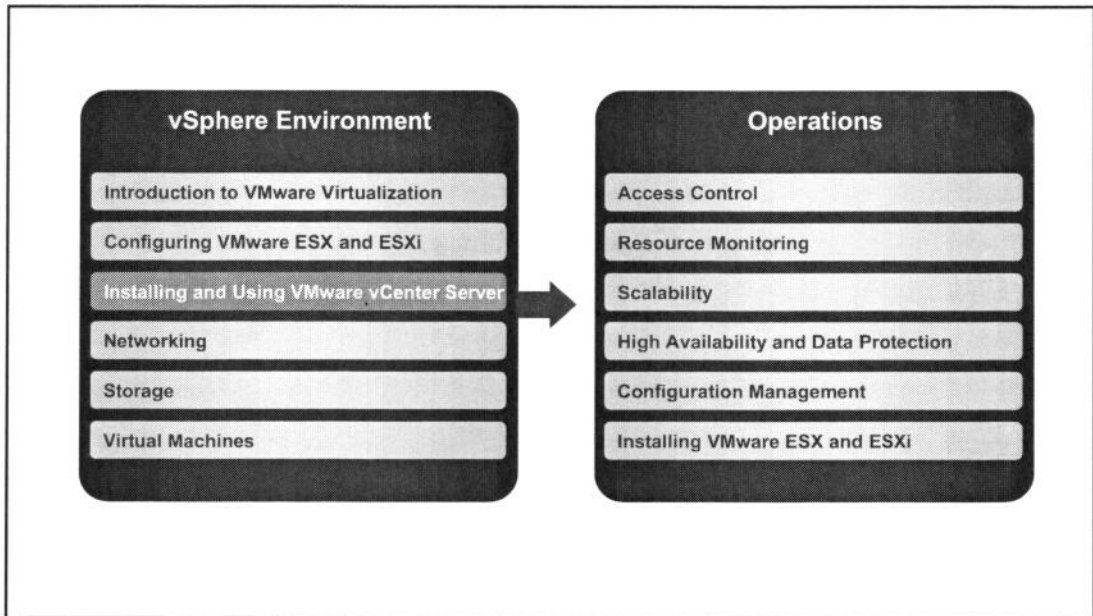
VMware vCenter Server

Slide 4-1



You Are Here

Slide 4-2



Importance

Slide 4-3

- > VMware® vCenter™ Server allows you to centrally manage multiple VMware ESX™/ESXi servers and their virtual machines. Failure to properly install, configure, and manage vCenter Server could result in reduced administrative efficiency or possible ESX/ESXi and virtual machine downtime.

Module Lessons

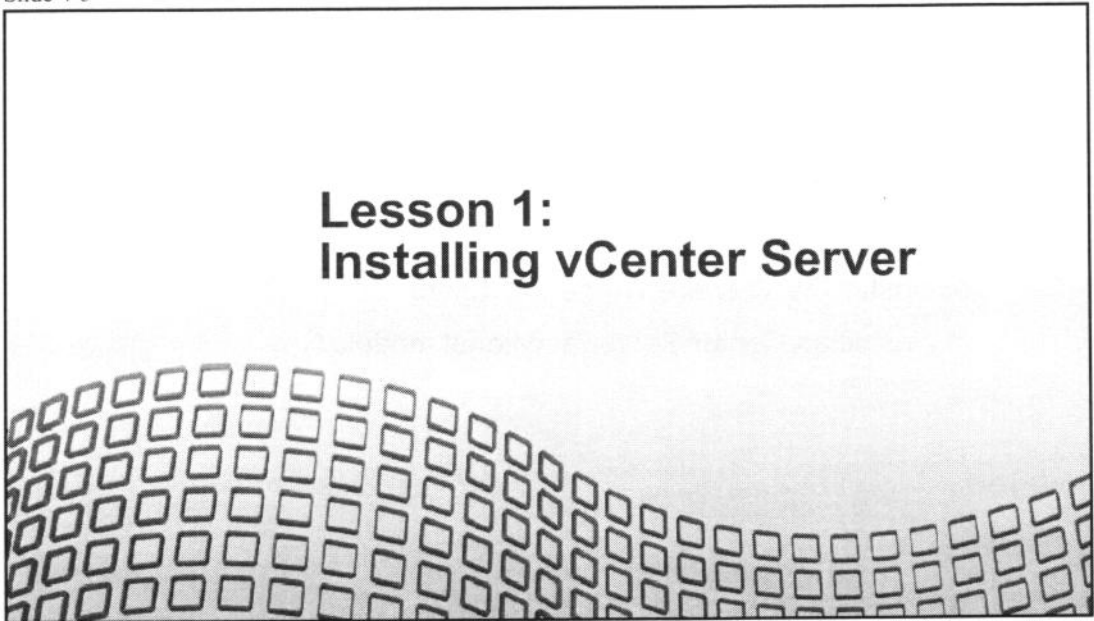
Slide 4-4

Lesson 1: Installing vCenter Server

Lesson 2: Using vCenter Server

Lesson 1: Installing vCenter Server

Slide 4-5



Lesson Objectives

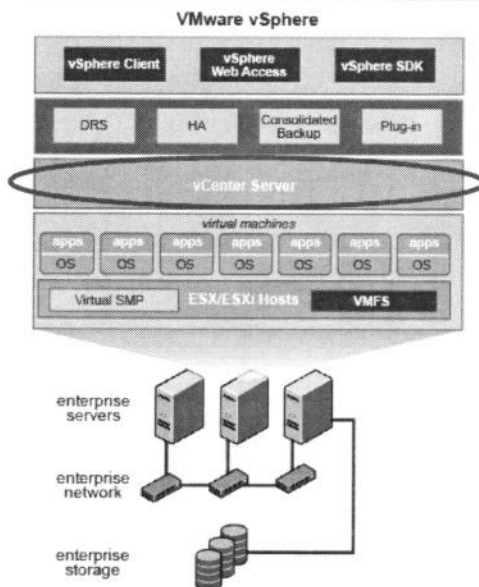
Slide 4-6

- > Describe the vCenter Server architecture
- > Describe the vCenter Server components
- > Install vCenter Server
- > Install the VMware vSphere™ Client
- > Install a vCenter Server additional module

vCenter Server: Management Platform

Slide 4-7

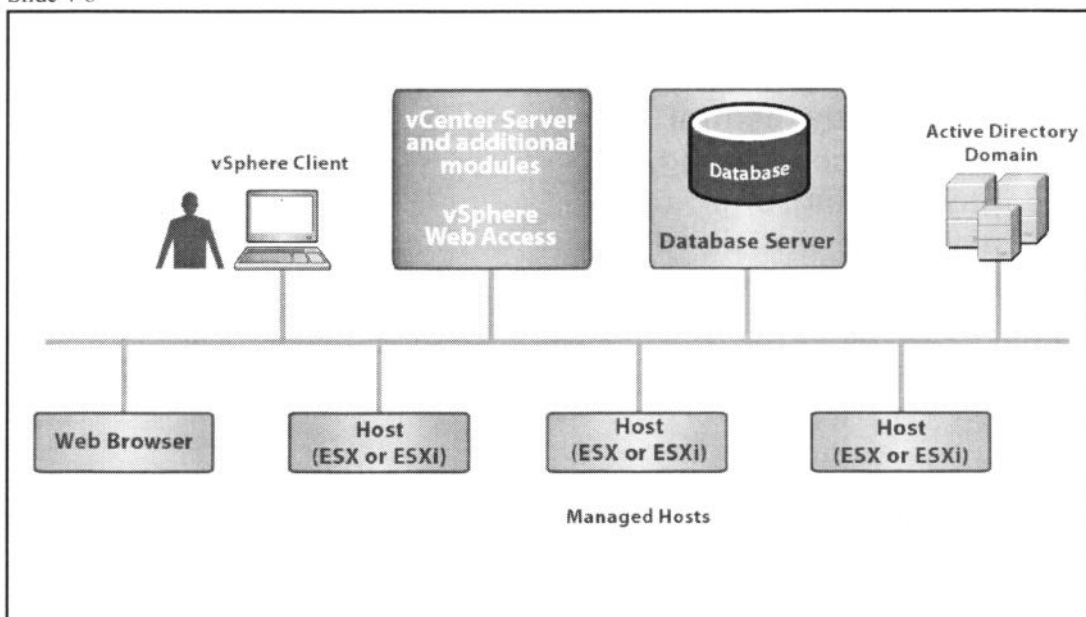
VMware vCenter Server is the central point for configuring, provisioning, and managing virtualized IT environments.



VMware® vCenter™ Server is the management server for VMware ESX™/ESXi hosts and virtual machines. The software consists of numerous services and modules. It is installed on a Windows server. vCenter Server provides advanced features such as VMware Distributed Resource Scheduler (DRS), VMware High Availability, and VMware VMotion™.

vCenter Architecture

Slide 4-8



The vCenter Server architecture relies on the following components:

- VMware vSphere™ Client – The same vSphere Client used to manage ESX/ESXi hosts is used to connect to the vCenter Server. Once an ESX/ESXi host is managed by vCenter, administrators should *always* use vCenter Server to manage that host.
- VMware vSphere Web Access – An alternative to the vSphere Client, vSphere Web Access is a browser-based application. You use it to manage virtual machines on ESX (currently, not ESXi) and vCenter Server deployments. Running vSphere Web Access does not require a lot of hardware resources, and you can use it to give users lightweight access to virtual machines.
- vCenter Server database – The most critical component is the vCenter Server database. The database stores the inventory items, security roles, resource pools, performance data, and other critical information for vCenter Server.
- Active Directory (AD) domain – Since the vCenter Server is installed on a Windows platform, security for the vCenter Server is built on Windows security. The vCenter Server system is not required to belong to an Active Directory domain. However, if the vCenter Server system is a member of an Active Directory domain, user accounts and groups from the domain will be available on the vCenter Server system. If the vCenter Server system is *not* a member of a domain, then vCenter Server uses local Windows users and groups.

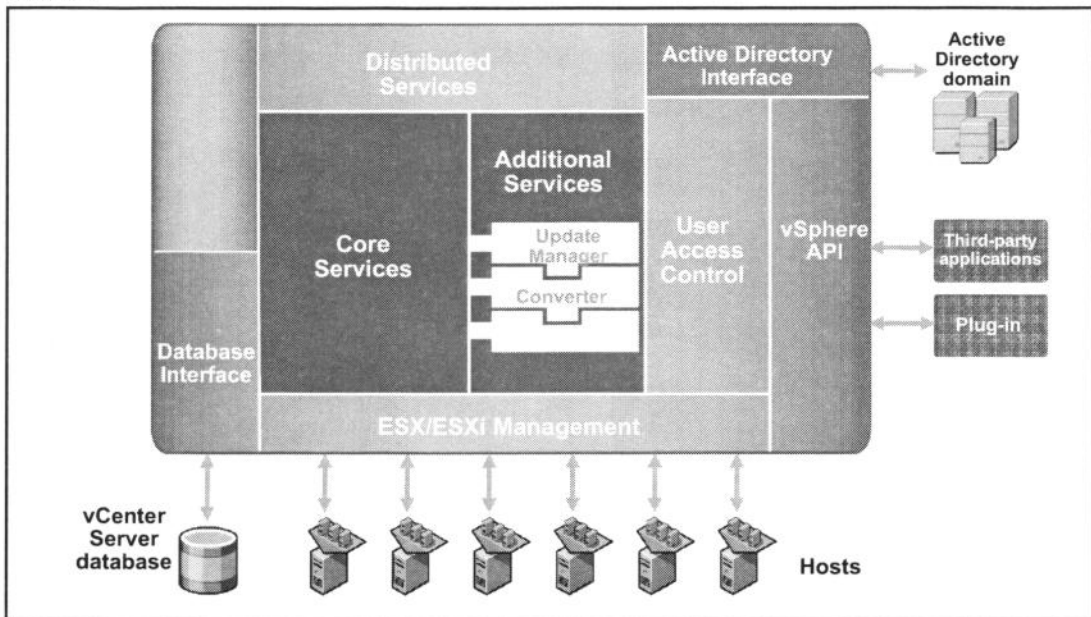
This has profound security implications for vSphere administration. For example, by default, anyone with Domain Administrator privileges in the AD domain will have full administrative

powers over all ESX/ESXi hosts and virtual machines that are being managed by vCenter Server. vSphere administrators will need to plan and coordinate security carefully with Windows Active Directory administrators.

- Managed hosts – vCenter Server manages ESX/ESXi hosts as well as the virtual machines that run on them.

vCenter Server Components

Slide 4-9



vCenter Server consists of the following services and interfaces:

- **Core services** – This represents the core functionality of the vCenter Server, which includes management of resources and virtual machines, task scheduling, statistics logging, management of alarms and events, virtual machine provisioning, and host and virtual machine configuration.
- **Distributed services** – This is the additional functionality of the vCenter Server; for example, VMotion, DRS, and VMware HA. They are installed with vCenter Server.
- **Plug-in** – This is also additional functionality. It is packaged separately from the base product and requires separate installation. No additional license is necessary. Examples of plug-ins include VMware vCenter Update Manager and vCenter Converter.
- **Database interface** – This provides access to the vCenter Server database.
- **ESX/ESXi management** – vCenter Server provides access to the ESX/ESXi host using a vCenter Server agent (also known as the `vpwa` process), which is installed on the host when it is added to vCenter Server inventory. The vCenter Server agent communicates with the host agent (also known as the `hostd` process) to relay the tasks to perform on the host. The host agent, like the vCenter Server agent, resides on the ESX/ESXi host.
- **Active Directory interface** – This provides access to domain user accounts.
- **VMware vSphere API** – Along with the vSphere SDK, the vSphere API provides an interface for writing custom applications that access vCenter Server functionality.

vCenter Server Modules

Slide 4-10

These modules provide additional features and functionality to vCenter Server.

Examples:

- > VMware vCenter Update Manager
- > VMware vCenter Converter

These modules include a server component and a client component:

- > The client component is a plug-in available for download and installation to vSphere Clients after the module is installed in vCenter Server.
- > The client component alters the interface by adding items related to the enhanced functionality.

vCenter Server modules are applications that provide additional features and functionality.

Typically, modules are comprised of a server component and a client component. After the server component of a module is installed, it is registered with vCenter Server, and the client component (also known as a plug-in) is available to vSphere Client for download. After a plug-in is installed on a vSphere Client, it might alter the interface by adding views, tabs, toolbar buttons, and menu options related to the enhanced functionality.

The vCenter Server additional modules are:

- vCenter Update Manager – Works with ESX/ESXi hosts, virtual machines, and virtual appliances running on ESX/ESXi hosts. Update Manager allows you to scan for compliance and apply updates for guest operating systems, virtual appliances, and hosts.
- vCenter Converter – Enables users to convert physical machines, and virtual machines in a variety of formats, to virtual machines that run on ESX/ESXi hosts. Converted systems can be imported into any location in the vCenter Server inventory.

Modules leverage core vCenter Server capabilities, such as authentication and permission management, but can have their own types of events, tasks, metadata, and privileges. Modules require vCenter Server, and they can be installed any time after vCenter Server has been installed. Modules and vCenter Server can be upgraded independently.

vCenter Server: Physical or Virtual Machine

Slide 4-11

When using a physical machine:

- A dedicated server is required.
- vCenter Server is not susceptible to potential VMware vSphere outage.
- vCenter Server performance is limited only by the system hardware.

When using a virtual machine:

- A dedicated server is not required.
- vCenter Server is susceptible to potential vSphere outage.
- The vCenter Server instance can be migrated from one system to another during maintenance activities.
- vCenter Server must contend for resources with the other virtual machines on the host.

vCenter Server can run on a physical machine or a virtual machine.

When running vCenter Server on a physical machine, a dedicated server is required. However, vCenter Server is not susceptible to potential outage in the vSphere environment. Backups of vCenter Server files are done using traditional backup tools, and vCenter Server performance is limited by the capabilities of the server hardware.

There are several advantages to running vCenter Server in a virtual machine:

- Instead of dedicating an entire physical server to vCenter Server, you can run it in a virtual machine along with others on the same ESX/ESXi host as other virtual machines. However, it is desirable to place the vCenter Server virtual machine outside of the environment you are managing.
- By encapsulating the vCenter Server instance in a virtual machine, you can transfer it from one host to another, enabling maintenance and other activities.
- The vCenter Server virtual machine can be backed up using Consolidated Backup. If the vCenter Server database is on a separate server, it is backed up separately.
- Using VMware HA, you can provide high availability for the vCenter Server system.

Remote SQL Recommended
Virtual of PHYSICAL
Either is supported.

vCenter Server Hardware/Software Requirements

Slide 4-12

Hardware requirements (physical or virtual machine)

- > **Processor** – 2.0GHz or higher Intel or AMD x86 processor*
- > **Memory** – 2GB RAM minimum*
- > **Disk storage** – 1GB minimum, 2GB recommended*
- > **Networking** – Gigabit recommended

*Requirements higher if vCenter Server database running on same system

Software requirements

- > Guest operating systems supported:
 - Windows XP Pro, Windows 2003 Server, Windows Server 2008
- > For a complete, detailed list of supported guest operating systems, see the vSphere installation guide.

vCenter Server hardware must meet the following requirements:

- Processor – 2.0GHz or higher Intel or AMD x86 processor. Processor requirements can be larger if your database is run on the same hardware.
- Memory – 2GB RAM minimum. RAM requirements can be larger if your database is run on the same hardware.
- Disk storage – 1GB minimum, 2GB recommended. You might need more storage if your database runs on the same hardware.
- Networking – Gigabit recommended (10/100 Ethernet adapter minimum).

vCenter Server is supported as a service on the 32-bit versions of a number of Windows guest operating systems. For the complete list of supported guest operating systems, see the vSphere installation guide at <http://www.vmware.com/support/pubs>.

vCenter Database Requirements

Slide 4-13

Each vCenter Server instance must have a connection to a database to organize all the configuration data.

Supported databases:

- > ~~IBM DB2~~
- > Microsoft SQL Server 2005
- > Microsoft SQL Server 2008
- > Oracle 10g and 11g
- > For a complete list of supported databases, see the vSphere installation guide.

Default database: Microsoft SQL Server 2005 Express

- > Bundled with vCenter Server
- > Used for product evaluations and demos
- > Also used for small deployments (up to 5 hosts and 50 virtual machines)

vCenter Server requires a database to store and organize server data. Update Manager also requires a database as well. It is possible for Update Manager to use the vCenter Server database. However, VMware recommends using one database for the vCenter Server and another database for Update Manager.

vCenter Server supports DB2, SQL Server, and Oracle databases. You must have administration credentials to log in to these databases. Contact your DBA for these credentials.

Alternatively, you can install the bundled Microsoft SQL Server 2005 Express database. This database is intended to be used for small deployments of up to 5 hosts and 50 virtual machines. For smaller deployments, you might not need a separate database for Update Manager.

For more details on the vCenter Server database requirements and for a complete list of supported databases, see the vSphere installation guide at <http://www.vmware.com/support/pubs>.

Calculating the Database Size

Slide 4-14

vCenter Server
has a built-in
database
calculator.

This is a “what
if” calculator.
No database
changes are
made.

vCenter Server Settings

Statistics
Select settings for collecting vCenter statistics

Statistics Intervals

Interval Duration	Save For	Statistics Level
<input checked="" type="checkbox"/> 5 Minutes	1 Days	1
<input checked="" type="checkbox"/> 30 Minutes	1 Week	1
<input checked="" type="checkbox"/> 2 Hours	1 Month	1
<input checked="" type="checkbox"/> 1 Day	1 Years	1

Database Size
Based on the current vCenter and inventory size, the vCenter database can be estimated. Enter the expected number of hosts and virtual machines in the inventory to calculate an estimate.

50 Physical Hosts Estimated space required: **14.28 GB**

2000 Virtual Machines

Click Help for details on how the vCenter database size is calculated.

The size of the database varies with the number of hosts and virtual machines to manage and the number of statistics to be collected. To ensure that your database can handle the statistics collection you configure, the vSphere Client provides you with a database estimation calculator in which you enter the number of hosts and virtual machines in your inventory. The calculator uses these numbers to determine how much database space is required for the collection interval configuration you defined. This ensures that you have the necessary resources.

To use the calculator

1. Choose **Administration > vCenter Server Settings**.
2. Select the **Statistics** option in the left pane.
3. Make your changes in the right-hand window.

The calculator automatically makes an estimate based on your changes. This is a “what-if” calculator. No changes are made to the size of the vCenter Server database.

Steps Before Installing vCenter Server

Slide 4-15

Before beginning the vCenter Server installation, perform the following steps:

1. Ensure that vCenter Server hardware and software requirements are met.
2. Ensure that the vCenter Server system belongs to a domain rather than a workgroup.
3. Create a vCenter Server database, unless using the default database.
4. Obtain and assign static IP address and host name to the vCenter Server system.

Before you begin the vCenter Server installation procedure, ensure that you have done the following:

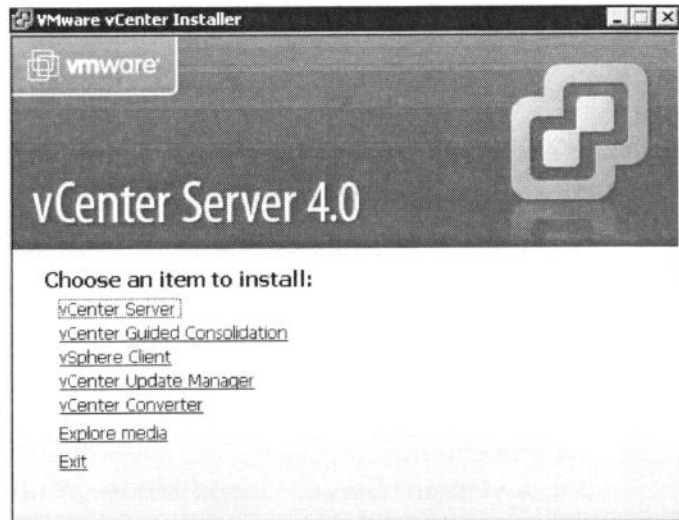
- Make sure that the system you use for vCenter Server meets the hardware and software requirements.
- Make sure that the system you use for vCenter Server belongs to a domain and not a workgroup. If assigned to a workgroup, vCenter Server is not able to discover all domains and systems available on the network when using such features as VMware vCenter Guided Consolidation and vCenter Server Linked Mode groups.
- Create a vCenter Server database, unless you want to use SQL Server 2005 Express, the default vCenter Server database.
- Obtain and assign a static IP address and host name to the Windows server that will host vCenter Server. This IP address must have a valid (internal) DNS registration that resolves properly from all managed ESX hosts.
- You can deploy vCenter Server behind a firewall. However, make sure there is no network address translation (NAT) firewall between vCenter Server and the hosts it will manage.

vCenter Server Installation Procedure

Slide 4-16

Launch the VMware vCenter Installer wizard.

Other vSphere components can also be installed with this wizard.



To install vCenter Server and its components, use the VMware vCenter Installer wizard. You can launch the installer by running the `autorun.exe` in the installation folder (or on the CD-ROM image).

To launch the vCenter Server installation, click the **vCenter Server** link.

vCenter Server Installation Information

Slide 4-17

The vCenter Server installer asks for the following information:

- > User name and organization
- > License key
- > Database information
 - Use default database or existing database.
 - If existing database, enter database user name and password.
- > SYSTEM account or user-specified account
- > Destination folder for software
- > Whether to install vCenter as a standalone instance or to join it to a vCenter Server Linked Mode group
- > vCenter Server ports

The vCenter Server installer prompts you for the following information:

- User name, organization, and license key

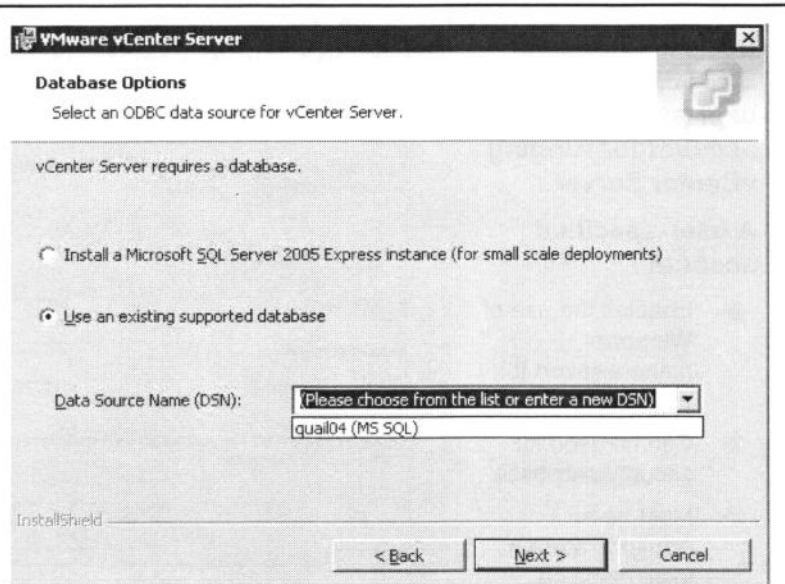
If you omit the license key, vCenter Server is installed in evaluation mode. After installation, you can use the vSphere Client to enter the vCenter Server license.
- Database information (discussed in a later slide)
- SYSTEM account or user-specified account (discussed in a later slide)
- Destination folder for software
- Whether to install a standalone vCenter Server instance or to join it to a Linked Mode group (discussed in a later slide)
- vCenter ports (discussed in a later slide)

Configuring Access to the Database

Slide 4-18

Database information:

- > Use the default database or an existing supported database.



The Database Options page of the vCenter Server installer allows you to choose between the default database or an existing supported database.

A data source name must be created. The DSN contains specific information about the database that the ODBC driver needs in order to connect to it.

If you chose to use an existing supported database, you will also be asked, on a different page in the installer, to enter the database user name and password (not shown above).

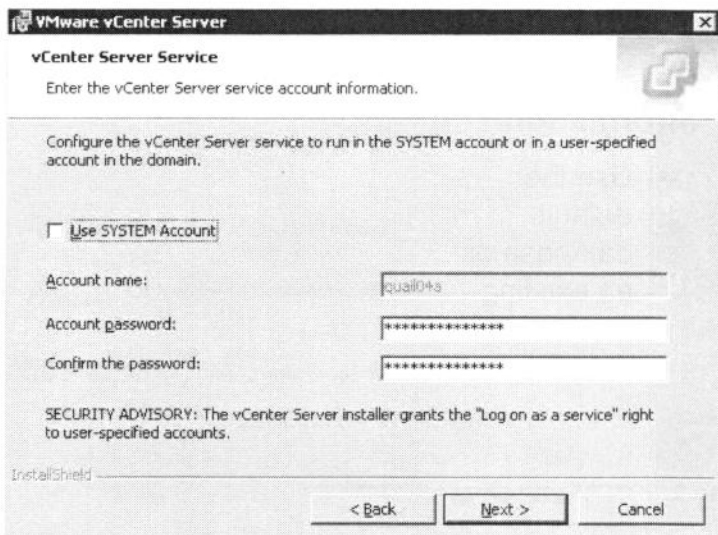
vCenter Server Account Considerations

Slide 4-19

Use the Windows SYSTEM account or a user-specified account for running vCenter Server.

A user-specified account

- Enables the use of Windows authentication for SQL Server
- Can be used for security purposes
- Must be an Administrator on local machine



The vCenter Server installer gives you the option to use the Windows system account or a user-specified account for the purpose of running vCenter Server.

The primary reason to use a user-specified account is to enable the use of Windows authentication for SQL Server. Another reason to use a user-specified account is security. The built-in SYSTEM account has more permissions and rights on the system than vCenter Server needs, which can contribute to security problems.

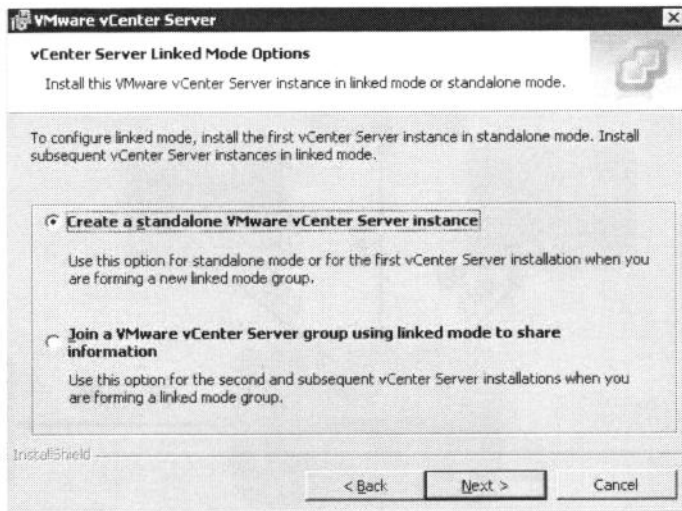
Even if you do not plan to use Windows authentication for SQL Server or you are using an Oracle database, you might want to set up a local user-specified account for vCenter Server. The only requirement is that the user-specified account is an Administrator on the local machine.

Standalone Instance or Linked Mode Group

Slide 4-20

Install vCenter Server as a standalone instance or as part of a vCenter Linked Mode group.

- > vCenter Linked Mode allows you to view and manage the inventories of multiple vCenter Server instances.
- > Use vCenter Linked Mode primarily for large-scale managing and monitoring of virtual environments.



The vCenter Server installer allows you to install vCenter Server as a standalone instance or as part of a vCenter Linked Mode group.

Use standalone mode if this is the first vCenter Server instance you are installing.

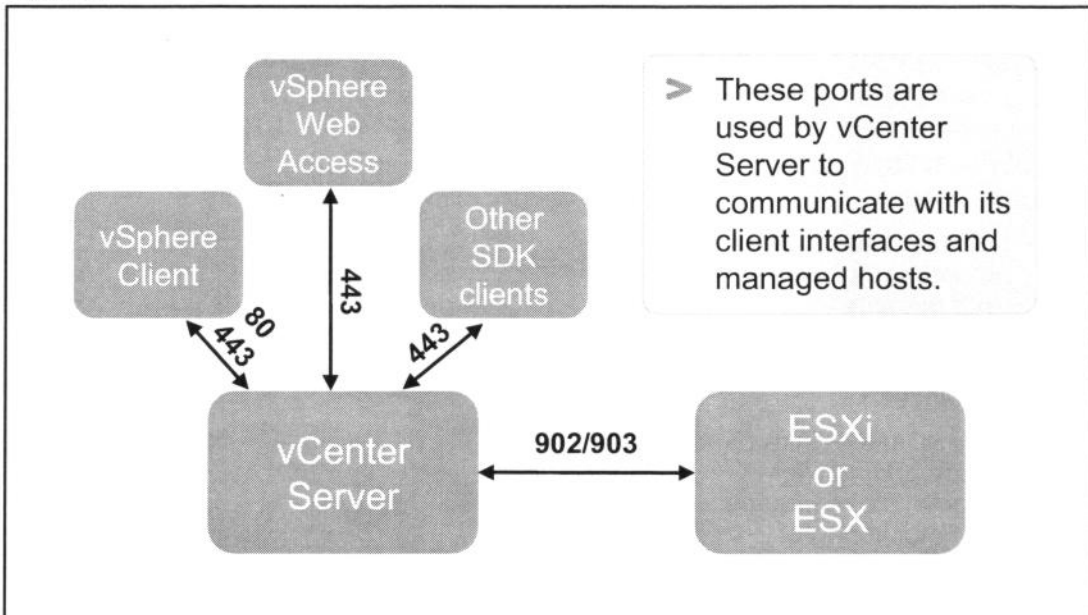
A Linked Mode group allows you to log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Server systems in the group. Linked Mode is used primarily in large-scale environments.

When adding a vCenter Server instance to a Linked Mode group, the user running the installer must be both a local administrator on the machine where vCenter Server is being installed and on the target machine of the existing Linked Mode group. This generally means that the installer must be run by a domain user who is an administrator on both systems.

For a complete list of the requirements to implement vCenter Linked Mode, see the vSphere installation guide at <http://www.vmware.com/support/pubs>.

Ports Used by vCenter Server

Slide 4-21



vCenter Server must be able to send data to every managed host and receive data from every vSphere Client. VMware uses designated ports for communication.

vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. vCenter Server uses port 443 to listen for data transfer from the vSphere Client, the vSphere Web Access Client, and other SDK clients

Additionally, the managed hosts listen for data from vCenter Server on designated ports. Port 902 is the default port that vCenter Server uses to send data to the managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to vCenter Server. Ports 902 and 903 must not be blocked between the vSphere Client and the hosts. They are used by the vSphere Client to display virtual machine consoles.

If a firewall exists between any of these elements, you must open the ports manually to allow data transfer to these designated ports.

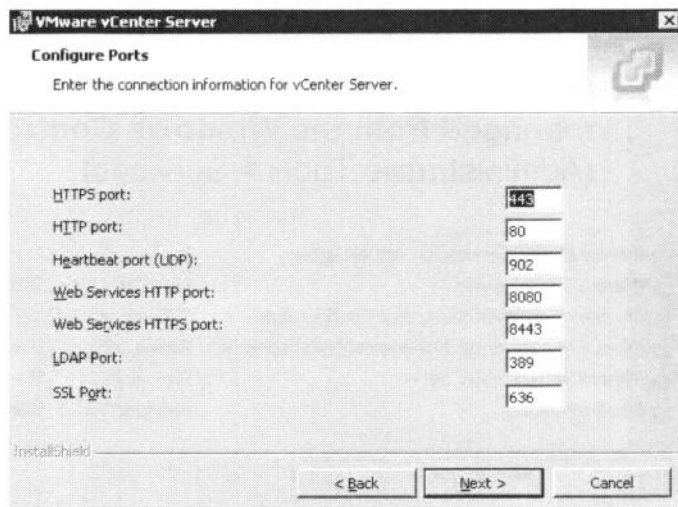
Configuring Ports Used by vCenter Server

Slide 4-22

Customize these ports or use the defaults.

In addition to ports 80, 443, and 902, other ports used are:

- 8080 and 8443: For Web Services HTTP and HTTPS ports
- 389 and 636: LDAP and SSL ports used by Directory Services



Unless you have a specific reason to change the ports, use the default ports assigned:

- For HTTPS, the default port is 443. If you use another port number, you must use this format: <ip_address>:<port> when you log in to vCenter Server.
- For HTTP, the default port is 80. Other services conflict with vCenter Server if they use port 80. 80 redirects requests to HTTPS port 443
- Managed hosts send a regular heartbeat over UDP port 902 to vCenter Server.
- The Web services HTTP and HTTPS ports are 8080 and 8443, respectively.
- For LDAP and SSL, vCenter Server needs to bind to port 389 and 636, even if you are not joining this vCenter Server instance to a Linked Mode group.

However, you can run the vCenter Server LDAP service and the vCenter Server SSL service on ports other than port 389 and 636 by changing to available ports from 1025 through 65535.

vCenter Server Services

Slide 4-23

vCenter Server is installed on a Windows system.

Once installed, vCenter Server services can be managed from the Windows Control Panel (Administrative Tools > Services).

 VMware Mount Service for VirtualCenter			Manual	Local System
 VMware Tools Service	Provides s...	Started	Automatic	Local System
 VMware vCenter Orchestrator Configuration	VMware vC...		Automatic	Local System
 VMware VirtualCenter Management Webservices	Allows conf...	Started	Automatic	Local System
 VMware VirtualCenter Server	Provides c...	Started	Automatic	Local System
 VMwareVCMSDS	Provides V...	Started	Automatic	Network Service

After vCenter Server is installed, a number of new Windows services appear on the vCenter Server system:

- VMware Mount Service for VirtualCenter – Used during guest operating system customization (during cloning a virtual machine or deploying a virtual machine from template)
- VMware VirtualCenter Management Webservices – Allows configuration of vCenter management services
- VMware VirtualCenter Server – The heart of vCenter Server, it provides centralized management of virtual machines and ESX/ESXi hosts
- VMwareVCMSDS – Provides vCenter Server LDAP directory services
- VMware vCenter Orchestrator Configuration – A service for Orchestrator, a workflow engine that can help administrators automate existing manual tasks.

The VMware Tools Service shown above is not installed during the vCenter Server installation. It is installed when VMware Tools is installed into the guest operating system of a virtual machine. VMware Tools is discussed in a later module.

vSphere Client Installation Procedure

Slide 4-24

- 1. Start the VMware vCenter Installer wizard.**
- 2. Select vSphere Client.**
- 3. In the vSphere Client installer:**
 - a. Accept the EULA.
 - b. Enter user name and company name.
 - c. Select Install VMware vSphere Host Update Utility if you plan to manage host patches, updates, and upgrades from this machine.
 - d. Accept the default installation location.

The vSphere Client can also be installed quickly and easily by using the VMware vCenter Installer wizard. The vSphere Client runs on a specific list of Windows operating systems.

For details on the vSphere Client hardware and software requirements, see the vSphere installation guide at <http://www.vmware.com/support/pubs>.

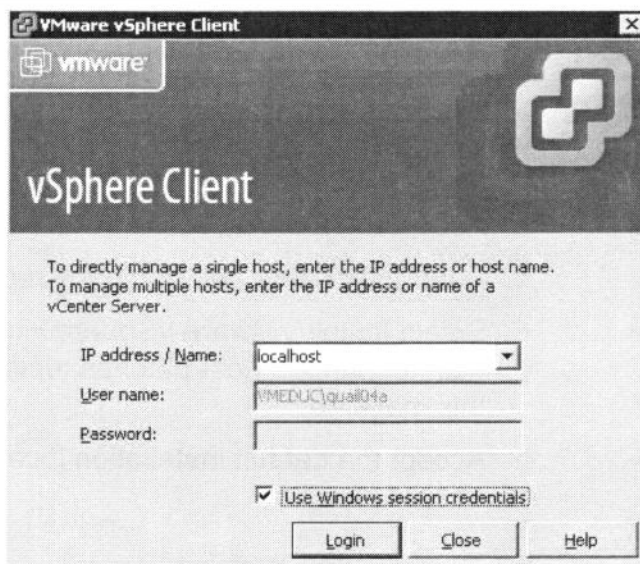
Logging In to the vSphere Client

Slide 4-25

At the vSphere Client login screen, enter:

- > Host name or IP address of the vCenter Server system
- > Windows user and password

(Optional) Use your Windows session credentials.



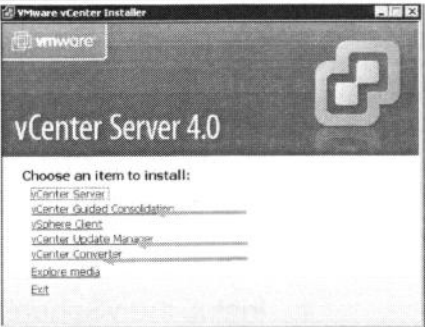
To launch the vSphere Client, double-click the vSphere Client icon, located on the desktop of the system on which you installed the client.

On the login window, shown above, enter the host name or IP address of the vCenter Server system. If you are launching the vSphere Client on the vCenter Server system, you can enter `localhost` as the name. Enter your Windows user and password, which is either a local or domain account. If you want to log in to the vCenter Server system with the same user name and password that you used to start your Windows session, select the **Use Windows session credentials** check box. If you do this, you do not have to enter your user name and password on this login window.

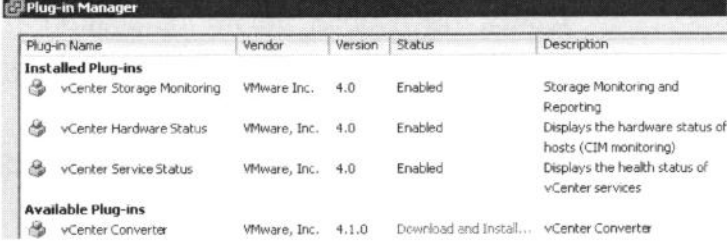
Installing vCenter Additional Modules and Plug-Ins

Slide 4-26

To install an additional vCenter Server module, use the VMware vCenter Installer wizard.



To install the corresponding plug-in, use the Plug-in Manager.



To install vCenter Server modules like vCenter Converter or Update Manager, use the VMware vCenter Installer to install the server component of these modules.

To view the Plug-in Manager, in the vSphere Client menu bar choose **Plug-ins > Manage Plug-ins**. After the server component of a vCenter Server additional module is installed, the Plug-in Manager allows you to download and install the plug-in for that module. In the example above, the vCenter Converter plug-in can be downloaded and installed.

The Plug-in Manager also allows you to view all installed plug-ins as well as download and install new plug-ins. By default, vCenter Server has three plug-ins installed and enabled:

- vCenter Storage Monitoring – Allows vCenter Server to monitor and report on storage. When enabled, this plug-in adds the host's **Storage Views** tab to the vSphere Client interface.
- vCenter Service Status – Allows vCenter Server to display the health status of vCenter services. When enabled, this plug-in adds the **vCenter Service Status** administration option to the vSphere Client interface. To display this option, go to **Home > Administration > vCenter Service Status**.
- vCenter Hardware Status – Allows vCenter Server to display the hardware status of hosts (CIM monitoring). When enabled, this plug-in adds the host's **Hardware Status** tab to the vSphere Client interface.

Lab 2

Slide 4-27

In this lab, you will install vCenter Server components.

1. Access your vCenter Server system.
2. Configure a SQL Server ODBC connection to a preconfigured database.
3. Install vCenter Server.
4. Install the vSphere Client.
5. Check the vCenter Server installation.
6. Install an additional vCenter Server module: vCenter Converter.
7. Install and enable a plug-in: Converter plug-in.

Lesson Summary

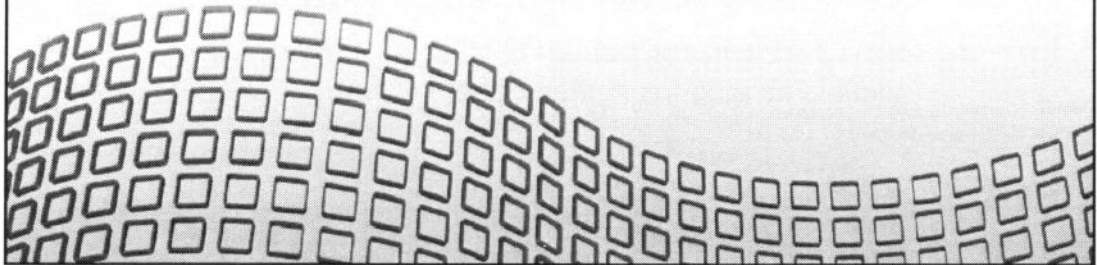
Slide 4-28

- > The vCenter architecture consists of the vCenter Server, the vCenter Server database, vSphere Web Access, vSphere Client, Active Directory, and managed ESX/ESXi hosts.
- > Install vCenter Server and its components using the VMware vCenter Installer wizard.
- > Install the server component of vCenter Server additional modules using the VMware vCenter Installer wizard.
- > Install the client component of vCenter Server additional modules as plug-ins in the vSphere Client.

Lesson 2: Using vCenter Server

Slide 4-29

Lesson 2: Using vCenter Server



Lesson Objectives

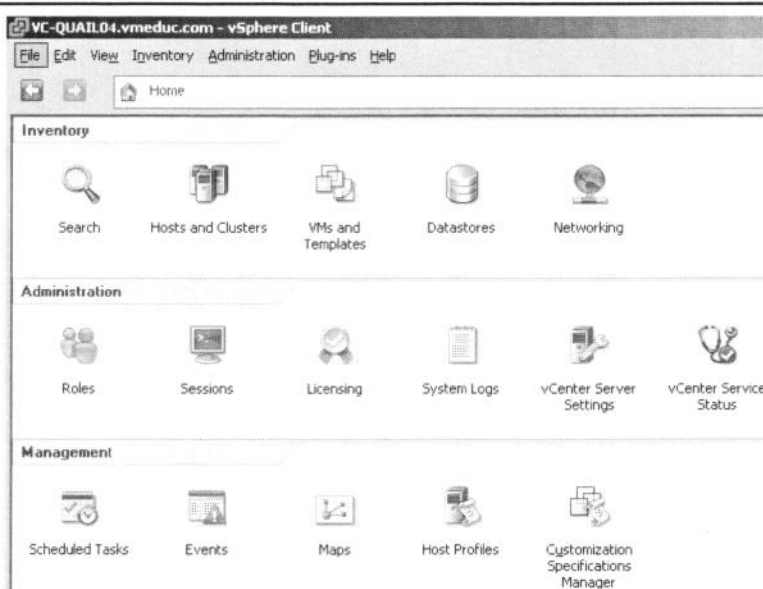
Slide 4-30

- > Navigate using the vSphere Client
- > Create and organize vCenter Server inventory objects
- > Add license keys to vCenter Server
- > View vCenter Server logs and events
- > Create a vCenter Server administrator

vSphere Client Home Page

Slide 4-31

This lesson focuses on the inventory and some administration tasks.



When you log in to vCenter Server using the vSphere Client, the Home page is displayed. The default layout is the Home page with a menu bar, navigation bar, search box, status bar, and panel sections. The Home page contains icons for major vSphere Client functions, divided in to four categories: **Inventory**, **Administration**, **Management**, and **Solutions and Applications**. When you log out of the vSphere Client, the client application retains the view that was displayed when it was closed and will return you to that view when you next log in.

You return to the Home page by clicking **Home** in the navigation bar.

Navigating the vSphere Client

Slide 4-32



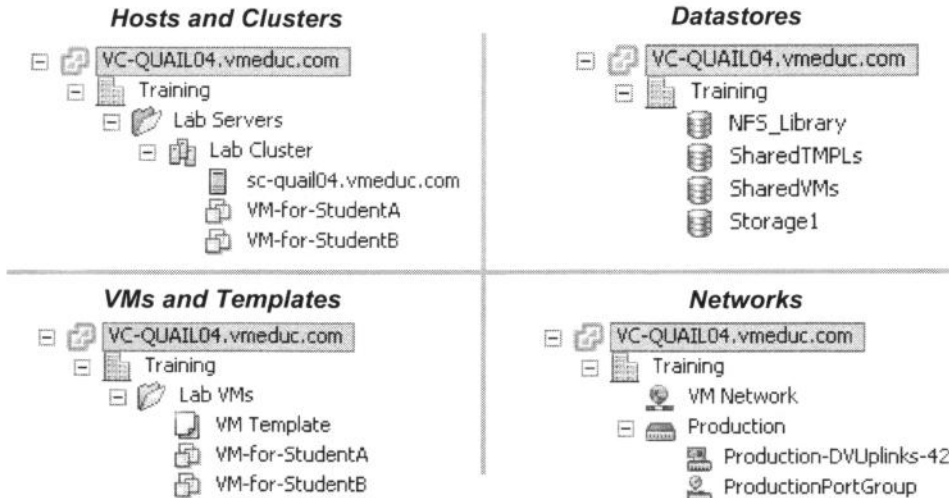
The navigation bar displays the hierarchical navigational path to the current vSphere Client view. For example, when you display the Host and Clusters Inventory view, the navigation bar displays **Home > Inventory > Hosts and Clusters**. You can click any item in the navigation bar to display a menu of all the options available at that level of the hierarchy.

The vSphere Client also has a search field, which is available in all its views. By default, the vSphere Client searches every kind of inventory object, but you can click the icon to limit your search. When you perform a simple search by entering search terms in the search field, the results appear in a results pane displayed directly beneath the search field.

vCenter Inventory Objects

Slide 4-33

The vCenter Server inventory panels organize objects into a hierarchy.



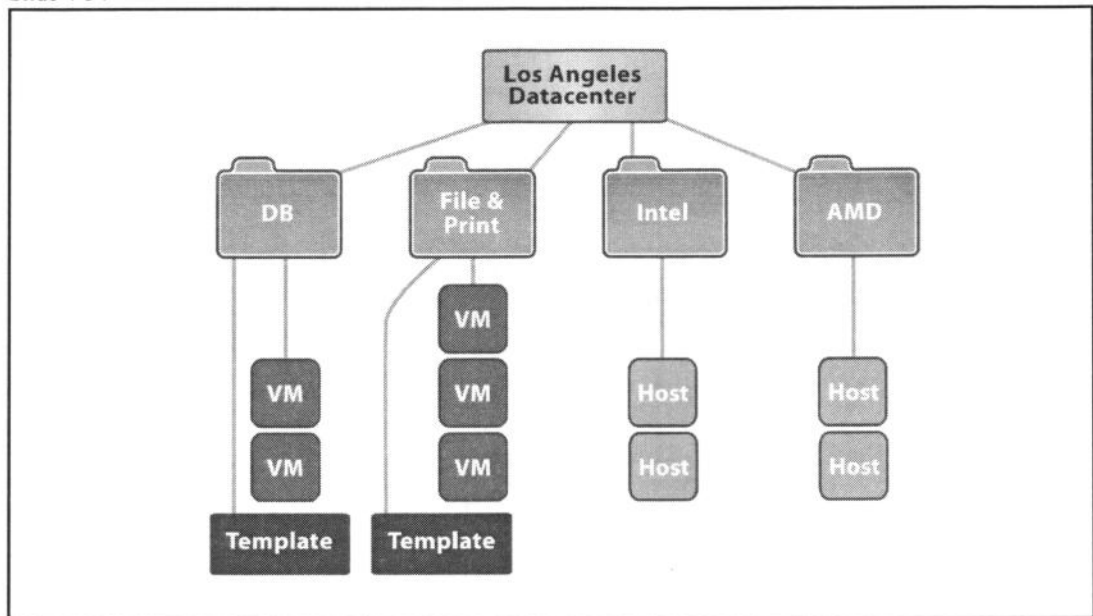
The vCenter Server inventory is a hierarchy of objects. These objects are either containers of other objects, such as folders, or objects that you manage. Objects can be hosts, virtual machines, templates, clusters, resource pools, datastores, or networks. The inventory hierarchy is used to group your objects in a meaningful way. It also provides a natural structure on which to apply permissions.

The topmost object in the vCenter Server inventory is vCenter Server, also known as the root folder. You can change the name of the root folder, but you cannot add or remove it.

Under the root folder, one or more datacenter objects are created. A datacenter is the primary container of inventory objects. From the datacenter you can add and organize inventory objects, such as your hosts, virtual machines, datastores, and networks.

Organizing Inventory Objects into Folders

Slide 4-34



Items within the datacenter can be placed into folders. Folders and subfolders can be created to better organize systems.

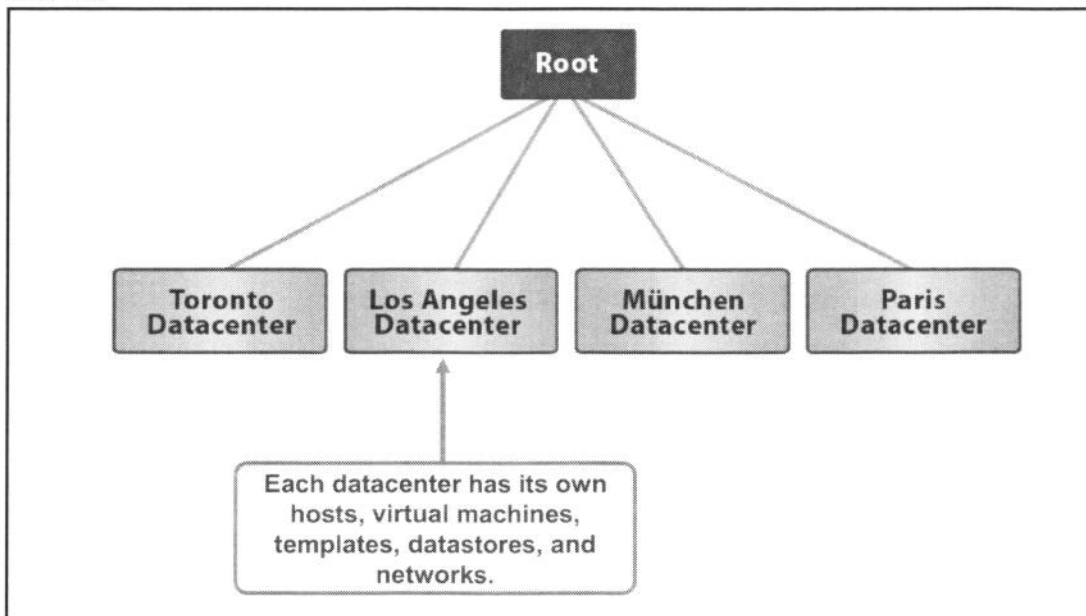
In the example above, virtual machines and templates are placed into folders based on function. Hosts are placed into folders based on CPU family.

An advantage of organizing objects into folders is that you can create a structure on which appropriate access can be assigned to administrators.

Design your inventory with care. Too many sublevels and too complicated a hierarchy can make management harder instead of easier.

Managing Multiple Datacenters

Slide 4-35



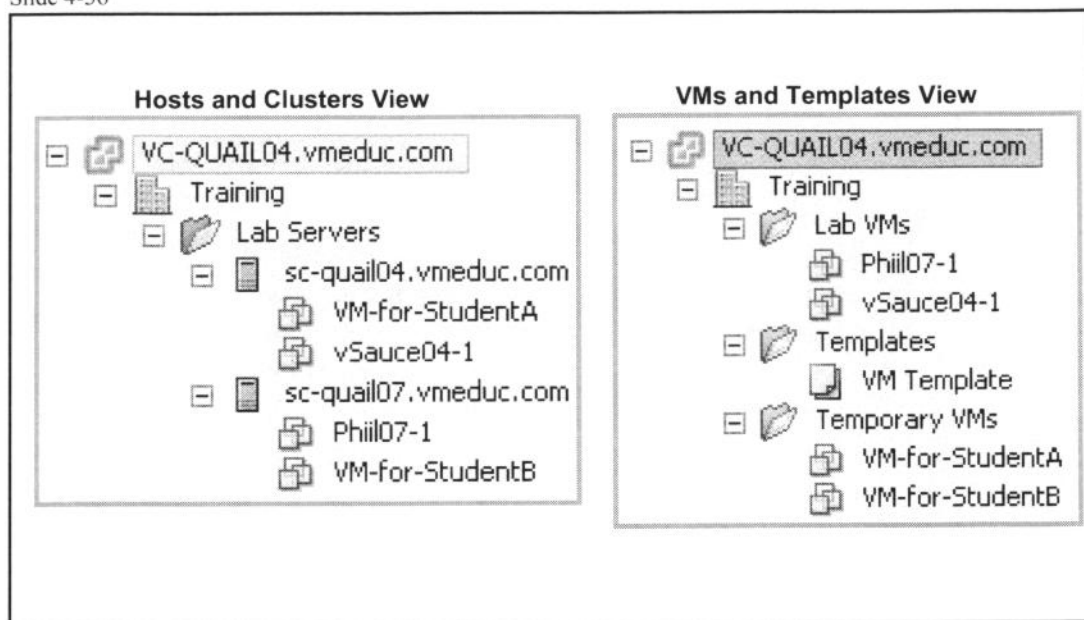
vCenter Server can be used to manage multiple datacenters. Large companies might use multiple datacenters to represent organizations or business units within the company.

Inventory objects can interact *within* datacenters, but have only limited interaction *across* datacenters. For example, you can migrate a virtual machine with VMotion from one host to another within a datacenter, but not to a host in a different datacenter. On the other hand, you can clone a virtual machine within a datacenter and to a different datacenter.

In the example above, datacenters are based on their geographical location, where each geographical location might have its own team of IT administrators, its own set of customers, and its own set of ESX/ESXi hosts, virtual machines, networks, and datastores for which it is responsible.

vCenter Views: Hosts, Clusters, VMs, Templates

Slide 4-36



The Hosts and Clusters view and the VMs and Templates view are two of the inventory views available in vCenter Server.

The Hosts and Clusters view displays all host and cluster objects in a datacenter. The VMs and Templates view displays all virtual machine and template objects in a datacenter.

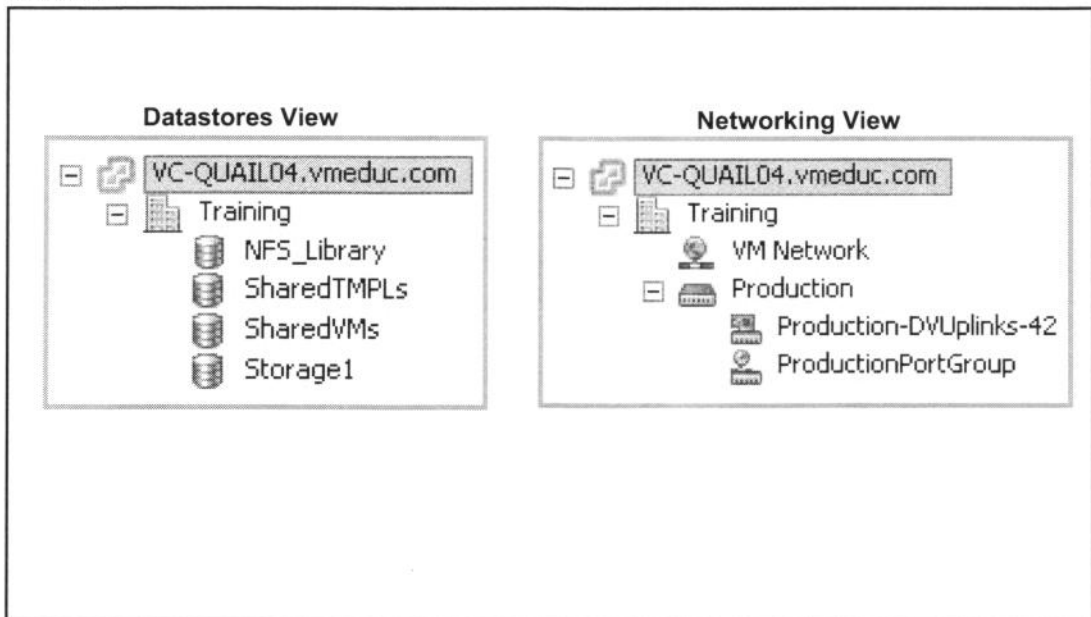
Each view maintains its own set of folders in the datacenter. In the example above, notice that the Intel folder under the datacenter in the Hosts and Clusters view does not appear in the VMs and Templates view. Likewise, the Database Servers folder under the datacenter in the VMs and Templates view does not appear in the Hosts and Clusters view.

You cannot see templates in the Hosts and Clusters view. It is possible to see templates in this view by selecting the Hosts & Clusters folder and clicking the **Virtual Machines** tab.

Also note that you cannot see hosts or clusters in the VMs and Templates view. It is possible to see hosts in this view by selecting the Virtual Machines & Templates folder and clicking the **Hosts** tab.

vCenter Views: Datastores and Networks

Slide 4-37



The Datastores view and the Networking view are also available in vCenter Server.

The Datastores view displays all the datastores in the datacenter. The Networking view displays all virtual machine port groups and distributed virtual switches.

As with the other inventory views, you can organize your datastore and network objects into folders.

Adding Host to vCenter Server Inventory

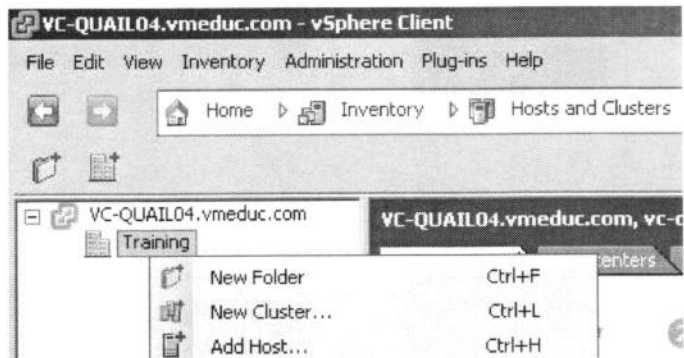
Slide 4-38

To add an ESX/ESXi host to the vCenter Server inventory, use the Add Host wizard. Specify:

- > Fully qualified domain name
- > User name and password
- > (ESXi hosts only) Lockdown mode enabled

You can also add legacy hosts:

- > ESX 2.5.x or later
- > ESXi 3.5 and later



To add a host to the vCenter inventory, you must be in the Hosts and Clusters view. You can add a host to the datacenter, or to a folder or cluster within the datacenter. In the example above, a host is being added to a folder in the datacenter. Right-click the folder, then choose **Add Host**. The Add Host wizard appears.

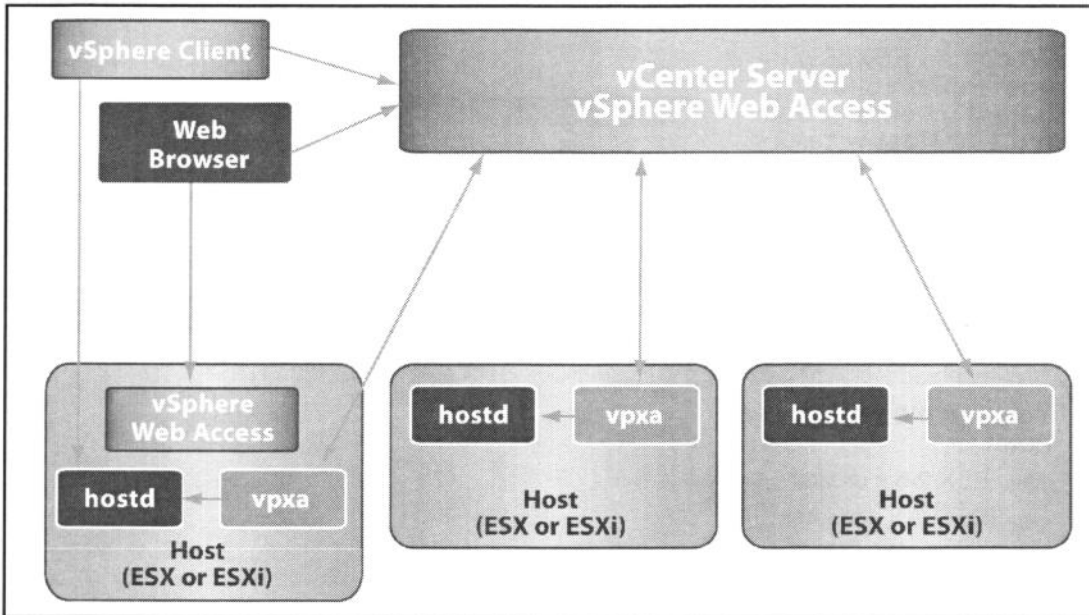
The Add Host wizard asks you for the host name. Enter either the short name or the fully qualified domain name. The wizard then asks you for the user name and password. Use the root user account and its password. vCenter Server uses the root account to log in to the system and then creates a special user account named vpxuser. vCenter Server uses the vpxuser account for all future authentication.

For ESXi hosts only, an additional page allows you to enable lockdown mode. Lockdown mode disables remote access for the administrator account after vCenter Server takes control of the host. It ensures that the host is managed only through vCenter Server.

You can also add certain older versions of ESX and ESXi hosts to the vCenter Server inventory. For the list of ESX and ESXi versions compatible with vCenter Server, see the vSphere installation guide at <http://www.vmware.com/support/pubs>.

ESX/ESXi and vCenter Communication

Slide 4-39



vCenter Server and ESX/ESXi hosts can be accessed using either the vSphere Client or a Web browser.

When using the vSphere Client, vCenter Server passes commands to the ESX/ESXi host via the `vpxa` process. If you are using the vSphere Client to communicate directly with an ESX host, the `vpxa` process is not used. Instead, communications go directly to the `vmware-hostd` process, often referred to as the host agent, or `hostd` for short.

When using a Web browser (either Internet Explorer or Mozilla Firefox), you connect to vSphere Web Access, a service that is available on both vCenter Server and ESX (but not ESXi).

vCenter License Overview

Slide 4-40

Licenses are managed and monitored from vCenter Server.

Licensing consists of the following components:

- > Product – A license to use a vSphere software component or feature
- > License key – A 25-character serial number that corresponds to a product
- > Asset – A machine on which a product is installed

vCenter Server can also manage licenses for legacy hosts.

- > vCenter Server must have a VMware License Server connection.
- > When adding a legacy host to the vCenter Server inventory, vCenter Server checks out vCenter Server agent licenses from the License Server.

In the vSphere environment, license reporting and management are centralized. All product and feature licenses are encapsulated in 25-character license keys that you can manage and monitor from vCenter Server.

License information can be viewed by product, license key, or asset:

- Product – A license to use a vSphere software component or feature. Examples of products are ESX Enterprise, vCenter Enterprise, and VMotion.
- License key – The serial number that corresponds to a product.
- Asset – A machine on which a product is installed. For an asset to run certain software legally, the asset must be licensed to do so.

You can split some license keys by applying them to multiple assets. For example, you can split a four-CPU license by applying it to two 2-CPU hosts.

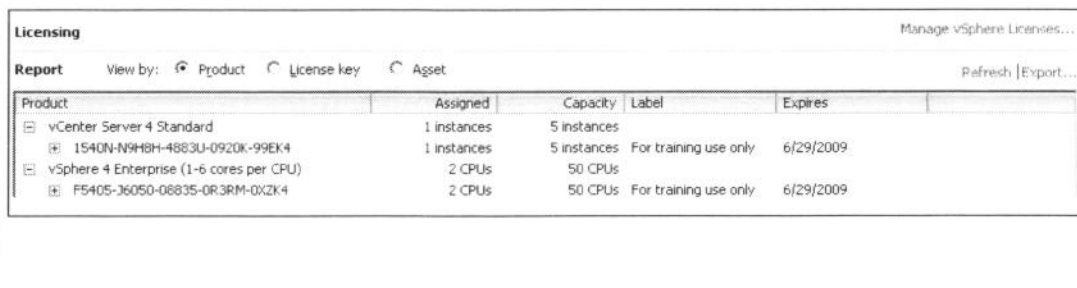
vCenter Server can also manage licenses for legacy hosts. To do this, you must download the VMware License Server at the VMware Web site and install the VMware License Server on the vCenter Server system. When you add an ESX 3.x/ESXi 3.5 host to the vCenter Server 4.0 inventory, vCenter Server checks out vCenter Server agent licenses from the License Server.

For detailed information about VMware licensing, go to the license portal at <http://www.vmware.com/support/licensing.html>.

Adding License Keys

Slide 4-41

1. In the navigation bar, go to Home > Administration > Licensing.
2. Enter license keys for each product.
 - (Optional) Enter a label for each license key.
3. Assign the license key to an asset.



The screenshot shows the 'Licensing' page in vSphere. At the top right is a link 'Manage vSphere Licenses...'. Below it is a 'Report' section with 'View by:' and three radio buttons: 'Product' (selected), 'License key', and 'Asset'. To the right of these buttons are 'Refresh' and 'Export...' links. The main part of the page is a table with the following columns: Product, Assigned, Capacity, Label, and Expires. The table contains two main product entries, each with a sub-entry for a specific license key.

Product	Assigned	Capacity	Label	Expires
[-] vCenter Server 4 Standard	1 instances	5 instances		
[+] 1540N-N9H8H-4883U-0920K-99EK4	1 instances	5 instances	For training use only	6/29/2009
[-] vSphere 4 Enterprise (1-6 cores per CPU)	2 CPUs	50 CPUs		
[+] F5405-36050-08835-0R3RM-0XZK4	2 CPUs	50 CPUs	For training use only	6/29/2009

After you purchase a vSphere asset and use the license portal to obtain your license key, you can add the license to the vCenter Server license inventory management system. You can add multiple license keys or add one license key at a time.

To add license keys, use the vSphere Client navigation bar to go to **Home > Administration > Licensing**. On the Licensing page, click the **Manage vSphere Licenses** link. In the dialog box, you can add license keys, assign licenses to assets, and remove license keys that are currently unassigned to assets.

When adding a license key, you can add an optional description of each key or set of license keys. These labels appear in the license report.

vCenter Server Events

Slide 4-42

event search

VC-QUALI01.vmeduc.com

VC-QUALI01 VMware vCenter Server, 4.0.0, 162856

Getting Started Datacenters Virtual Machines Hosts Tasks & Events Alarms Permissions Maps

View: Tasks Events

Description, Type or Target contains: Clear

Description	Type	Date Time	Task	Target
Failed to import machine to sc-quali01.vmeduc.com in Training	error	4/29/2009 3:22:53 PM		
vCenter Converter logs are on myhotclone at "C:\Documents and Settings\All Users\Application Data\VMware\VMware Converter Enterprise\Logs\vmware-converter-agent"	info	4/29/2009 3:22:53 PM		
Configuring parameters for the target virtual machine	info	4/29/2009 3:22:50 PM		

details of selected event

Event Details

Type: **error** User: VMEDUC\quali01a Time: 4/29/2009 3:22:53 PM

Description: 4/29/2009 3:22:53 PM, Failed to import machine to sc-quali01.vmeduc.com in Training

Related Events:

- 4/29/2009 3:22:53 PM, vCenter Converter logs are on myhotclone at "C:\Documents and Settings\All Users\Application Data\VMware\VMware Converter Enterprise\Logs\vmware-converter-agent"
- 4/29/2009 3:22:50 PM, Configuring parameters for the target virtual machine

A vCenter Server event is the outcome or result of running a vCenter Server task.

To display events, go to any inventory view and click any object. A **Tasks & Events** tab exists for any object and allows you to view the tasks and events related to that object.

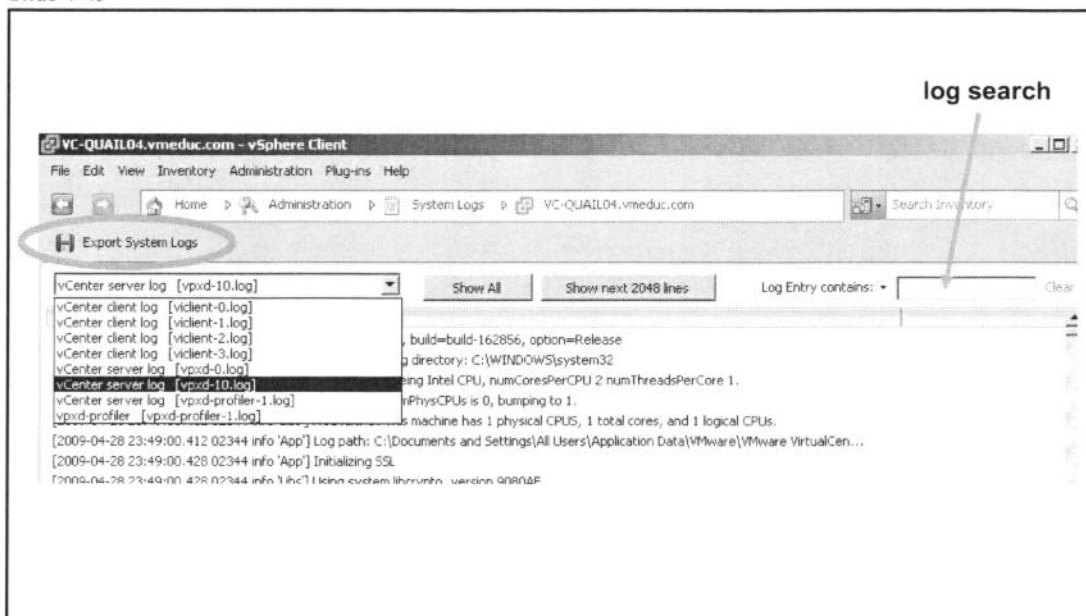
You can also view events for the entire vCenter Server by going to the menu bar and choosing **View > Management > Events**.

You can search for a particular event—for example, by description, type, or target—using the event search box.

Being able to view vCenter Server events can be very useful when troubleshooting problems.

vCenter Server System Logs

Slide 4-43



Like events, vCenter Server system logs can also be very useful, in particular to VMware Support, for troubleshooting problems.

To view the list of system logs, go to **Home > Administration > System Logs**.

Logs can be searched in the same way as events.

In the system log list, you see all the logs that are currently available for viewing. You can view vCenter client logs and vCenter server logs. Like ESX host logs, you can export vCenter Server's system logs to a compressed, archive file. This is useful when you are working with VMware technical support to troubleshoot your vCenter Server problems.

Creating a vCenter Server Administrator

Slide 4-44

Avoid using the Windows Administrator user to run vCenter Server after it has been installed.

- By default, the Windows local Administrators group is given the vCenter Server role named Administrator.

Instead, use a nonadministrative Windows account to run vCenter Server.

VC-QUAIL04.vmeduc.com

Rawlinson (user) and vSphereGurus (group) are assigned vCenter Server Administrator role.

Remove the Administrators group from the list.

VC-QUAIL04.vmeduc.com, vc-quail04 VMware

Getting Started | Datacenters | Virtual Machines

User/Group	Role	Defined in
Rawlinson	Administrator	This object
Administrators	Administrator	This object
vSphereGurus	Administrator	This object

The Administrator role is the most powerful role in vCenter Server. It allows the user to perform every available action in vCenter Server. You should grant this role to as few users as possible.

To limit the scope of access, it is a best practice to avoid using the Windows Administrator user account to run vCenter Server after you install it. Instead, assign the vCenter Administrator role to a normal, nonadministrative Windows user or group account.

In the example above, a Windows user named Rawlinson and a Windows group named vSphereGurus are assigned the vCenter Server Administrator role. You can then delete the vCenter Server role assigned to the Windows Administrators group or change the role to, for example, Read-only.

Lab 3

Slide 4-45

In this lab, you will use the vCenter Server inventory, add a license key, and view system logs.

1. Add container objects to the Hosts and Clusters inventory view.
2. Add your ESX host to the Hosts and Clusters inventory view and display general host information.
3. Add folder objects to the VMs and Templates inventory view.
4. Assign a normal user to be the vCenter Server administrator.
5. Add vCenter Server and ESX host license keys.

Lesson Summary

Slide 4-46

- > The vSphere Client Home page allows you to view the inventory, as well as perform various management and administrative tasks.
- > The vCenter Server **Inventory** panel organizes vCenter Server objects – such as hosts, virtual machines, datastores, and networks – into a hierarchy.
- > vCenter system logs and events are viewed using the vSphere Client.

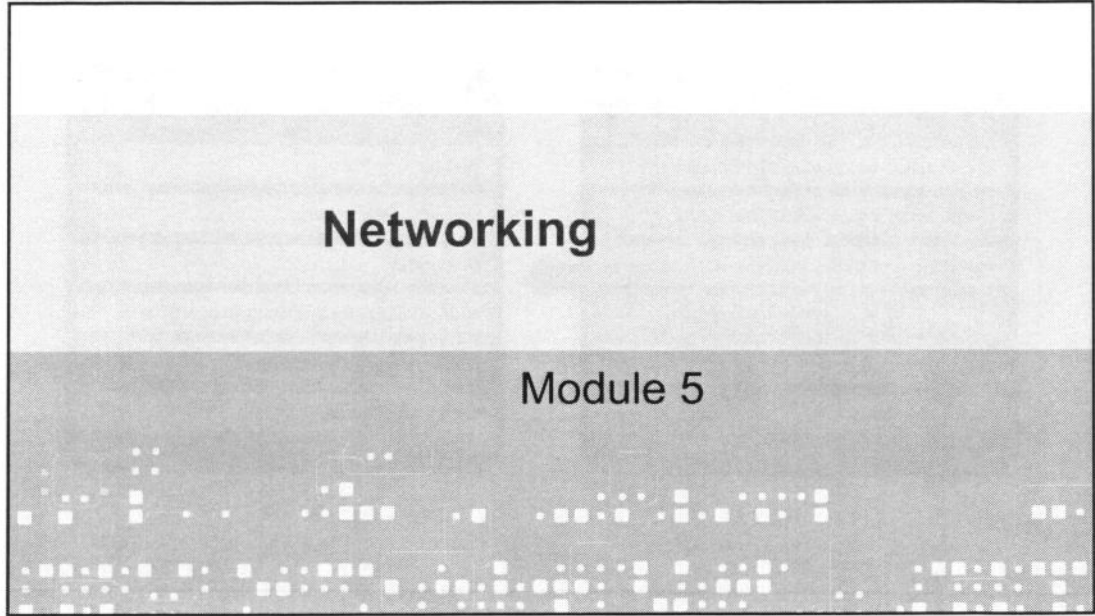
Key Points

Slide 4-47

- > Use vCenter Server to centrally manage your hosts and virtual machines instead of logging directly in to each host.
- > Use the inventory views to organize inventory objects in a meaningful way.
- > Assign the vCenter Server Administrator role to a normal Windows user account and remove this role from the Windows Administrator group.

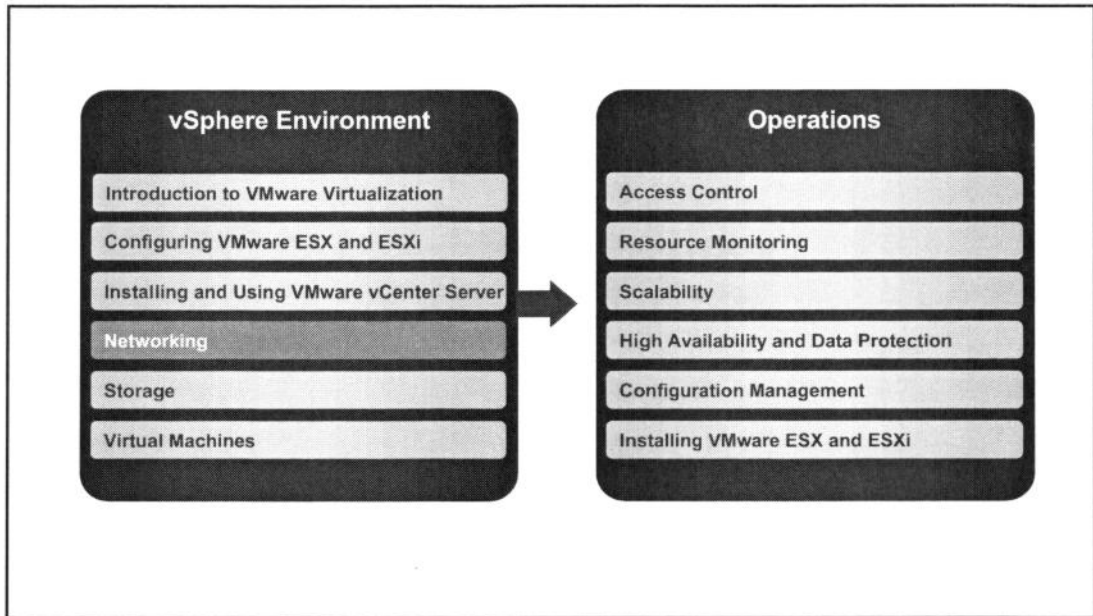
Networking

Slide 5-1



You Are Here

Slide 5-2



Importance

Slide 5-3

- VMware ESX™/ESXi networking features allow virtual machines to communicate with other virtual and physical machines, allow management of the ESX/ESXi host, and allow the VMkernel to access IP-based storage and perform VMotion™ migrations. Failure to properly configure ESX/ESXi networking can negatively affect virtual machine, management, and storage operation.

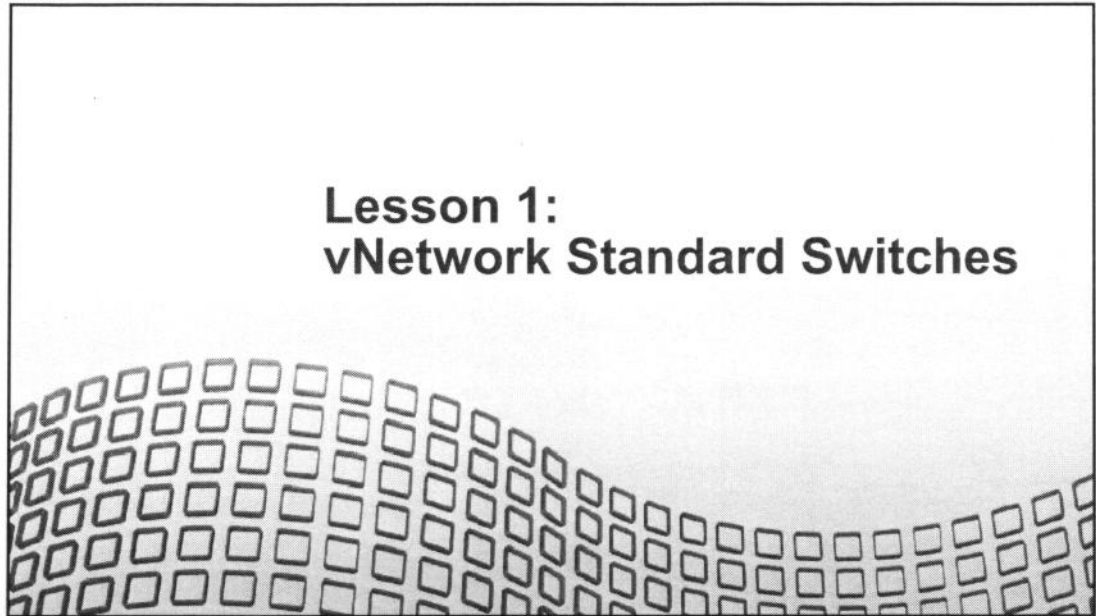
Module Lessons

Slide 5-4

- Lesson 1: vNetwork Standard Switches**
- Lesson 2: vNetwork Distributed Switches**
- Lesson 3: Modifying Virtual Switch Properties**

Lesson 1: vNetwork Standard Switches

Slide 5-5



Lesson Objectives

Slide 5-6

- > Describe the components of a vNetwork standard switch
- > Describe the vNetwork connection types
- > View the vNetwork standard switch configuration

What Is vNetwork?

Slide 5-7

vNetwork capabilities optimally align physical and virtual machine networking, and provide the networking for hosts and virtual machines.

vNetwork supports two types of virtual switches:

- > vNetwork standard switches
 - Virtual switch configuration for a single host
- > vNetwork distributed switches
 - Virtual switches that provide a consistent network configuration for virtual machines as they migrate across multiple hosts

vNetwork provides several different services to the host and virtual machines. You can enable three types of network services in VMware® ESX™/ESXi:

- Connecting virtual machines to the physical network.
- Connecting VMkernel services (such as NFS, iSCSI, or VMware VMotion™) to the physical network.
- Networking for the service console, which runs management services for ESX, is set up by default during installation.

A service console port is required for ESX to connect to any network or remote services, including the VMware vSphere™ Client.

vNetwork supports two kinds of virtual switches:

- vNetwork standard switch – A virtual switch configuration at the host level.
- vNetwork distributed switch – Components are similar to a standard switch, but it functions as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across multiple hosts. This switch is configured at the VMware vCenter™ Server level.

vNetwork Standard Switch

Slide 5-8

A vNetwork standard switch (vSwitch)

- > Directs network traffic between virtual machines and links to external networks
- > Combines the bandwidth of multiple network adapters and balances traffic among them. It can also handle physical NIC failover.
- > Models a physical Ethernet switch
 - Default number of logical ports is 56 (4,088 maximum).
 - A virtual machine's NIC can connect to a port.
 - Each uplink adapter uses one port.

A virtual switch is a software construct, implemented in the VMkernel, that provides networking connectivity for an ESX/ESXi host.

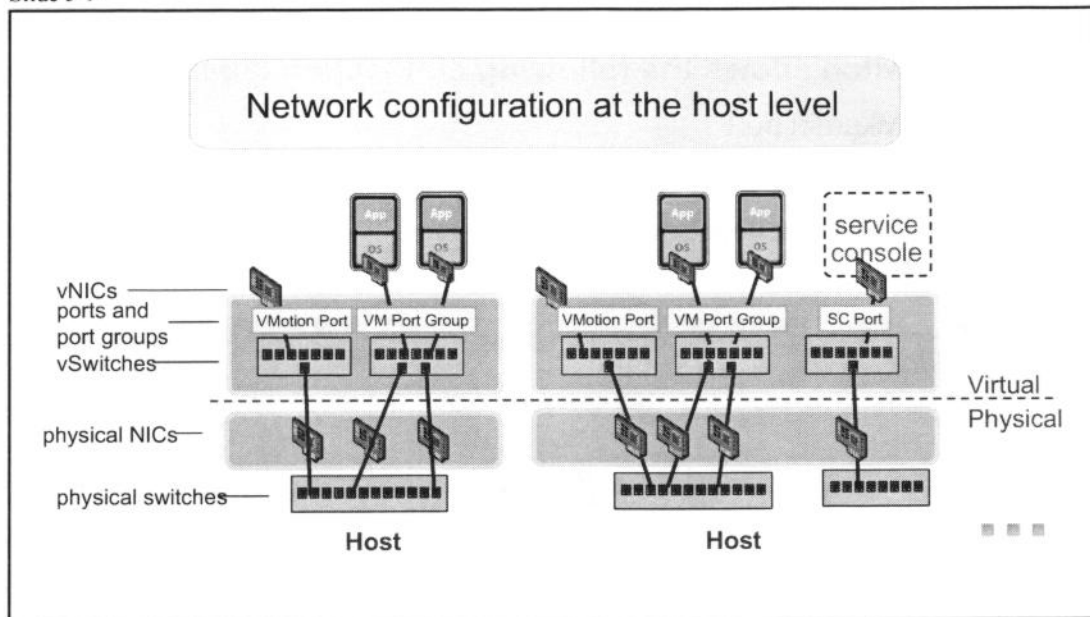
All network communication, whether it is internal or external to the ESX/ESXi host, must be defined through a virtual switch. A virtual switch provides connections for virtual machines to communicate with one another, whether they are on the same host or on a different host. The VMkernel connects to a virtual switch in order to access IP storage. The service console connects to a virtual switch for remote management of the ESX host.

Use vSwitches to combine the bandwidth of multiple network adapters and balance communications traffic among them. They can also be configured to handle physical NIC failover.

When two or more virtual machines are connected to the same vSwitch, network traffic between them is routed locally. If an uplink adapter is attached to the vSwitch, each virtual machine can access the external network that the adapter is connected to.

vNetwork Standard Switch Components

Slide 5-9



vNetwork standard switch components are configured at the host level. Each virtual machine and the service console has one or more of its own virtual network adapters, or vNICs. The operating system and applications talk to a vNIC through a standard device driver or a VMware-optimized device driver. The VMkernel also has vNICs for VMotion and IP storage network requirements.

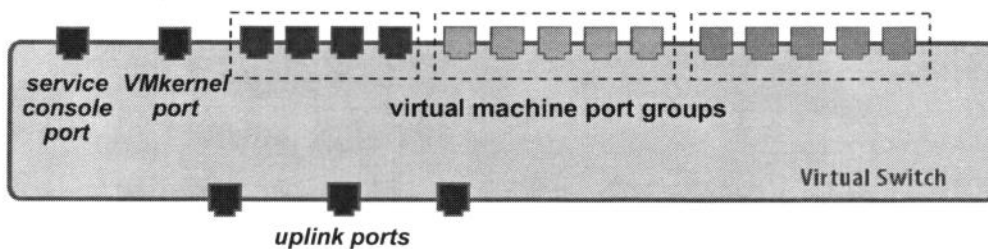
Each ESX/ESXi host has one or more virtual switches. You can create a maximum of 127 vSwitches on a single host. On one side of the virtual switch are port groups that connect to virtual machines. Each logical port on the vSwitch is a member of a single port group. The default number of logical ports for a vSwitch is 56. However, a vSwitch can be created with up to 4,088 ports in ESX/ESXi. On the other side are uplink connections to physical Ethernet adapters on the server where the virtual switch resides.

vSwitch Ports

Slide 5-10

A vSwitch allows the following connection types:

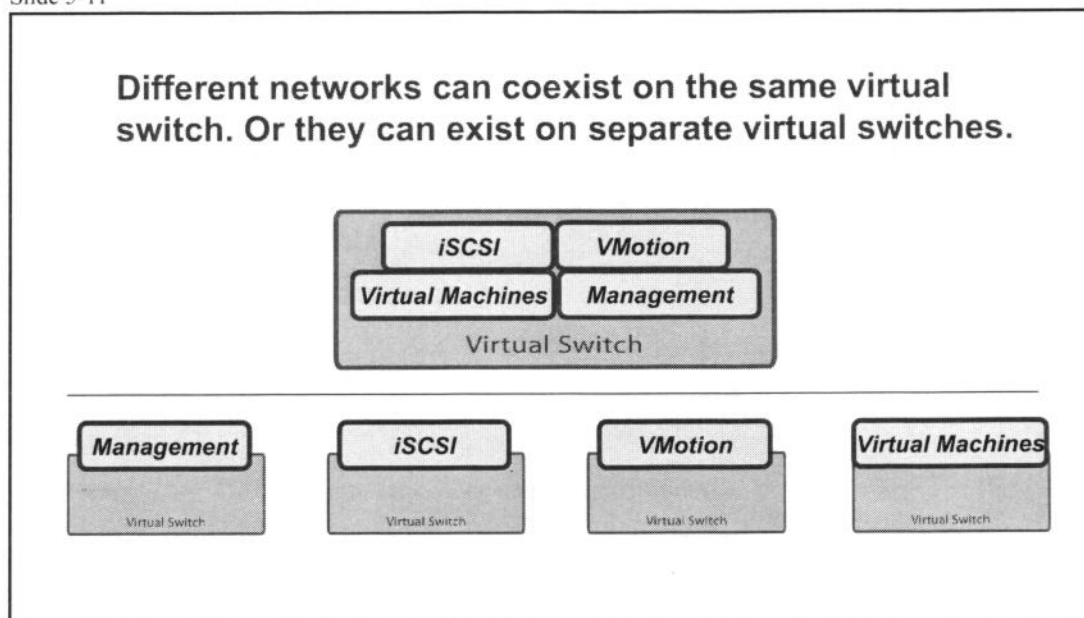
- > VMkernel port
- > Service console port (ESX only)
- > Virtual machine port group



Before using a virtual switch, one or more connections must be defined. The graphic above shows a single virtual switch with all three connection types defined. Virtual machines, the service console, and VMkernel components connect to the outside world through the physical Ethernet adapters that are connected to the virtual switch uplink ports.

vSwitch Examples

Slide 5-11

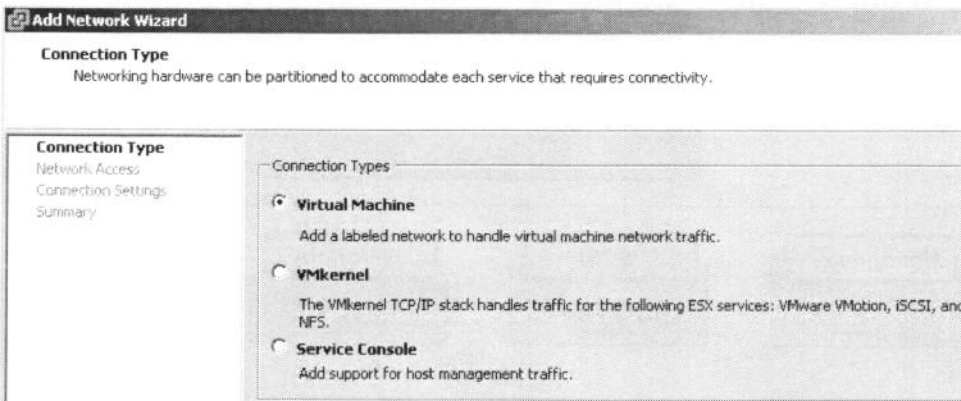


When designing your networking environment, you must determine whether to place all your networks on a single virtual switch or opt for multiple virtual switches, each with a separate network. The decision partly depends on the layout of your physical networks. For example, you might not have enough network adapters to create a separate virtual switch for each network. Instead, you might team your network adapters in a single virtual switch and create isolate the networks using VLANs. A key point to remember is that physical NICs are assigned at the virtual switch level, so all ports and port groups defined for a particular switch share the same hardware (although which NICs are active can be configured differently for each port group).

Adding a Network: Connection Type

Slide 5-12

1. In the **Configuration** tab, click **Add Networking**.
2. In the Add Network wizard, choose desired connection type: **Virtual Machine**, **VMkernel**, or **Service Console**.



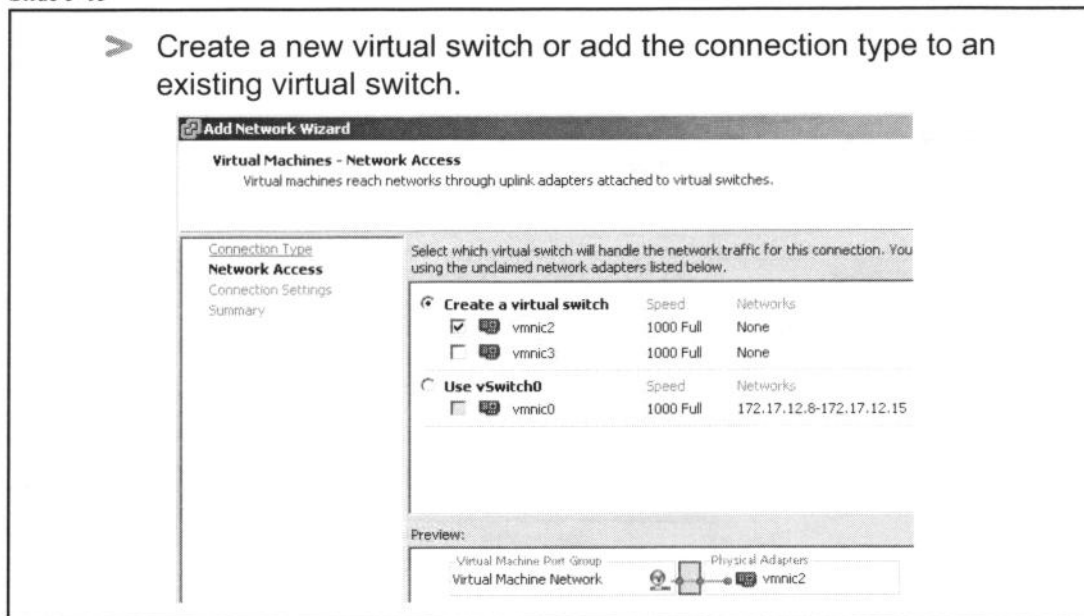
To create a standard switch or add a port group to an existing virtual switch, use the Add Network wizard. To launch the wizard, select your host in the inventory, then click the **Configuration** tab. Select **Networking** in the **Hardware** section, then click the **Add Networking** link. The Add Network wizard appears, as shown above.

The first step is to choose the type of connection to create: virtual machine, VMkernel, or service console (ESX hosts only). This is shown above.

Adding a Network: Network Adapters

Slide 5-13

- Create a new virtual switch or add the connection type to an existing virtual switch.



Continuing in the Add Network wizard, the next step is to either create a new virtual switch or use an existing virtual switch for the connection type.

If you create a new virtual switch, you select one or more physical network adapters to be used by that switch. If you select more than one adapter for the switch, you are creating a NIC team, which is useful for load balancing and NIC failover.

It is also possible to select zero network adapters for the virtual switch. In this case, this is known as an internal virtual switch. Virtual machines connected to this switch can communicate with each other but not with external networks.

Adding a Network: Connection Settings

Slide 5-14

- > Name the connection and optionally define a VLAN ID (1–4,094) if using VLANs.

Add Network Wizard

Virtual Machines - Connection Settings
Use network labels to identify migration compatible connections common to two or more hosts.

Connection Type
Network Access
Connection Settings
Summary

Port Group Properties

Network Label:

VLAN ID (Optional):

Preview:

Virtual Machine Port Group: Production

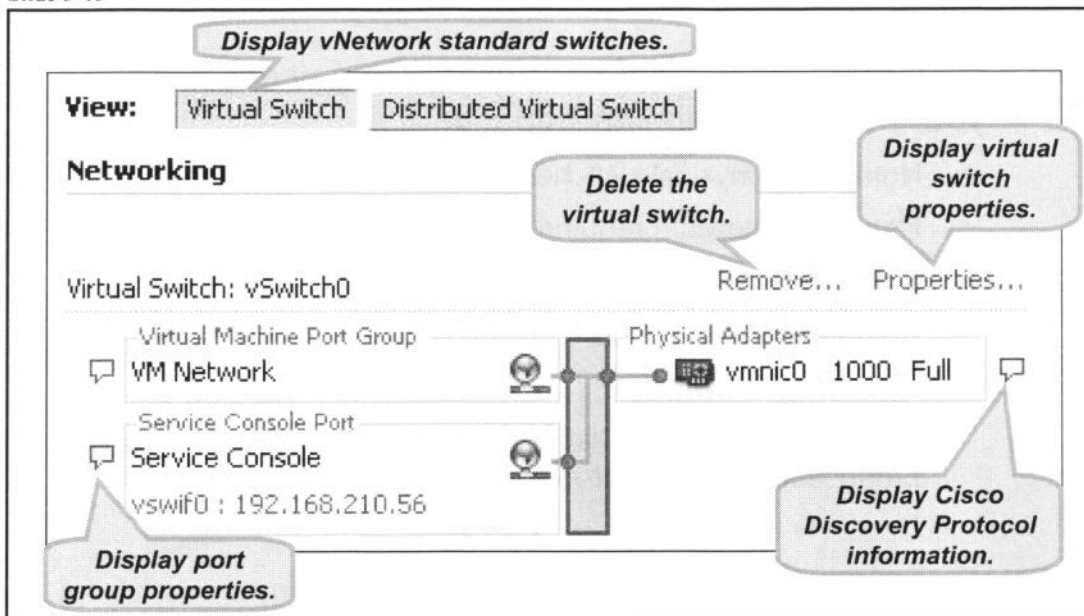
Physical Adapters: vmnic2

Continuing in the Add Network wizard, the next step is to define the name of the network, or network label. Provide a descriptive name; for example, one that describes the network's function. In the example above, the network label is Production, to which production virtual machines will be attached.

Optionally, you can specify a VLAN ID. VLANs are discussed later in this module.

vSwitch Configuration

Slide 5-15



You can view a host's virtual switch configuration by clicking the **Networking** link of a host's **Configuration** tab.

In the example above, the Virtual Switch view is displayed. The virtual switch, vSwitch0, is created during the ESX/ESXi installation. Also created during installation is a virtual machine port group named VM Network and a service console port named Service Console. It is a good practice to remove the VM Network virtual machine port group and keep virtual machine networks and management networks separated for performance and security reasons.

To remove a virtual switch, click the **Remove** link next to the virtual switch to be deleted. To display virtual switch properties, click the **Properties** link next to the virtual switch.

The "callout" icon next to a port or port group lists the port group properties. The callout icon next to a physical adapter lists Cisco Discovery Protocol (CDP) information, if applicable.

Cisco Discovery Protocol (CDP) allows ESX/ESXi administrators to determine which Cisco switch port is connected to a given vSwitch. When CDP is enabled for a particular vSwitch, you can view properties of the Cisco switch (such as device ID, software version, and timeout) from the vSphere Client.

For vNetwork standard switches, use the ESX service console command-line interface to enable CDP. For details, see the *ESX Configuration Guide* at <http://www.vmware.com/support/pubs>. For vNetwork distributed switches, use the vSphere Client to enable CDP. This is covered later in the module.

Physical Network Considerations

Slide 5-16

Discuss VMware vSphere™ networking needs with your network administration team:

- > Number of physical switches
- > Network bandwidth required
- > Physical switch support for 802.3AD (for NIC teaming)
- > Physical switch support for 802.1Q (for VLAN trunking)
- > Network port security
- > Cisco Data Protocol (CDP) and its operational modes: listen, broadcast, listen and broadcast, and disabled.

Because your virtual networking environment ultimately relies on the physical network infrastructure, you should discuss your vSphere networking needs with your network administration team.

How you design your virtual networks depends on many factors, including how much physical network equipment is available to you, how much network bandwidth is required for your applications, and whether you will use networking features like NIC teaming and VLANs. Network port security is also a consideration.

Lesson Summary

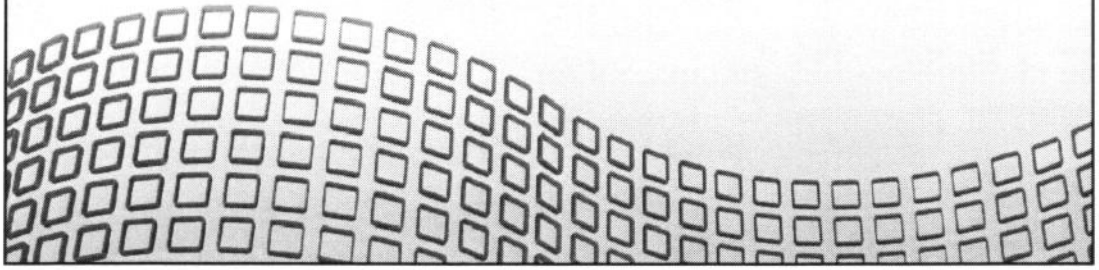
Slide 5-17

- > A vNetwork consists of two types of switches: standard switches and distributed switches.
- > A standard switch allows virtual machine networking and is configured at each host.
- > There are three connection types: virtual machine, VMkernel, and service console.

Lesson 2: vNetwork Distributed Switches

Slide 5-18

Lesson 2: vNetwork Distributed Switches



Lesson Objectives

Slide 5-19

- > List the benefits of using vNetwork distributed switches
- > Describe the vNetwork distributed switch architecture
- > Create a vNetwork distributed switch
- > Manage the vNetwork distributed switch using the VMware vSphere Client

vNetwork Distributed Switch

Slide 5-20

A vNetwork distributed switch provides similar functionality to a vNetwork standard switch, but it exists across the entire datacenter to use.

- VMware vCenter™ Server owns the configuration of the distributed switch, and the configuration will be consistent across all the hosts that use it.

The behavior of distributed switches is consistent with standard switches.

- You can configure virtual machine port groups, VMkernel ports, and service console ports on a distributed switch.

A vNetwork distributed switch provides similar functionality to a vNetwork standard switch, but its configuration is centralized to vCenter Server.

The distributed switch implements capabilities similar to those of standard switches. There are port groups that virtual machines connect to. Virtual machines, service console, and VMkernel interfaces can be connected to port groups.

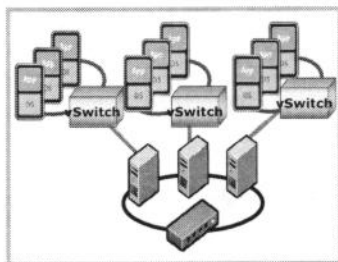
There is some configuration that is specific to the host, however. A host's uplinks are allocated to the distributed switch and are managed at each host, not through vCenter Server. Similarly, the configuration of the VMkernel and service console port groups is also specific to each host, and therefore defined on each host instead of on the distributed switch as in vCenter Server.

Benefits of Distributed Switches

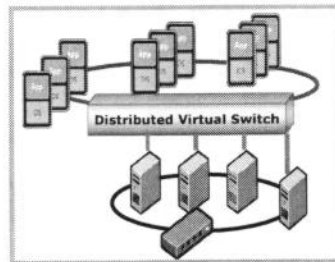
Slide 5-21

The benefits of distributed switches over standard switches:

- Simplify datacenter administration
- Provide support for private VLANs
- Enable networking statistics and policies to migrate with virtual machines during a migration using VMware VMotion™
- Provide for customization and third-party development



standard switches



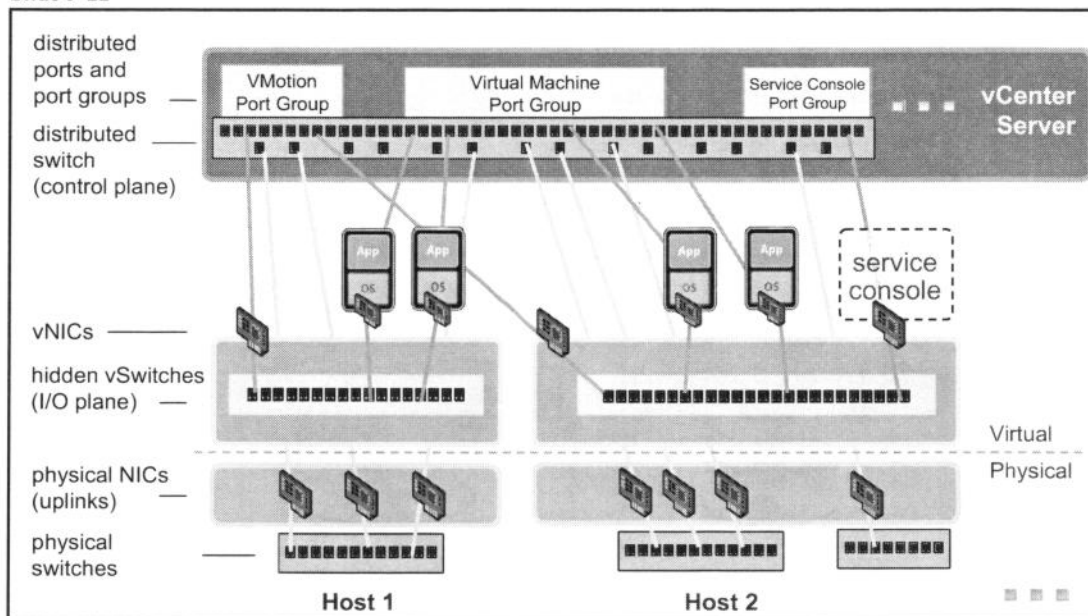
distributed switches

Having the network configuration at the datacenter level (distributed switches) instead of at the host level (standard switches) offers several advantages:

- Datacenter setup and administration are simplified by centralizing network configuration. For example, adding a new host to a cluster and making it VMotion compatible is much easier.
- Distributed switches support private VLANs. Private VLANs allow you to use VLAN IDs within a private network without having to worry about duplicating VLAN IDs across a wider network.
- Distributed ports migrate with their clients. So for example, when you migrate a virtual machine with VMotion, the distributed port statistics and policies move with the virtual machine, thus simplifying debugging and troubleshooting.
- Enterprise networking vendors can provide proprietary networking interfaces to monitor, control, and manage virtual networks. The vNetwork Appliance API allows third-party developers to create distributed switch solutions.

vNetwork Distributed Switch Architecture

Slide 5-22



The vNetwork distributed switch components move network management to the datacenter level.

A distributed switch is a managed entity configured inside vCenter Server. It abstracts a set of virtual switches configured on each associated host. vCenter Server owns the configuration of distributed switches, and the configuration is consistent across all hosts.

Each distributed switch included distributed ports. A distributed port represents a port to which we can connect any networking entity, such as a virtual machine, a service console interface, or a VMkernel interface.

vCenter Server stores the state of distributed ports in the vCenter Server database, so networking statistics and policies migrate with virtual machines when moved from host to host. This network VMotion feature is key to implementing state-dependent features like inline intrusion-detection systems, firewalls, and third-party virtual switches.

A distributed port group provides a way to logically group distributed ports to simplify configuration. A distributed port group specifies port configuration options for each member port on a vNetwork distributed switch. Distributed virtual port groups define how a connection is made through a distributed switch to a network. Ports can also exist without port groups.

An uplink is an abstraction to associate the vmnics from multiple hosts to a single distributed switch. An uplink is to a distributed switch what a vmnic is to a standard vSwitch.

The vNetwork distributed switch architecture consists of two planes: the control plane and the I/O plane. The control plane resides in vCenter Server. The control plan is responsible for configuring distributed switches, distributed port groups, distributed ports, uplinks, NIC teaming, and so forth. The control plane also coordinates the migration of the ports and is responsible for the switch configuration. For example, in the case of a conflict in the assignment of a distributed port (say, because a virtual machine and its template are powered on), the control plane is responsible for deciding what to do.

The I/O plane is implemented as a hidden vSwitch inside the VMkernel of each ESX/ESXi host. The I/O plane manages the I/O hardware on the host and is responsible for forwarding packets.

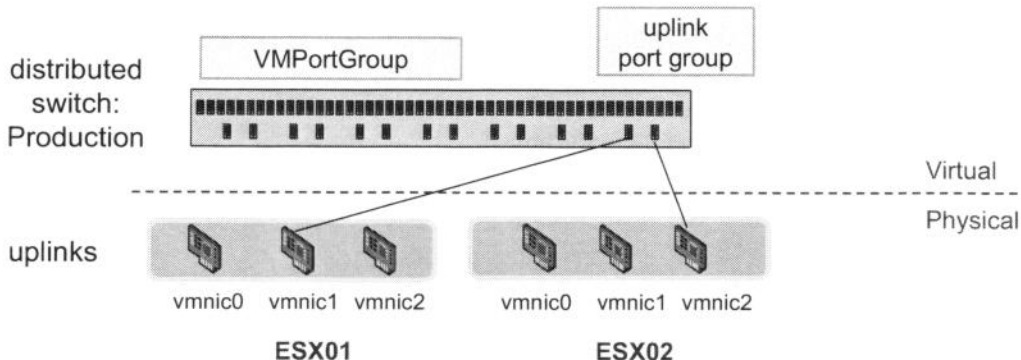
Be careful not to confuse a distributed switch with a single switch spanning across several hosts. Two virtual machines on different hosts can communicate with each other only if both virtual machines have uplinks in the same broadcast domain. Consider a distributed switch as a template for the network configuration on each ESX/ESXi host.

Distributed Switch Example

Slide 5-23

Example:

- > Create a distributed switch named Production, to be used for virtual machine networking. Assign uplinks, vmnic1 on host ESX01 and vmnic2 on host ESX02, to the distributed switch.



In the example above, a distributed switch named Production is created. A port group named VMPortGroup is defined on this switch. vmnic1 on host ESX01 is assigned to the distributed switch as is vmnic2 on ESX02. When the distributed switch is created, an uplink port group is also created to include the uplinks of the hosts.

Creating a Distributed Switch

Slide 5-24

Create vNetwork Distributed Switch

General Properties
Specify the vNetwork distributed switch properties.

General Properties
Add hosts and physical adapters:
Ready to complete

General
Name: Production
Number of dvUplink ports: 4
Maximum number of physical adapters per host

Create vNetwork Distributed Switch

Add hosts and physical adapters
Select hosts and physical adapters to add to the new vNetwork distributed switch.

General Properties
Add hosts and physical adapters
Ready to complete

When do you want to add hosts and their physical adapters to the new vNetwork distributed switch?
☒ Add now
☐ Add later

Host/Physical adapters In use by switch Physical adapter details

☒ sc-quail04.vmeduc.com
Select physical adapters

Physical adapter	In use by switch	Physical adapter details
<input checked="" type="checkbox"/> vmnic1	--	View details...
<input type="checkbox"/> vmnic2	--	View details...
<input type="checkbox"/> vmnic3	--	View details...

☐ sc-quail07.vmeduc.com

Enter name of switch, number of uplink ports, then choose the physical adapters from each host to add to the switch.

To create a distributed switch, go to the Networking inventory view (**Home > Inventory > Networking**). You can create a distributed switch at the datacenter or cluster level. Right-click the datacenter, then choose **New vNetwork Distributed Switch**. The Create vNetwork Distributed Switch wizard appears, as shown above.

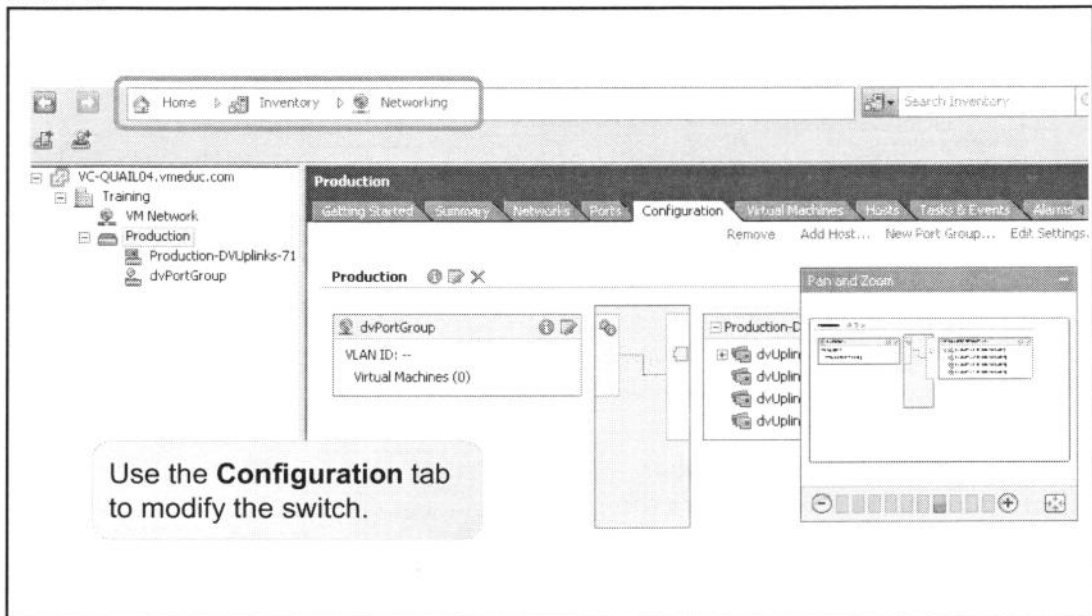
The General Properties page of the wizard prompts you to name the distributed switch and select the maximum number of uplink ports for any host associated with this distributed switch.

On the Add Hosts page of the wizard, select the physical adapters to use for the distributed switch. Adapters are listed by host.

The Ready to Complete page prompts you to confirm the configuration and choose whether to create a default distributed port group. No virtual machine or VLANs are assigned to the port group at this time.

Viewing Distributed Switches

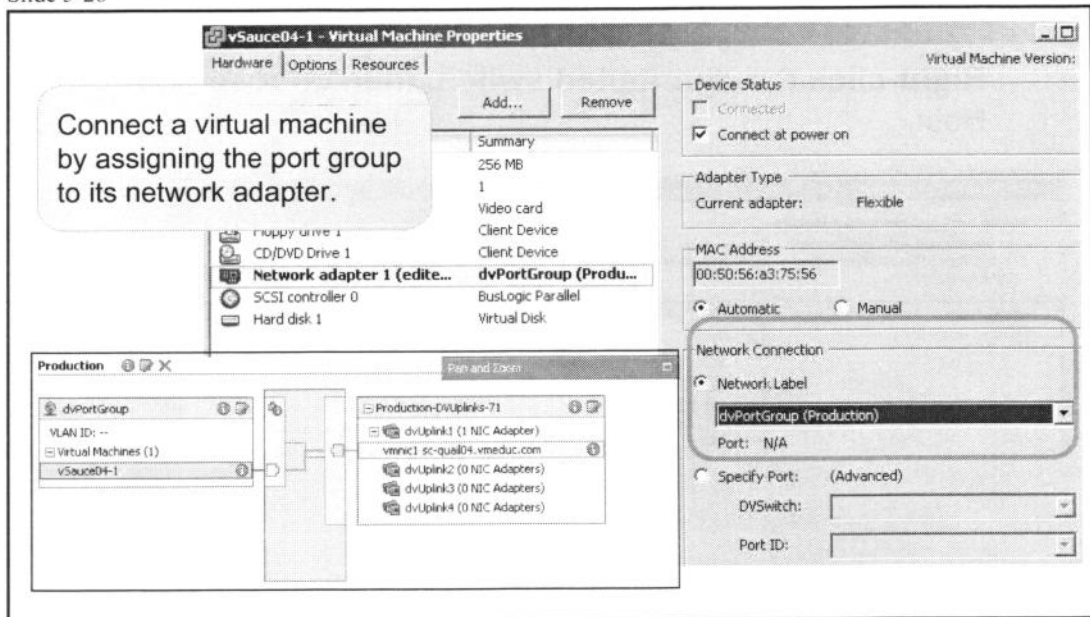
Slide 5-25



To view a distributed switch, select the distributed switch in the inventory, then click the **Configuration** tab. The left pane shows the port groups. In the example above, there is only one port group, dvPortGroup, which has no virtual machines connected to it. The right pane shows the uplink port group. In the example above, the uplink port group is named dvProduction-DVUplinks-425. It consists of two uplinks: vmnic1, which belongs to the host sc-goose07, and vmnic1, which belongs to the host sc-goose06.vmeduc.com.

Connecting a Virtual Machine to a Port Group

Slide 5-26



You connect a virtual machine to a distributed switch by connecting the virtual machine's NIC to a port group on the distributed switch. For an individual virtual machine, this can be done through the virtual machine's properties.

To display a virtual machine's properties, right-click the virtual machine in the Hosts and Clusters (or VMs and Templates) inventory view, then choose **Edit Settings**. The virtual machine properties dialog box appears. Select the desired network adapter in the **Hardware** list. The right pane shows network connection information for the virtual machine. In the **Network Label** list, choose the distributed switch to connect to. You can select by network label or you can specify a port on the distributed switch with the port ID.

Adding a Host to a Distributed Switch







Slide 5-27

Right-click the distributed switch, then choose Add Host.

Add Host to Distributed Virtual Switch

Select host and physical adapters

Select a host and physical adapters to add to this distributed virtual switch. Use Host Profiles to add multiple hosts to the switch simultaneously. Host profiles can be accessed from the Home view. To add additional physical adapters to a host already added to the switch, go to Host > Configuration > Networking.

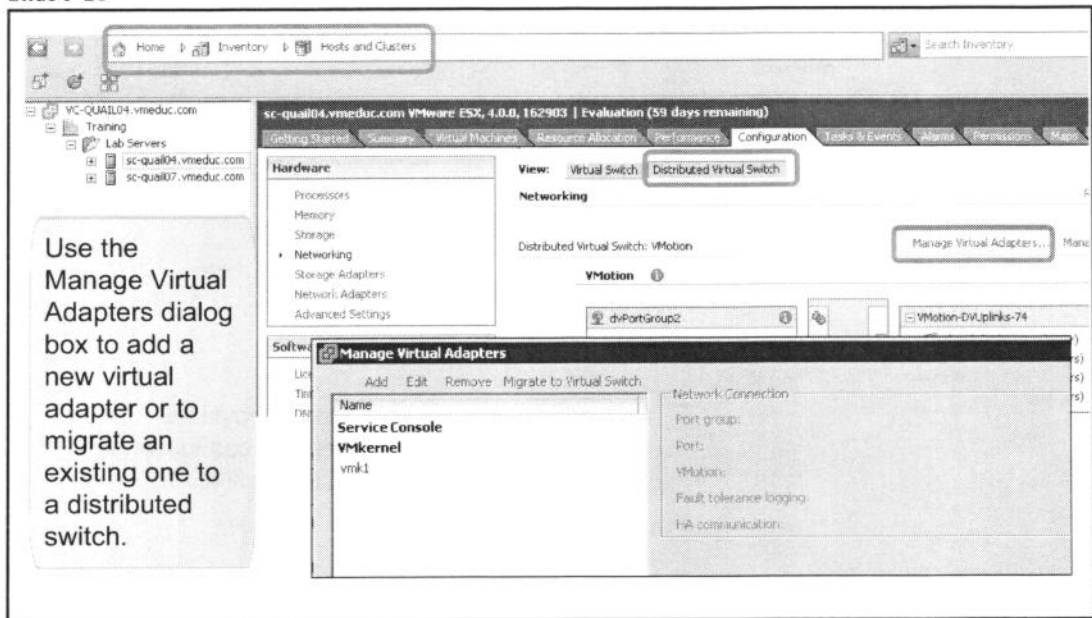
Select host and physical adapters		Host/Physical adapters	In use by switch	Physical adapter details	DVUplink port group
Ready to complete		  sc-qual07.vmeduc.com			
		Select physical adapters			
		<input type="checkbox"/>  vmnic0	vSwitch0	View details...	Production-DVUplinks-71
		<input checked="" type="checkbox"/>  vmnic1	--	View details...	Production-DVUplinks-71
		<input type="checkbox"/>  vmnic2	--	View details...	Production-DVUplinks-71
		<input type="checkbox"/>  vmnic3	--	View details...	Production-DVUplinks-71

To add a host to a distributed switch, go to the Networking inventory view. Right-click the distributed switch, then choose **Add Host**. The Add Host to Distributed Virtual Switch wizard appears.

Select the host from the list, then select one or more of its network adapters to add to the distributed switch. You can add only one host at a time.

VMkernel and Service Console Connections

Slide 5-28



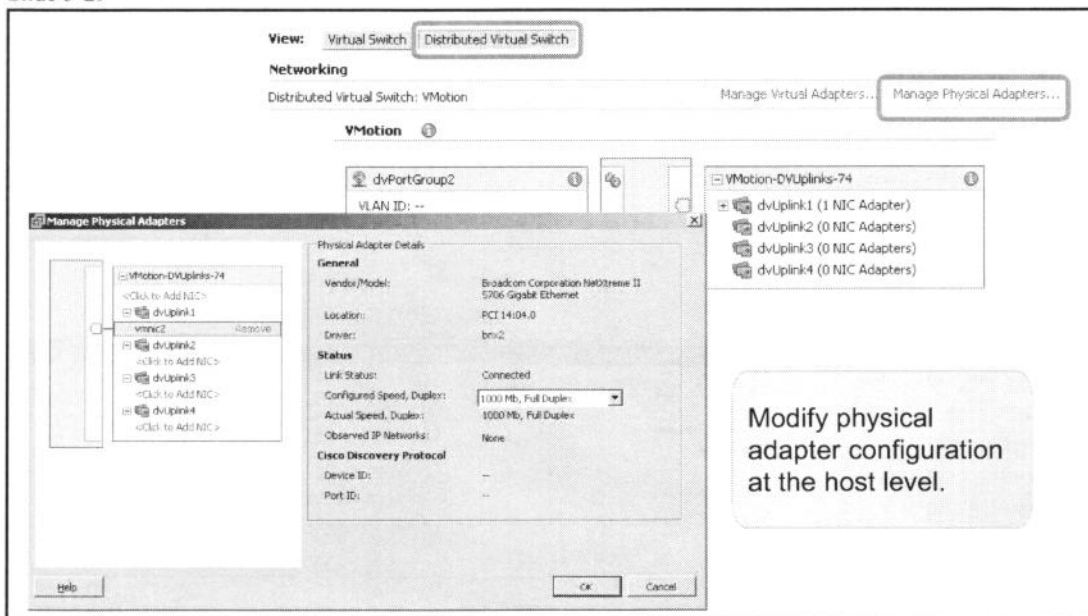
The Manage Virtual Adapters dialog box provides the means to add, edit, and remove the service console and VMkernel virtual adapters used by the selected host. To get to this dialog box, select your host in the Hosts and Clusters inventory view, then click the **Configuration** tab. In the **Hardware** section, select **Networking**, then click **Manage Virtual Adapters**.

In the Manage Virtual Adapters dialog box, if you select **Add**, you can create a new adapter. But you also have the option to migrate the existing adapters from the vSwitch to the distributed switch.

If you already have a virtual adapter listed (in the example above, vmk1), you also have the option to migrate the virtual adapter to a different virtual switch.

Managing Physical Adapters (Uplinks)

Slide 5-29



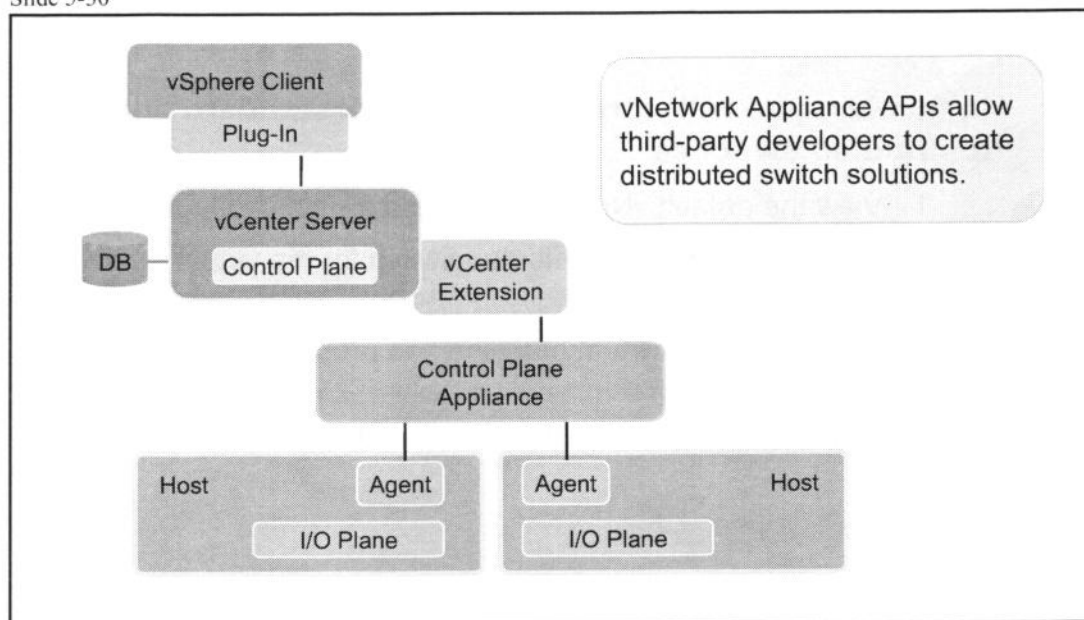
To add or remove a physical adapter from the uplink port group, go to the Distributed Virtual Switch view in the Networking display of the host's **Configuration** tab. Then click the **Manage Virtual Adapters** link. The association of physical adapters to distributed virtual switch uplink groups is a per-host configuration, so you cannot perform it at the datacenter level.

In the Manage Physical Adapters dialog box, click the **Click to Add NIC** link to add a physical adapter. Click the **Remove** link next to an uplink to delete the uplink from the distributed switch.

When adding adapters, you can assign them directly to a specific uplink category. Or you can select the topmost **<Click to Add NIC>** link to allow the system to decide.

Third-Party Distributed Switches

Slide 5-30



The vNetwork Appliance API allows third-party developers to create distributed switch solutions for use in a vSphere datacenter. Third-party solutions allow network administrators to extend existing network operations and management into the vSphere datacenter.

This diagram shows the basic way a third-party solution plugs in to the vNetwork architecture. The custom control plane is implemented outside of vCenter Server. For example, it can be implemented as a virtual appliance. The vSphere Client includes a plug-in to provide a management interface. vCenter Server includes an extension to handle the communication with the control plane. On the host, a custom I/O plane agent replaces the standard I/O plane agent. And the I/O plane itself can be replaced for customization of forwarding and filtering.

For example, the Cisco Nexus 1000v is a third-party switch to leverage vNetwork Appliance APIs. Network administrators can use this solution in place of the vNetwork distributed switch to extend vCenter Server to manage Cisco Nexus and Cisco Catalyst switches.

Lab 4

Slide 5-31

In this lab, you will work with vNetwork standard and distributed switches.

1. View the default vNetwork standard switch configuration.
2. Create a vNetwork distributed switch for the virtual machine network.
3. Verify that your virtual machine has proper access to the Production network.
4. Create a distributed switch for the VMotion network.

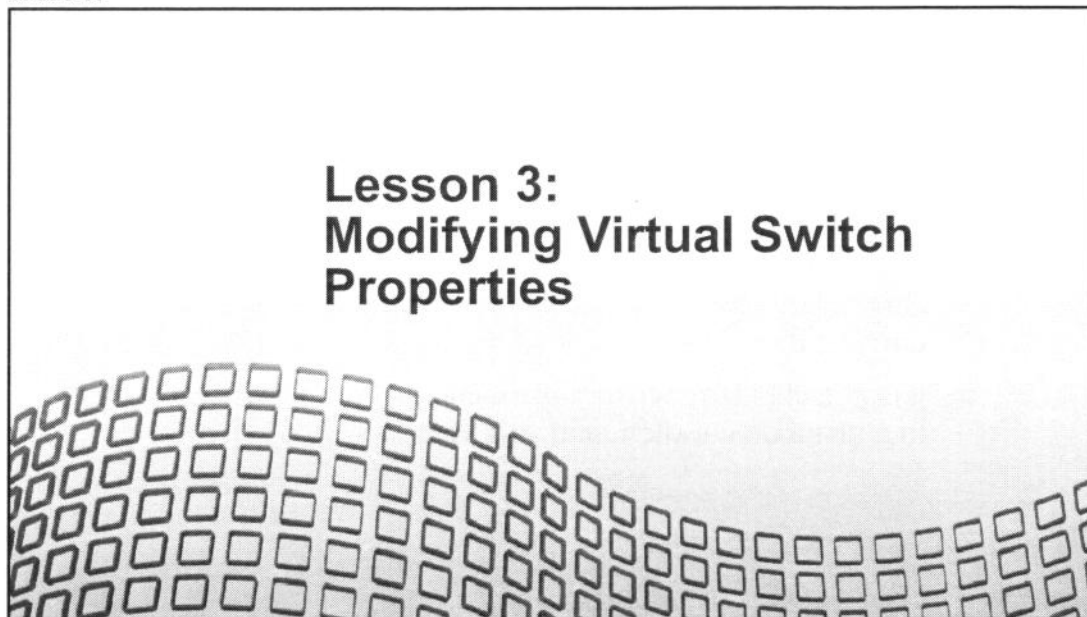
Lesson Summary

Slide 5-32

- A vNetwork distributed switch is similar to a vNetwork standard switch, except that it is configured at the vCenter Server level.
- Although the distributed switch is controlled by vCenter Server, the VMkernel connection, the service console connection, and the physical uplinks are still managed on each host.
- It is possible to move virtual machines from a standard switch to a distributed switch, and vice versa.

Lesson 3: Modifying Virtual Switch Properties

Slide 5-33



Lesson Objectives

Slide 5-34

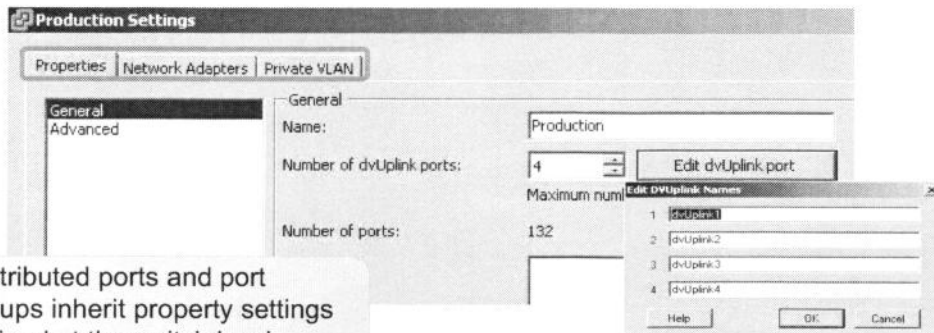
- > Describe the properties of a distributed switch
- > Describe the properties and policies of a distributed port group

Editing General Switch Properties

Slide 5-35

The Properties tab has settings for general information, policies, and advanced settings.

- General information includes name, number of uplink ports and optional names, number of ports, and notes.



If necessary, you can edit the properties of a distributed switch. To do this, in the Networking inventory view, right-click the distributed switch, then choose **Edit Settings**. The distributed switch settings dialog box appears, as shown above.

The distributed switch settings dialog box includes three tabs: **Properties**, **Network Adapters**, and **Private VLAN**.

The **Network Adapters** tab is a read-only form that allows you to verify which physical adapters are connected to the distributed switch.

The **Private VLAN** tab allows you to set up private VLANs for the distributed switch. Private VLANs are discussed later in the lesson.

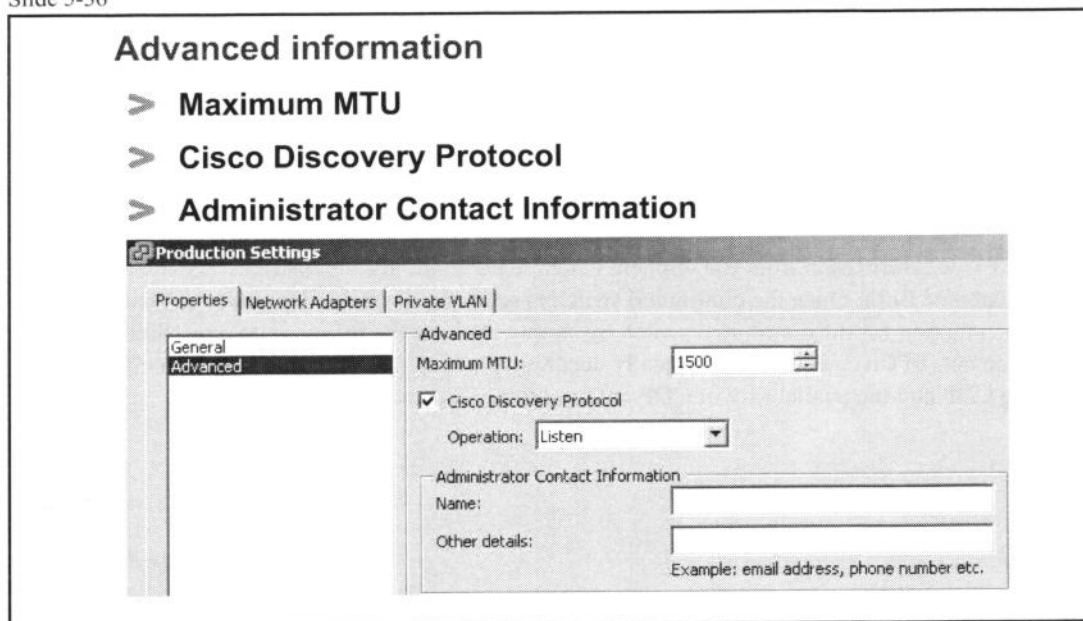
The **Network Adapters** and **Private VLAN** tabs are available only for distributed switches, not for distributed ports or distributed port groups.

Settings on the **Properties** tab are grouped into three major categories: **General**, **Policies**, and **Advanced**. With few exceptions, the same properties apply to distributed ports and distributed port groups.

General properties for the distributed switch allow you to edit the information specified when creating the distributed switch. You also have the option to name the uplinks and add notes. Naming uplinks is a good way to help administrators understand which uplinks to associate with port groups for the policies settings.

Editing Advanced Switch Properties

Slide 5-36



Advanced properties on the distributed switch allow you to define the maximum transmission unit, the Cisco Discovery Protocol status, and administrator contact details.

Maximum transmission unit (MTU) determines the maximum size of frames in this distributed switch. The distributed switch drops any frames bigger than the specified size. If your environment supports jumbo frames, use this option to enable or disable jumbo frames on the distributed switch. To enable jumbo frames on the distributed switch, set **Maximum MTU** to 9000.

To take advantage of jumbo frames, the network must support it end to end. That is, jumbo frame support must be enabled on the physical switch, on the distributed switch, and in the guest operating system of the virtual machine. This feature is available for the guest operating systems shown here.

To enable jumbo frames in the guest operating system of a virtual machine, first ensure that the latest version of VMware Tools is installed. Then, for the virtual network adapter, use either the vmxnet3, enhanced vmxnet, or e1000 virtual device.

ESXi supports jumbo frames only in the guest operating system. It does not include support for jumbo frames in the ESXi VMkernel TCP/IP stack.

Like standard switches, distributed switches support Cisco Discovery Protocol (CDP). CDP allows vCenter Server and the vSphere Client to identify properties of a physical switch, such as switch name, port number, port speed/duplex settings, and so forth. Use this option to configure CDP so that information about the physical adapter name and ESX/ESXi host names are passed to Cisco switches.

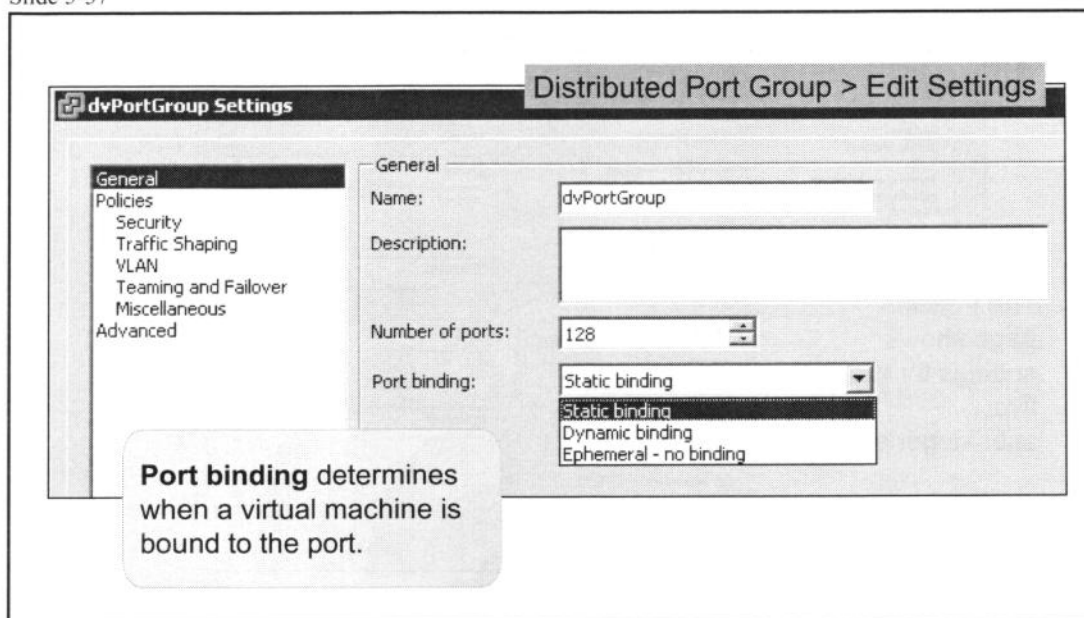
Once enabled, CDP has three operation modes:

- Listen mode – The ESX/ESXi host detects and displays information about the associated Cisco switch port, but information about the vSwitch is not available to the Cisco switch administrator.
- Advertise mode – The ESX/ESXi host makes information about the vSwitch available to the Cisco switch administrator, but does not detect and display information about the Cisco switch.
- Both mode – The ESX/ESXi host detects and displays information about the associated Cisco switch and makes information about the vSwitch available to the Cisco switch administrator.

To view Cisco information from the vSphere Client, CDP mode for the distributed switch must be either **Listen** or **Both**. Once the distributed switch is set to the correct CDP mode, you can view the Cisco information for the distributed switch by simply clicking the information icon. Since the CDP advertisements of Cisco equipment typically occur once a minute, you might notice a delay between enabling CDP and the availability of CDP data from the vSphere Client.

Editing Distributed Port Group Settings

Slide 5-37



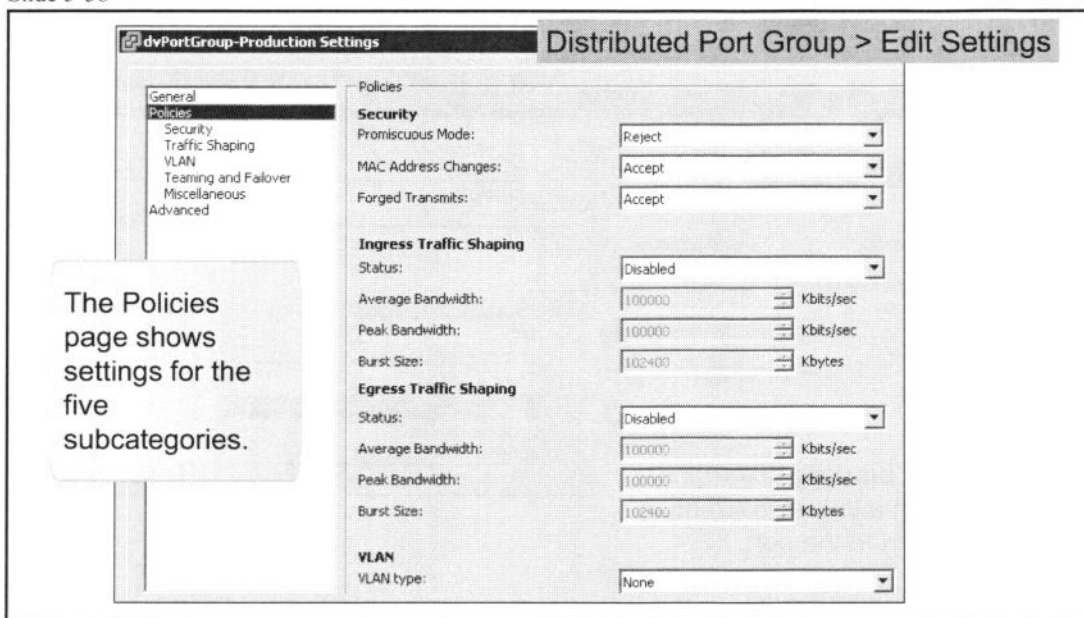
After creating a distributed port group, use the Distributed Port Group Settings dialog box to edit the general information and set policies for the ports within the port group. To get to the dialog box, go to the Networking inventory view. Right-click the distributed port group, then choose **Edit Settings**.

General settings for the distributed port group allow you to rename the distributed port group, give it a description, and specify the number of ports. You also have the option to select the port binding type. In the port binding, choose when ports are assigned to virtual machines connected to this port group:

- Select **Static binding** to assign a port to a virtual machine when the virtual machine is connected to the port group.
- Select **Dynamic binding** to assign a port to a virtual machine the first time the virtual machine powers on after it is connected to the port group. This is useful if you want to assign more virtual machines to the distributed port group than the number of ports, because the virtual machines are not all running at the same time. For example, you can have a distributed port group with 16 distributed ports and 40 virtual machines configured to connected to it. This results in a maximum of 16 virtual machines that can be powered up at the same time.
- Select **Ephemeral – no binding** for no port binding.

Editing Port Group Policies

Slide 5-38



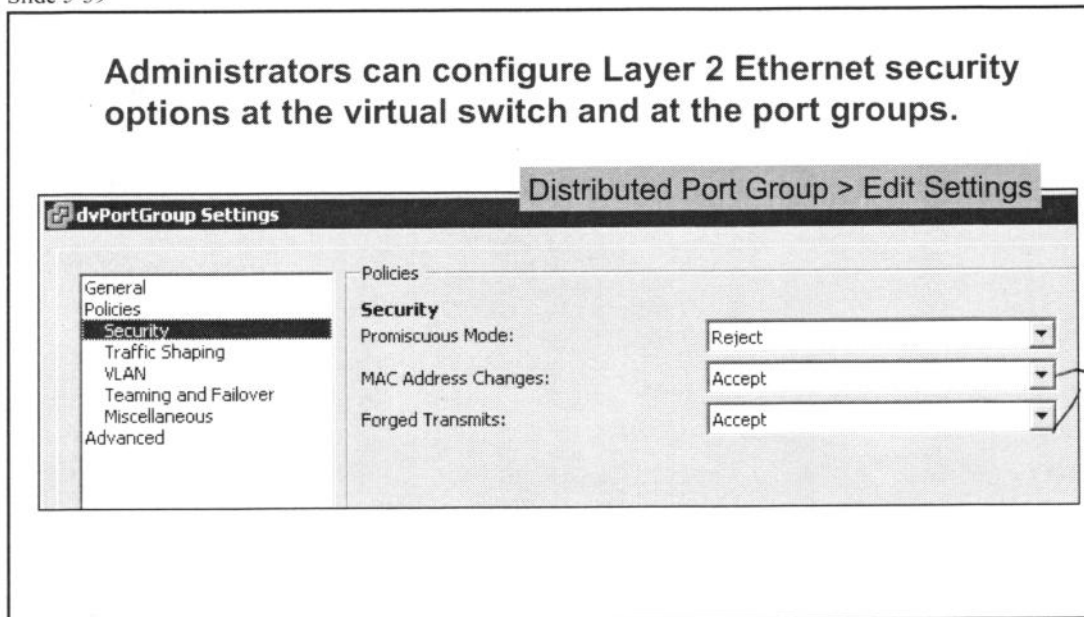
The Policies page shows all the options for each of the five subcategories below it. Most of the distributed port group policies are also used with standard switches:

- Security policies – Security policies are discussed shortly. They apply to both distributed switches and standard switches.
- Traffic-shaping policies – Traffic shaping is discussed shortly. Ingress and egress traffic shaping apply distributed switches. Egress traffic shaping applies only to standard switches.
- VLAN policies – VLANs are discussed shortly. They apply to both distributed switches and standard switches. Distributed switches have additional options.
- Teaming and failover policies – Teaming and failover are discussed in the “Scalability” module. They apply both to distributed switches and to standard switches.
- Miscellaneous policies – A miscellaneous policy applies only to distributed switches. It allows you to specify whether to block all ports of the distributed switch or distributed port group. Blocking has the same meaning as it has in the physical switch environment: no traffic will go through, but the NIC will still sense the carrier.

To edit the distributed port group policies, go to the Networking inventory view, right-click the distributed port group, then choose **Edit Settings**. Click the appropriate policy in the left pane of the port group’s Settings dialog box.

Security Policy

Slide 5-39



Security policies are defined at the distributed port group level (in a standard switch, security policies can be defined at both the virtual switch and port group level).

The network security policy contains the following exceptions:

- **Promiscuous Mode** – When set to **Reject**, placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter (default is **Reject**).
- **MAC Address Changes** – When set to **Reject**, if the guest attempts to change the MAC address assigned to the virtual NIC, it stops receiving frames (default is **Accept**).
- **Forged Transmits** – When set to **Reject**, drops any frames that the guest sends, where the source address field contains a MAC address other than the assigned virtual NIC MAC address (default is **Accept**).

In general, these policies give you the option of disallowing certain behaviors that could compromise security. For example, a hacker might use a promiscuous mode device to capture network traffic for unscrupulous activities. Or someone could impersonate a node and gain unauthorized access by spoofing its MAC address.

Set **Promiscuous Mode** to **Accept** if you want to use an application in a virtual machine that sniffs packets, such as a network-based intrusion-detection system.

Set **MAC Address Changes** and **Forged Transmits** to **Reject** to help protect against certain attacks launched by a rogue guest operating system.

Leave **MAC Address Changes** and **Forged Transmits** at their default value (**Accept**). The default retains the functions of certain guest applications if these applications normally change the mapped MAC address, as do some guest operating system–based firewalls.

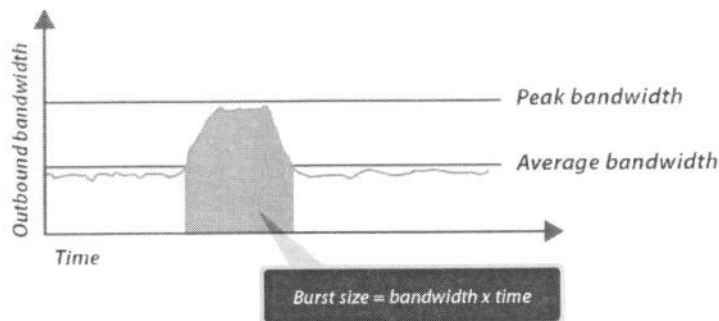
A possible scenario for wanting to set these policies is the case of a host that has “public exposure,” such as a Web server. One might be concerned with the possibility of it being compromised and then used as a launch pad for attacks either on other hosts owned or operated by the owner or against other hosts owned by others. By changing the originator information, a host could intend to spoof another system into allowing unauthorized access or it might want to avoid calling attention to its intrusion.

Traffic-Shaping Policy

Slide 5-40

Network traffic shaping is a mechanism for controlling a virtual machine's network bandwidth.

Average rate, peak rate, and burst size are configurable.



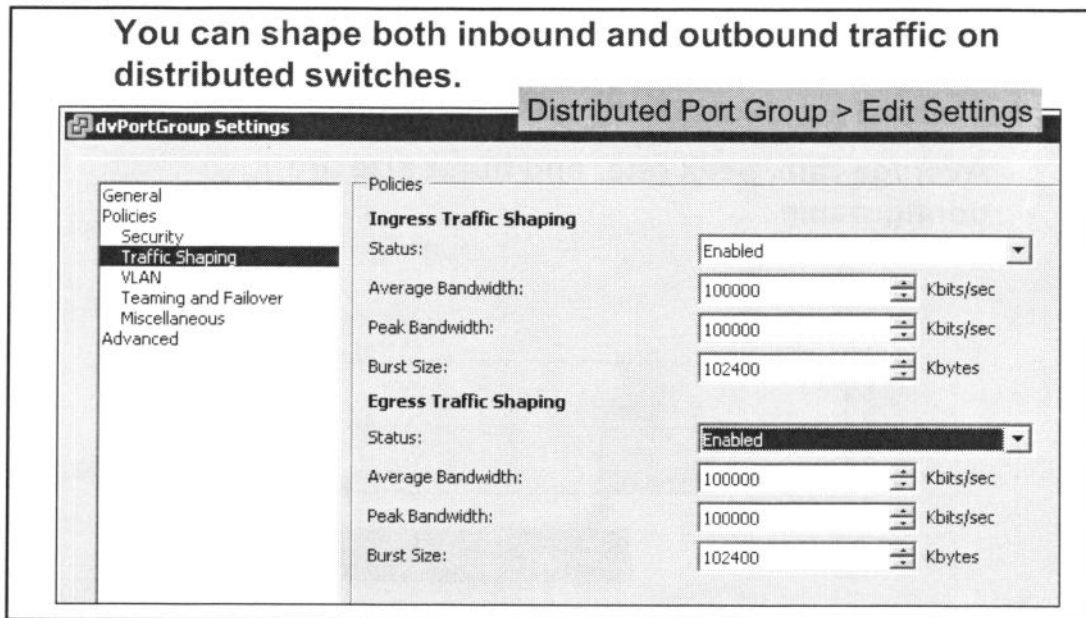
A virtual machine's network bandwidth can be controlled by enabling the network traffic shaper. The ESX/ESXi host shapes traffic by establishing parameters for three traffic characteristics: average bandwidth, peak bandwidth, and burst size. You can set values for these characteristics through the vSphere Client, establishing a traffic-shaping policy for each uplink adapter:

- **Average Bandwidth** – Establishes the number of kilobits per second to allow across the vSwitch averaged over time—the allowed average load.
- **Peak Bandwidth** – The maximum bandwidth the vSwitch can absorb without dropping packets. If traffic exceeds the peak bandwidth you establish, excess packets are queued for later transmission after traffic on the connection has returned to the average and there are enough spare cycles to handle the queued packets. If the queue is full, the packets are dropped. Even if you have spare bandwidth because the connection has been idle, the peak bandwidth parameter limits transmission to no more than peak until traffic returns to the allowed average load.
- **Burst Size** – Establishes the maximum number of kilobytes to allow in a burst. If a burst exceeds the burst-size parameter, excess packets are queued for later transmission. If the queue is full, the packets are dropped. When you specify values for these two characteristics, you indicate what you expect the vSwitch to handle during normal operation.

Average bandwidth and peak bandwidth are specified in Kbps (kilobits per second), and the burst size is specified in KB (kilobytes). Network traffic shaping is off by default.

Configuring Traffic Shaping

Slide 5-41



Distributed switches have the ability to shape both inbound and outbound traffic. (Standard switches can shape only outbound traffic.) Traffic-shaping policies are disabled by default so that services have a free, clear connection to the physical network. Enabling the policy for either ingress traffic shaping or egress traffic shaping sets limits on the amount of networking bandwidth allocated for each virtual adapter associated with the port group.

If you enable the policy, you must define the average bandwidth available for the distribute switch. **Peak Bandwidth** is the bandwidth to allow for short bursts, while **Burst Size** defines the maximum amount of traffic that can be generated at a speed above average.

Virtual machines connected to the port group will use the burst capacity once they have accumulated enough burst bonus, which is the difference between the amount of traffic generated and the average, capped by the burst size.

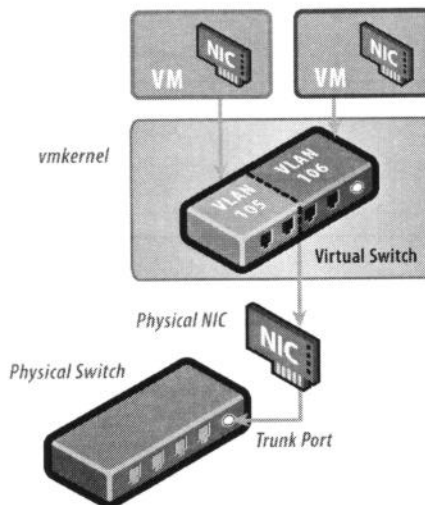
VLANs

Slide 5-42

ESX/ESXi supports 802.1Q VLAN tagging.

Virtual switch tagging is one of three tagging policies supported.

- Packets from a virtual machine are tagged as they exit the virtual switch.
- Packets are cleared (untagged) as they return to the virtual machine.
- There is little effect on performance.



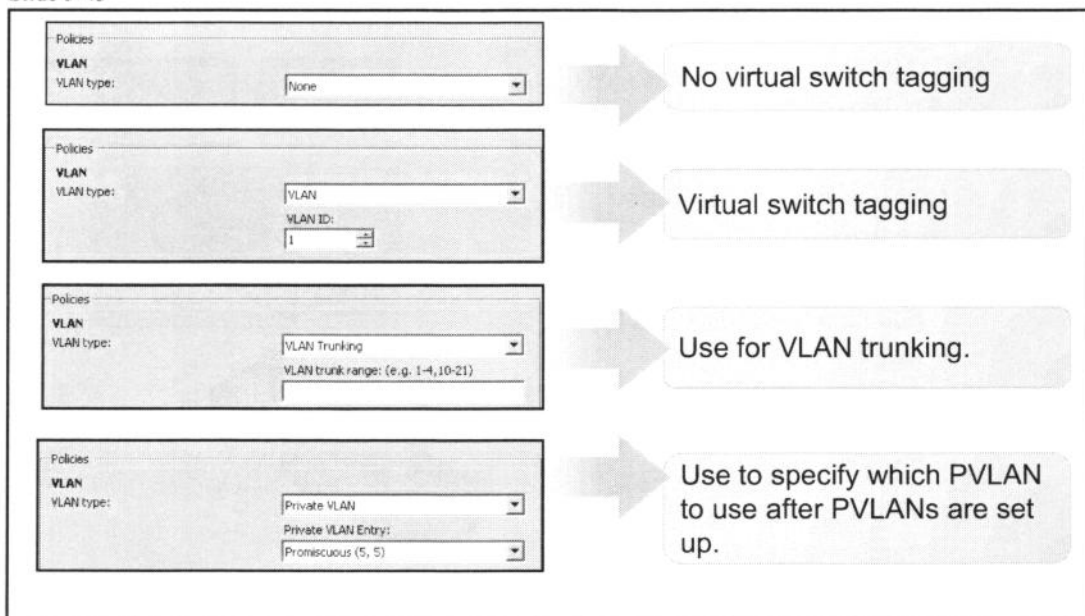
The ESX/ESXi host provides VLAN support through virtual switch tagging, which is provided by giving a port group a VLAN ID (by default, a VLAN ID is optional). The VMkernel then takes care of all tagging and untagging as the packets pass through the virtual switch.

A switch port on the physical ESX host must be defined as a static trunk port. A trunk port is a port on a physical Ethernet switch configured to send and receive packets tagged with a VLAN ID. No VLAN configuration is required in the virtual machine. In fact, the virtual machine does not know it is connected to a VLAN.

For more information on how ESX has implemented VLANs, see the white paper “VMware ESX Server 3 802.1Q VLAN Solutions” at http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

VLAN Policy

Slide 5-43

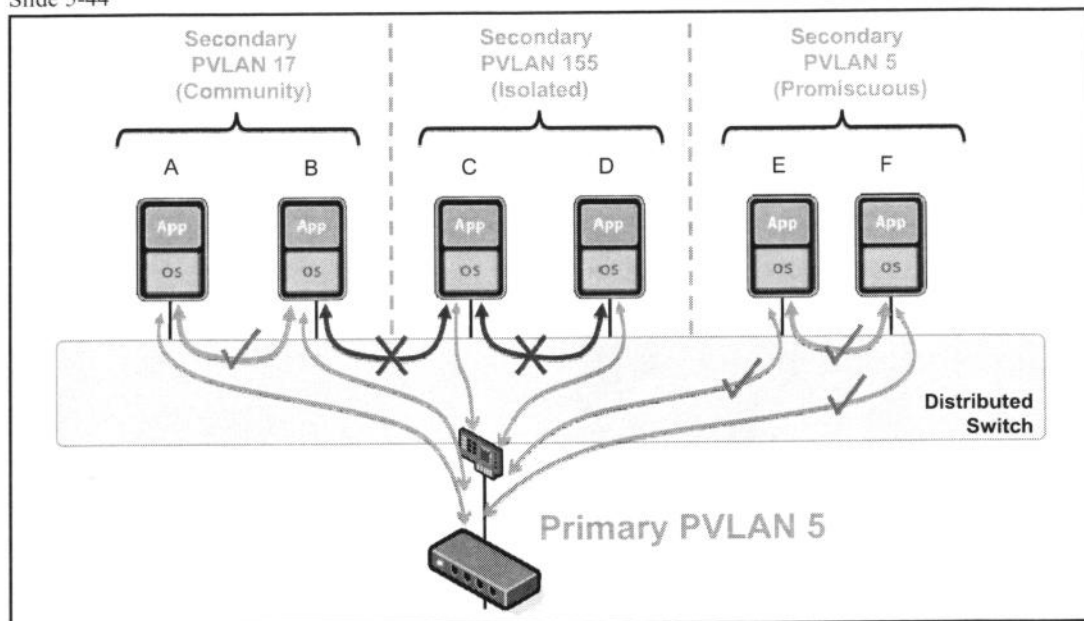


The VLAN policy allows you to choose a VLAN type. These are the options for VLAN type:

- **None** – This option means that the distributed switch will perform no tagging or untagging, and the traffic will travel untagged between virtual machines and the physical switch. Use this option for external switch tagging or for cases in which you are not using VLANs at all.
- **VLAN** – Also known as virtual switch tagging, this option allows you to specify which VLAN to tag or untag. This means that all traffic from the distributed switch and the physical switch is tagged to the specified VLAN, and all traffic between the distributed switch and the virtual machines is untagged. The accepted values are 1 to 4094, as 0 and 4095 are not allowed.
- **VLAN Trunking** – This option is used for VLAN trunking and allows you to specify which VLANs to allow in the trunk.
- **PVLAN** – This option allows you to specify which PVLAN to use. Choose this option after you define PVLANS on the **PVLAN** tab for the distributed switch.

Private VLAN Architecture

Slide 5-44



Private VLANs (PVLANS) allow you to isolate traffic between virtual machines in the same isolated VLAN. They provide additional security between virtual machines on the same subnet without exhausting VLAN number space. PVLANS are particularly useful on a DMZ where the server needs to be available to external connections and possibly internal connections, but rarely needs to communicate with the other servers on the DMZ.

The basic concept behind private VLANs is to divide an existing VLAN, referred to as the primary VLAN, into one or more separated VLANs, called secondary VLANs.

There are three types of secondary VLANs: *promiscuous*, *isolated*, and *community*.

- Virtual machines in a promiscuous PVLAN are reachable by and can reach any machine in the same primary VLAN. In this example, virtual machines E and F are in promiscuous PVLAN 5, so all virtual machines in PVLAN 5 can communicate with them.
- Virtual machines in an isolated PVLAN can talk to no virtual machines except those in the promiscuous PVLAN. In this example, virtual machines C and D are in isolated PVLAN 155, so they can communicate only with E and F.
- Virtual machines in a community PVLAN can talk to each other and to the virtual machines in the promiscuous PVLAN, but not to any other virtual machine. In this example, virtual machines A and B can talk to each other and to E and F because they are in the promiscuous VLAN. However, they cannot communicate with C or D, because they are not in the community.

Traffic in both community and isolated PVLANS travels tagged as the associated secondary PVLAN.

There are a couple of things to note about how vNetwork implements private VLANs:

- vNetwork does not encapsulate traffic inside private VLANs. In other words, there is no secondary PVLAN encapsulated inside a primary private VLAN packet.
- Traffic between virtual machines on the same private VLAN, but on different hosts, moves through the physical switch. Therefore, the physical switch must be PVLAN-aware and configured appropriately so that traffic in the secondary PVLANS can reach its destination.

Configuring and Assigning PVLANS

Slide 5-45

dvSwitch-zir01 Settings

Properties | Network Adapters | **Private VLAN**

Enter or edit primary private VLAN ID.

Primary private VLAN ID
5
[Enter a private VLAN ID here]

Configure.

Network Configuration > Distributed Switch > Edit Settings

Enter or edit a secondary private VLAN ID and Type.

Secondary private VLAN ID	Type
5	Promiscuous
155	Isolated
17	Community

[Enter a private VLAN ID here] Select

dv-Production Settings

General | Policies | Security | Traffic Shaping | **VLAN** | Teaming and Failover | Miscellaneous | Advanced

Policies

VLAN

VLAN type: Private VLAN

Private VLAN Entry:

- Community (5, 17)
- Promiscuous (5, 5)
- Isolated (5, 155)
- Community (5, 17)

Assign.

The first step to set up a private VLAN is to create the PVLAN primary and secondary associations. To do so, edit the settings of the distributed switch. On the PVLAN tab, first specify the primary VLAN ID. The vSphere Client automatically creates a promiscuous secondary PVAN with the same ID.

To create additional secondary PVLANS, for each addition, click **Enter a private VLAN ID here**, enter an ID, and select a type.

After the primary and secondary PVLANS are associated for the distributed switch, use the association to configure the VLAN policy for the distributed port group. To do so, go to the VLAN policy for the distributed port group. In **VLAN type**, select **Private VLAN**, and select one of the associations you just created.

Advanced Settings

Slide 5-46

Blocking, traffic shaping, VLAN, NIC teaming, and security policies can be configured at the port level if permitted at the port group level.

Settings	Overrides Allowed?
Block Port:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Traffic Shaping:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Vendor Configuration:	<input type="radio"/> Yes <input checked="" type="radio"/> No
VLAN:	<input type="radio"/> Yes <input checked="" type="radio"/> No
DVUplink Teaming:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Security Policy:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Advanced distributed port group properties allow you to fine-tune port behavior.

Distributed port group policies can be overridden on a per-port level. Click the **Edit Override Settings** link to fine-tune which policies can be overridden at the port level. You can also specify which settings are allowed or not allowed to be overridden at the port level.

Additional advanced port group properties:

- **Live port moving** – Allows standalone ports to be moved to a distributed port group while the ports are in use. Moving the port to a distributed port group allows the port to acquire all of that port group's configuration. Standalone ports can be created only by using the vSphere SDK and not from the vSphere Client interface.
- **Configure reset at disconnect** – When a distributed port is disconnected from a virtual machine, the configuration of the distributed port is reset to the distributed port group setting and any per-port configuration is discarded.
- **Port Name Format** – Provides a template for assigning names to the distributed ports in this distributed port group.

Lab 5

Slide 5-47

In this lab, you will design a network configuration for an ESX host based on a set of requirements.

1. Analyze the requirements.
2. Design virtual switches and physical connections.

Lesson Summary

Slide 5-48

- > Properties at the distributed port group level can be overridden per port.
- > The security policy and the network traffic-shaping policy can be configured for a distributed port group or a standard virtual switch.
- > Distributed switches support VLANs and private VLANs.

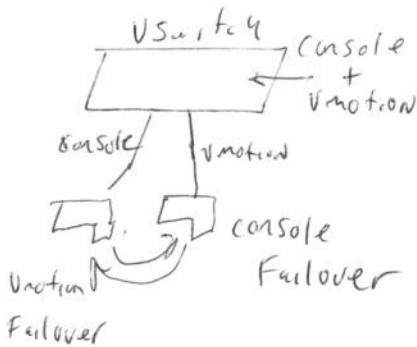
Key Points

Slide 5-49

- > Both distributed switches and standard switches can be used in the vSphere environment.
- > Both distributed switches and standard switches support the three connection types: virtual machines, VMkernel, and service console.
- > Distributed switches are configured at the vCenter Server level, while standard switches are configured at the host level.

Switch port numbers

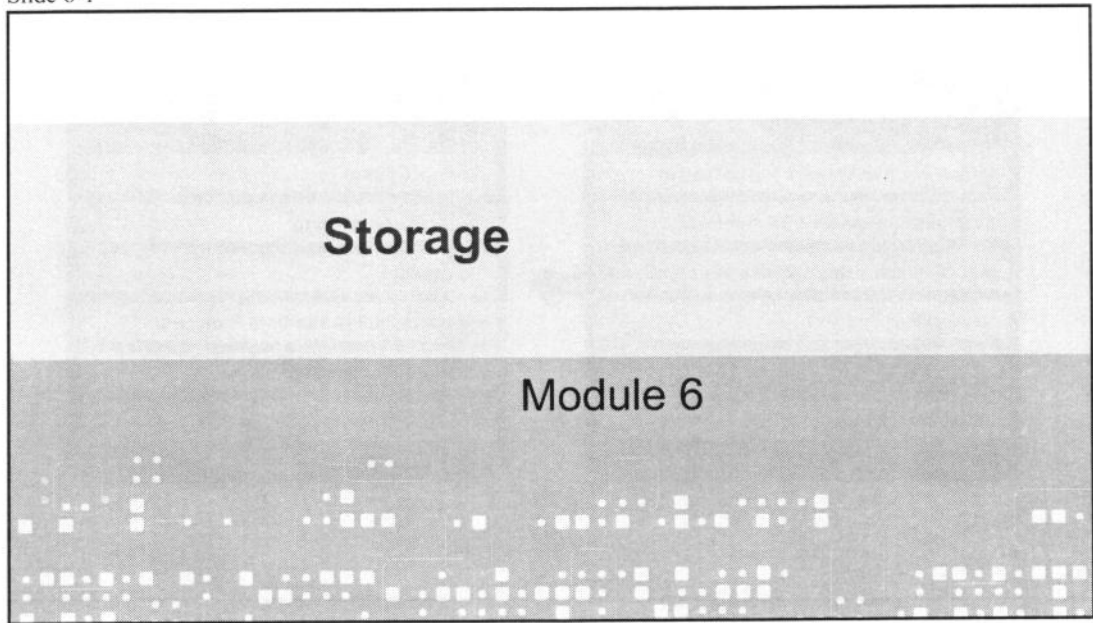
$$64 - 1 (\text{Reserved for kernel}) = 56$$



more than 1 kernel port must
Be on diffrent subnets

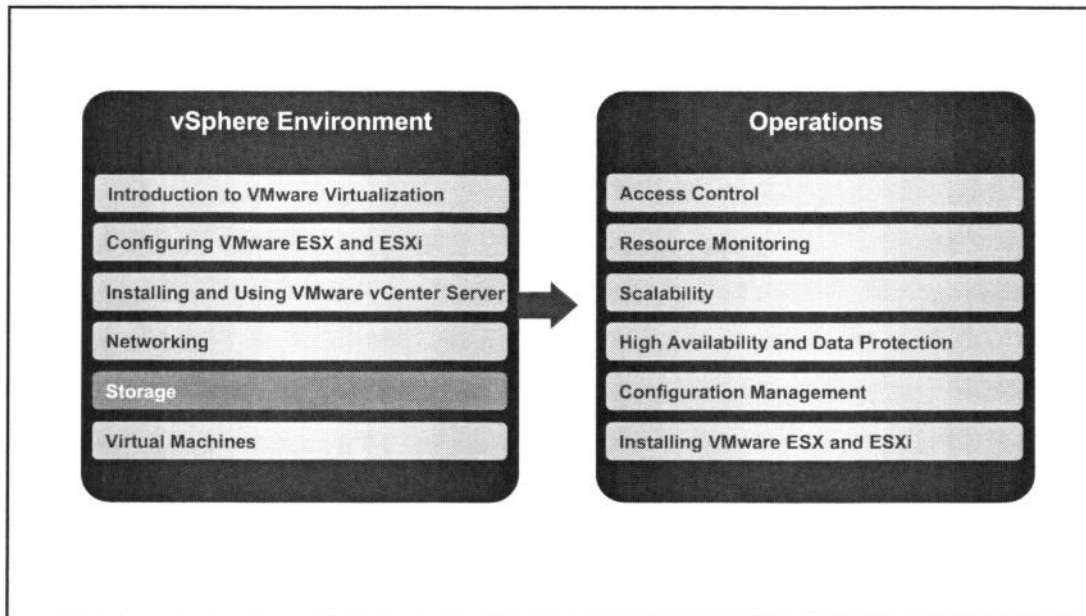
Storage

Slide 6-1



You Are Here

Slide 6-2



Importance

Slide 6-3

- Storage options give you the flexibility to set up your storage based on your cost, performance, and manageability requirements. Shared storage is useful for disaster recovery, high availability, and moving virtual machines between hosts.

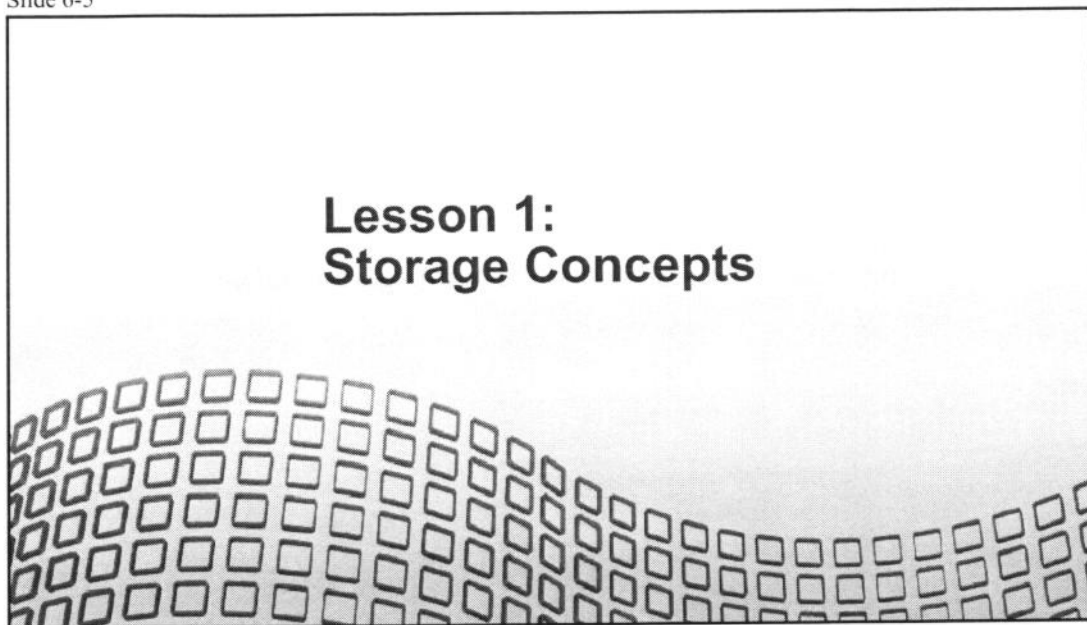
Module Lessons

Slide 6-4

- Lesson 1: Storage Concepts**
- Lesson 2: Fibre Channel SAN Storage**
- Lesson 3: iSCSI Storage**
- Lesson 4: VMFS Datastores**
- Lesson 5: NAS Storage and NFS Datastores**

Lesson 1: Storage Concepts

Slide 6-5



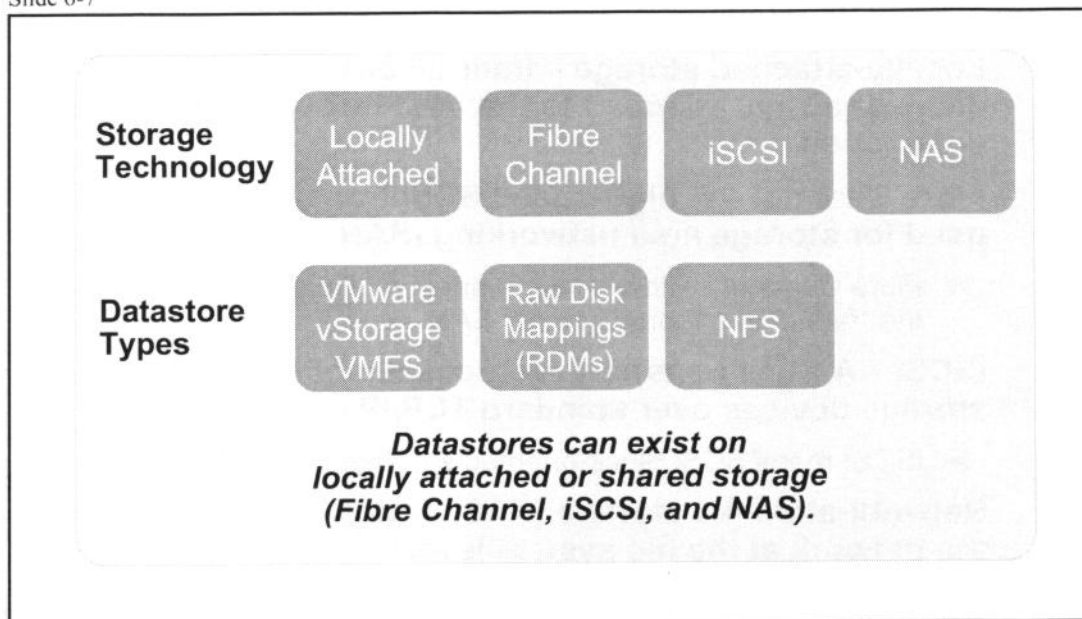
Lesson Objectives

Slide 6-6

- > Describe VMware® vSphere™ storage technologies and datastores
- > Describe the various ways to view storage information
- > Understand the storage device naming convention

Storage Overview

Slide 6-7



Several storage technologies are supported in by VMware® ESX™/ESXi hosts in the VMware vSphere™ environment: locally attached storage, Fibre Channel storage, iSCSI storage, and network-attached storage (NAS).

Datastores are logical containers, analogous to file systems, that hide specifics of each storage device and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images. Depending on the type of storage you use, datastores can have the following file system formats: VMware vStorage Virtual Machine File System (VMFS), raw device mapping (RDM), and Network File System (NFS).

Datastores can exist on either locally attached storage or shared storage, such as Fibre Channel, iSCSI, and NAS.

Storage Technology Overview

Slide 6-8

Locally-attached storage – Internal or external storage disks or arrays attached to the host through a direct connection

Fibre Channel – A high-speed SCSI transport protocol used for storage area networking (SAN)

- Fibre Channel switches interconnect multiple nodes to form the “fabric” in a Fibre Channel SAN.

iSCSI – A SCSI transport protocol, enabling access to storage devices over standard TCP/IP networks

- iSCSI maps SCSI block-oriented storage over TCP/IP.

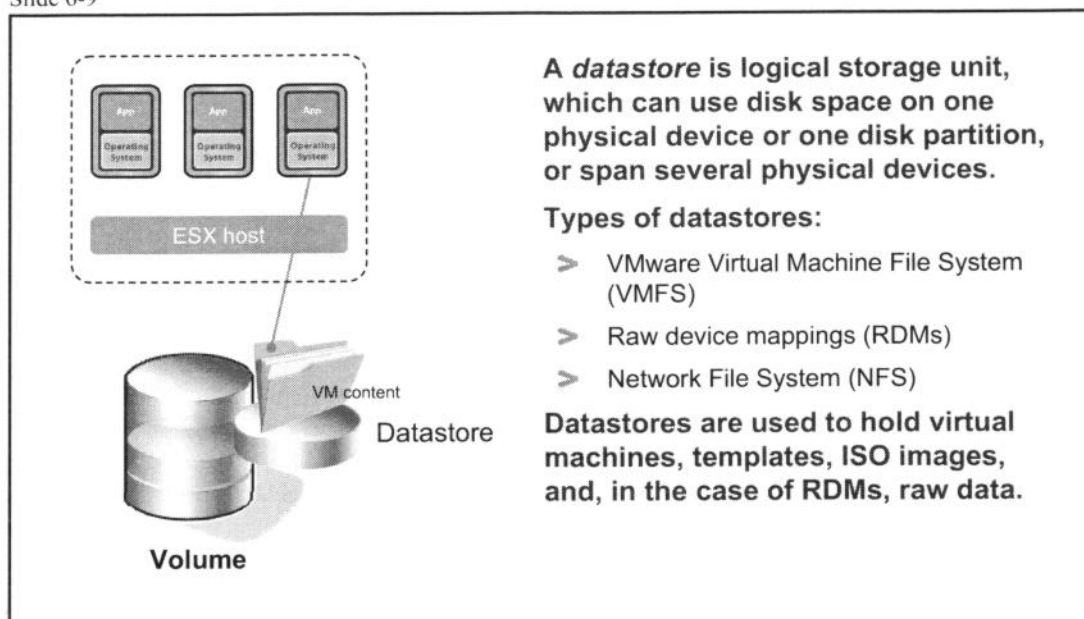
Network-attached storage (NAS) – Storage shared over the network at the file system level

vSphere supports a number of storage technologies:

- Local storage – Internal or external storage disks or arrays attached to the host through a direct connection.
- Fibre Channel – A high-speed transport protocol used for storage area networks (SANs). Fibre Channel encapsulates SCSI commands, which are transmitted between Fibre Channel nodes. In general, a Fibre Channel node is a server, a storage system, or a tape drive. A Fibre Channel switch interconnects multiple nodes, forming the “fabric” in a Fibre Channel network.
- iSCSI – A SCSI transport protocol, enabling access to storage devices over standard TCP/IP networks. iSCSI maps SCSI block-oriented storage over TCP/IP. *Initiators*, such as an iSCSI HBA in an ESX/ESXi host, send SCSI commands to *targets*, located in iSCSI storage systems.
- NAS – Storage shared over standard TCP/IP networks at a file system level. NAS storage is used to hold NFS datastores.

Datastores

Slide 6-9



A **datastore** is logical storage unit, which can use disk space on one physical device or one disk partition, or span several physical devices.

Types of datastores:

- > VMware Virtual Machine File System (VMFS)
- > Raw device mappings (RDMs)
- > Network File System (NFS)

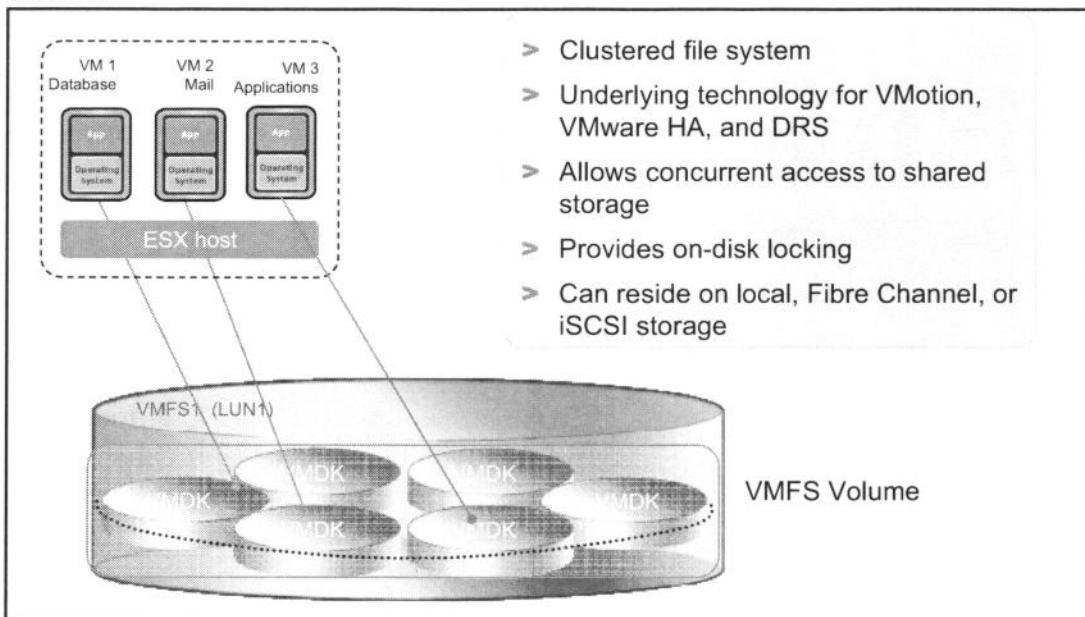
Datastores are used to hold virtual machines, templates, ISO images, and, in the case of RDMs, raw data.

A virtual machine is stored as a set of files in its own directory in the datastore. The datastore is formatted as VMFS, RDM, or NFS, depending on the type of physical storage in the datacenter.

The datastore can be manipulated (copied, moved, backed up, and so on) just like a file. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images.

VMFS

Slide 6-10



VMFS is a clustered file system that allows multiple physical servers to read and write to the same storage device simultaneously. The cluster file system enables unique virtualization-based services, such as live migration of running virtual machines from one physical server to another, automatic restart of a failed virtual machine on a separate physical server, and clustering virtual machines across different physical servers.

VMFS allows IT organizations to greatly simplify virtual machine provisioning by efficiently storing the entire machine state in a central location. VMFS allows multiple ESX/ESXi hosts to access shared virtual machine storage concurrently. VMFS provides the foundation that allows the scaling of virtualization beyond the boundaries of a single system.

VMFS provides on-disk distributed locking to ensure that the same virtual machine is not powered on by multiple servers at the same time. If a physical server fails, the on-disk lock for each virtual machine can be released so that virtual machines can be restarted on other physical servers.

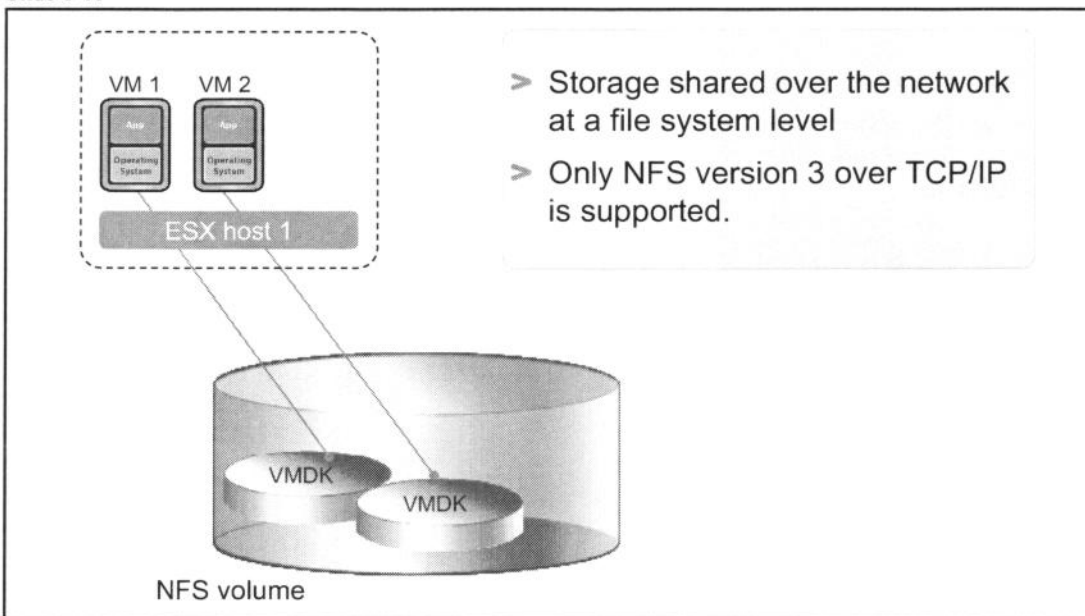
In the example above, the ESX host has three virtual machines running on it. The lines connecting the virtual machines to the disk icons for the virtual machine disks (VMDKs) are logical representations of the association and allocation of the larger VMFS volume, which is made up of one large volume with a unique logical unit number (LUN). The virtual machines see the assigned storage volume only as a SCSI target from within the guest operating system. The virtual machine contents are really just files on the VMFS volume.

VMFS can be deployed on a variety of SCSI-based storage devices: locally attached storage, Fibre Channel storage, and iSCSI storage. A virtual disk stored on VMFS always appears to the virtual machine as a mounted SCSI device. The virtual disk hides the physical storage layer from the virtual machine's operating system. This feature allows you to run even operating systems not certified for SAN inside the virtual machine.

For the operating system inside the virtual machine, VMFS preserves the internal file system semantics, which ensure correct application behavior and data integrity for applications running in virtual machines.

NFS

Slide 6-11



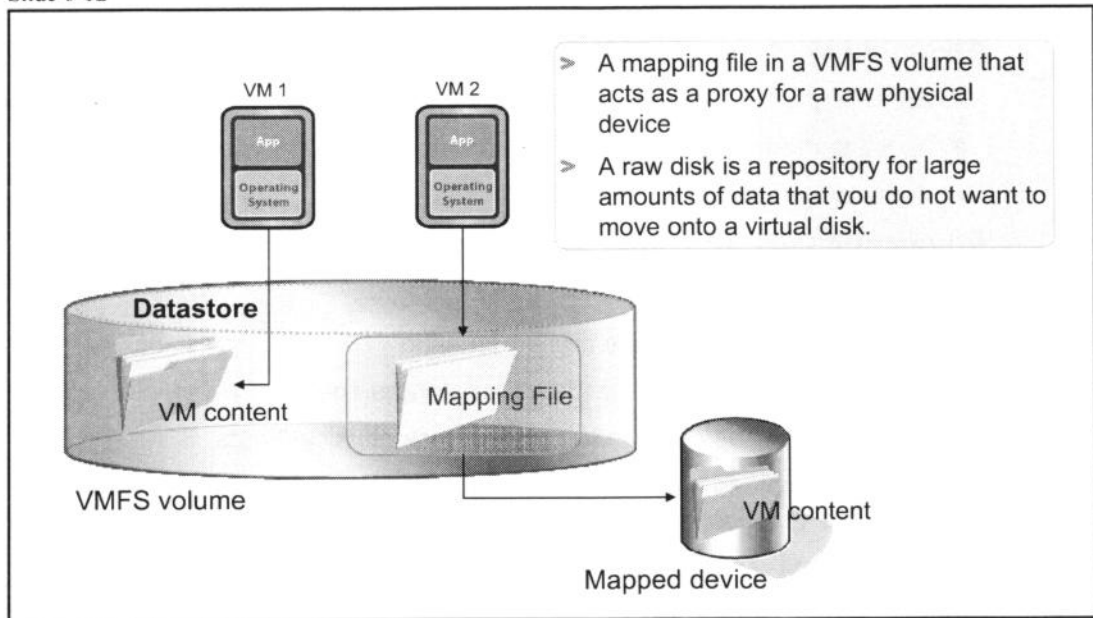
NFS is a file-sharing protocol that ESX/ESXi hosts use to communicate with a NAS device. NAS is a specialized storage device that connects to a network and can provide file access services to ESX/ESXi hosts.

NFS datastores are treated just like VMFS datastores. They can be used to hold virtual machines' files, templates, and ISO images. In addition, an NFS volume allows the migration using VMware VMotion™ of virtual machines whose files reside on an NFS datastore.

ESX/ESXi hosts support NFS version 3 over TCP only.

Raw Device Mapping (RDM)

Slide 6-12



For virtual machines running on an ESX/ESXi host, instead of storing virtual machine data in a virtual disk file, you can store the data directly on a raw LUN. This is useful if you are running applications in your virtual machines that must know the physical characteristics of the storage device. Additionally, mapping a raw LUN allows you to use existing SAN commands to manage storage for the disk. A raw device mapping (RDM) is used to map to the raw LUN.

An RDM is a special file in a VMFS volume that acts as a proxy for a raw LUN. An RDM maps a file in a VMFS volume to a raw volume. A virtual machine then references the RDM, which in turn points to the raw volume holding the virtual machine's data.

An RDM is recommended when a virtual machine must interact with a real disk on the SAN. This is the case, for example, when you make disk array snapshots, or when you have a large amount of data that you do not want to move onto a virtual disk. An RDM is also used when you want to cluster a virtual machine with a physical machine using Microsoft Cluster Service (MSCS). For more information on setting up Microsoft Cluster Service with RDMs, see *Setup for Microsoft Cluster Service* at <http://www.vmware.com/support/pubs>.

Local versus Shared Storage

Slide 6-13

Advantages of using local storage

- > Easy to physically move the box
- > Easy to manage
- > More secure

Advantages of using shared storage

- > Central repository
- > Scalable and recoverable implementation
- > Multiple hosts can access the same storage space
- > Virtual machines can be clustered across physical hosts
- > Virtual machines can take advantage of vSphere features such as VMware VMotion™
- > Allows data replication

Local storage can be used to hold virtual machines. In many small environments, this is how the ESX/ESXi host is first implemented. And, since the virtual machines are all located on the locally attached storage device of the host, Managing the host, securing the host, or physically relocating the host can be easier because all storage is contained within a single host.

Shared storage offers a number of benefits over local storage. Shared storage allows VMotion migrations to be performed; allows you to have a fast, central repository for virtual machine templates; allows you to recover virtual machines on another host if you have a host failure; allows clustering of virtual machines across hosts; and allows you to allocate large amounts (terabytes) of storage to your ESX/ESXi hosts.

Storage Device Naming Conventions

Slide 6-14

Storage devices are identified in several ways:

- > SCSI ID – Unique SCSI identifier
- > Canonical name – The Network Address Authority (NAA) ID is a unique LUN identifier, guaranteed to be unique across reboots.
 - For those devices without a unique ID, a VMware mpx reference is used instead.
- > Runtime name – Uses the convention vmhbaN:C:T:L. This name is not persistent through reboots.

SCSI ID	Canonical Name	Runtime Name	Lun
000000000766d686261303a303a30	mpx.vmhba0:C0:T0:L0	vmhba0:C0:T0:L0	0
01000100002020457378536373692d...			
020000000050060160c1e0eb0a5006...	naa.50060160c1e0eb0a50060160c1e0eb0a	vmhba1:C0:T0:L0	0
020006000060060160d2b02000bcb9...	naa.60060160d2b02000bcb96451d6b1dd11	vmhba1:C0:T0:L6	6

On ESX/ESXi hosts, SCSI storage devices use a variety of identifiers:

- SCSI ID – This is the unique address of a SCSI device.
- Canonical name – This is the Network Address Authority ID. NAA IDs are globally unique identifiers that are persistent across system reboots.

For those devices that do not have an NAA ID, an “mpx” name is used instead. mpx is not an acronym. It is a VMware-specific namespace. The mpx namespace is used when no other valid namespace can be obtained from the LUN, such as an NAA ID. An mpx name is not globally unique and is not persistent across reboots. Typically, only local devices will not have a globally unique identifier such as an NAA ID and thus names starting with mpx.

- Runtime name – This name exists to assist customers who are familiar with this format from earlier versions of ESX/ESXi. The naming convention is vmhbaN:C:T:L, where N is the number of the vmhba (host bus adapter), C is the channel number (always zero for ESX/ESXi), T is the target ID, and L is the LUN number. This name is not persistent across system reboots.

Additional names for storage devices are the iSCSI qualified name (IQN), used for iSCSI targets, and the World Wide Name (WWN), used for Fibre Channel targets.

Storage device names appear in various panels in the vSphere Client. You will see examples of these panels later in the module.

Physical Storage Considerations

Slide 6-15

Discuss vSphere storage needs with your storage administration team:

- > LUN sizes
- > I/O bandwidth
- > Disk cache parameters
- > Zoning and masking
- > Identical LUN presentation to each VMware ESX™/ESXi host
- > Active-active or active-passive arrays
- > Export properties for NFS datastores

Before you implement your vSphere environment, discuss your vSphere storage needs with your storage administration team.

Discuss things like LUN sizes, I/O bandwidth required by your applications, disk cache parameters, zoning and masking, identical LUN presentation to each ESX/ESXi host, which multipathing setting to use (active-active or active-passive) for your storage arrays, and what NFS settings to use.

For information that will help you plan for your storage needs, see the *SAN System Design and Deployment Guide* at <http://www.vmware.com/support/pubs>.

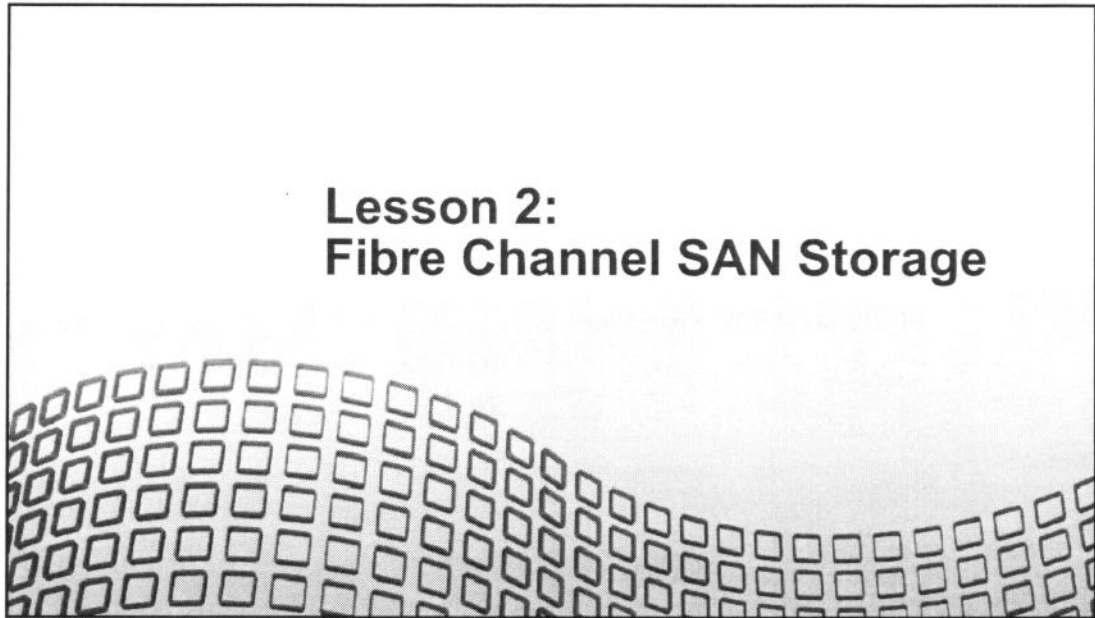
Lesson Summary

Slide 6-16

- > vSphere supports Fibre Channel, iSCSI, and NAS storage technologies.
- > vSphere supports VMFS datastores, RDMs, and NFS datastores.
- > View storage information from the host's **Configuration** tab or the **Storage Views** tab.
- > Storage devices are uniquely identified using the NAA ID.

Lesson 2: Fibre Channel SAN Storage

Slide 6-17



Lesson Objectives

Slide 6-18

- > Describe uses of Fibre Channel with ESX/ESXi
- > Describe Fibre Channel components and addressing
- > Access Fibre Channel storage
- > View Fibre Channel storage information

Using Fibre Channel with ESX/ESXi

Slide 6-19

Uses of Fibre Channel SAN LUNs:

- > VMFS datastores to hold virtual machines, ISO images, and templates
- > RDMs to hold a virtual machine's raw data
- > Supports vSphere features such as VMotion, VMware High Availability, and VMware Distributed Resource Scheduler (DRS)
- > To boot ESX from a SAN LUN

ESX/ESXi supports:

- > 8GB Fibre Channel
- > Fibre Channel over Ethernet (FCoE)

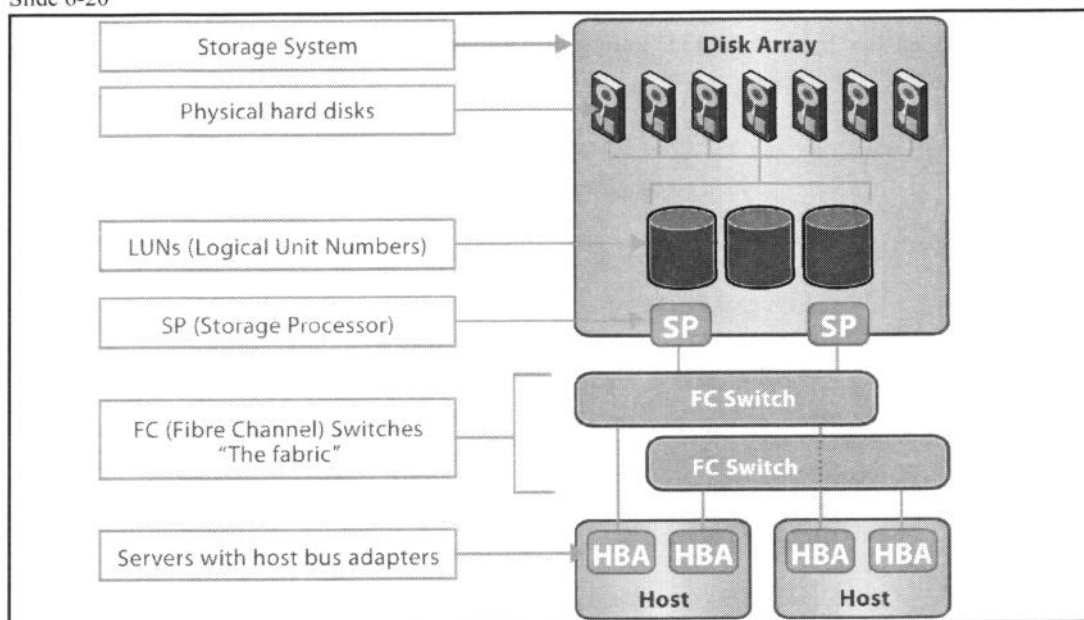
Fibre Channel SAN storage is commonly used for VMFS datastores. VMFS datastores are used to hold virtual machines' files, ISO images, templates, and RDMs that point to raw volumes on the Fibre Channel SAN.

VMFS datastores on a Fibre Channel SAN can be shared across multiple ESX/ESXi hosts. As a result, Fibre Channel plays an important role in supporting vSphere features such as VMotion, VMware High Availability, VMware Distributed Resource Scheduler (DRS), and VMware Consolidated Backup.

Installing and booting an ESX host from a Fibre Channel SAN LUN is supported. To boot from SAN, the BIOS of the Fibre Channel adapter must be configured with the WWN and LUN number of the boot device, and the system BIOS must designate the Fibre Channel adapter as a boot controller.

Fibre Channel SAN Components

Slide 6-20

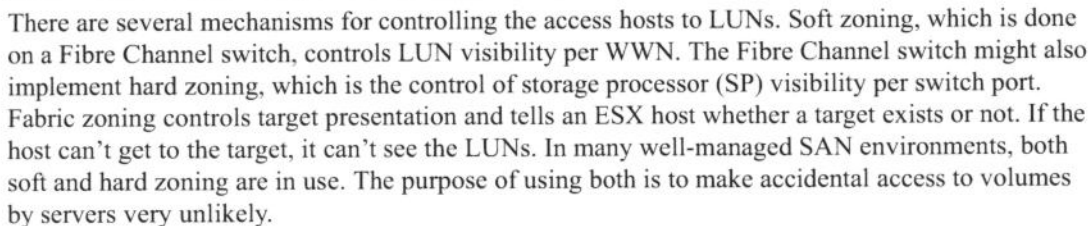


A Fibre Channel SAN consists of the following:

- **Storage system** – This is the hardware that consists of a set of physical hard disks, or disk array, and one or more intelligent controllers. The storage system supports the creation of LUNs. Disk arrays' storage processors aggregate physical disks into logical volumes, or LUNs, each with a LUN number identifier.
- **LUN** – The logical unit number is the address of a logical unit (LU). An LU is a unit of storage access. An LU can be a JBOD (just a bunch of disks) or a part of a JBOD, a RAID set (also referred to as a "storage container"), or a part of a storage container. Both a JBOD and a storage container can be partitioned into multiple LUNs. An LU can also be a control function like an array gatekeeper LUN or tape controller.
- **Storage processor** – A storage processor can partition a JBOD or RAID set into one or more LUNs. It can restrict access of a particular LUN to one or more server connections. Each connection is referenced by the server HBA's WWN, and it might also require defining the operating system in the connection tables to adjust how the storage array controller presents Fibre Channel and SCSI commands to a particular server.
- **HBA** – The host bus adapter connects the ESX/ESXi host to the Fibre Channel network. It is required, along with cables attached to the Fibre Channel switch ports. A minimum of two HBA adapters are used for fault-tolerant configurations. Virtual machines see standard SCSI connections and are not aware of the underlying SAN being accessed.

- Fibre Channel switches – One or more Fibre Channel (FC) switches form the Fibre Channel fabric. The FC fabric interconnects multiple nodes. The FC switches form packets from the FC messages and add the source and destination addresses to each packet. The FC switch might have to be updated by flash upgrade to firmware to resolve interoperability issues and to add new features.

Slide 6-21



Zoning is especially important in environments where physical Windows servers are accessing the SAN, because Windows operating systems typically write a disk signature on any storage volumes they see. These volumes might, in fact, be in use by non-Windows systems.

WWNs are assigned by the manufacturer of the SAN equipment. HBAs and SPs have WWNs. WWNs are used by SAN administrators to identify your equipment for zoning purposes.

The SP or the hosts themselves might also implement LUN masking, which controls LUN visibility per host. An ESX/ESXi host offers a mechanism for LUN masking. Although LUN masking can be done within the ESX/ESXi host, LUN masking is normally performed at the SP level and, with newer switches, can also be done at a switch/fabric level. Though it could be done at the host level, it normally is not, for the sake of security and data integrity. If a LUN is masked, the SP does not tell the host the LUN exists, nor does it allow any communication with it.

Accessing Fibre Channel Storage

Slide 6-22

- > Install Fibre Channel adapters.
- > During the boot sequence, the adapters are recognized by the ESX/ESXi host.

Storage Adapters

Refresh

Rescan...

Device	Type	WWN
ISP2432-based 4Gb Fibre Channel to PCI Express HBA		
vmhba1	Fibre Channel	50:01:43:80:02:ae:b2:05 50:01:43:80:02:ae:b2:04
vmhba2	Fibre Channel	50:01:43:80:02:ae:b2:07 50:01:43:80:02:ae:b2:06

- > Clicking the **Rescan** link allows the ESX/ESXi host to rescan all host bus adapters for new storage devices.
 - An ESX/ESXi host supports up to 256 LUNs and 16 HBAs.

All supported PCI devices (SCSI, Fibre Channel, Ethernet, iSCSI, and so on) are assigned to the VMkernel and are recognized by the VMkernel when the ESX/ESXi host boots. ESX/ESXi supports 256 LUNs, found in the range of 0–255. However, during installation, the ESX installer can see only the first 128 LUNs.

To display a list of storage adapters, select your host in the inventory, click the **Configuration** tab, and then click the **Storage Adapters** link.

Viewing Fibre Channel Storage Information

Slide 6-23

The Storage Views tab provides information about all SCSI adapters and NAS mounts.

View: Reports Maps

Show all SCSI Volumes (LUNs) ▾

- Show all Virtual Machines
- Show all Datastores
- ☒ Show all SCSI Volumes (LUNs)
- Show all SCSI Paths
- Show all SCSI Adapters
- Show all SCSI Targets (Array Ports)
- Show all NAS Mounts

Linking Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permissions Maps **Storage Views** Hardware Status
Last Update

Storage Views are generated periodically and may be out of date. To update to the most recent inventory, please click "Update..."

View: Reports Maps

Show all SCSI Volumes (LUNs) ▾

SCSI ID, Canonical Name or Runtime Name c

SCSI ID	Canonical Name	Runtime Name	Lun	Status	Host status	Size	Volume Name	Vendor	Device type
0000000000766d6...	mpx.vmhba0:C0:T0:L0	vmhba0:C0:T0:L0	0	Up	Up	136.70 GB	Local VMware Disk (mpx.vmhba0:C0:T0:L...	VMware	Disk
020000000050060...	naa.50060160c1e0eb...	vmhba1:C0:T0:L0	0	Up	Up	0.00 B	DGC Fibre Channel Disk (naa.50060160c1...	DGC	Disk
020006000060060...	naa.60060160d2b020...	vmhba1:C0:T0:L6	6	Up	Up	10.00 GB	DGC Fibre Channel Disk (naa.60060160d2...	DGC	Disk
020015000060060...	naa.60060160d2b020...	vmhba1:C0:T0:L21	21	Up	Up	10.00 GB	DGC Fibre Channel Disk (naa.60060160d2...	DGC	Disk
020016000060060...	naa.60060160d2b020...	vmhba1:C0:T0:L22	22	Up	Up	10.00 GB	DGC Fibre Channel Disk (naa.60060160d2...	DGC	Disk
020019000060060...	naa.60060160d2b020...	vmhba1:C0:T0:L25	25	Up	Up	100.00 GB	DGC Fibre Channel Disk (naa.60060160d2...	DGC	Disk

The **Storage Views** tab allows you to review associations between all storage entities available in VMware vCenter™ Server and analyze storage usage. The storage usage data appears as reports and storage topology maps on the **Storage Views** tab. Use the Reports view to analyze storage space utilization and availability, multipathing status, and other storage properties of the selected object and items related to it.

Use the **Storage Views** tab to view information about your Fibre Channel storage. You can also view the relationship between various entities and storage, for example:

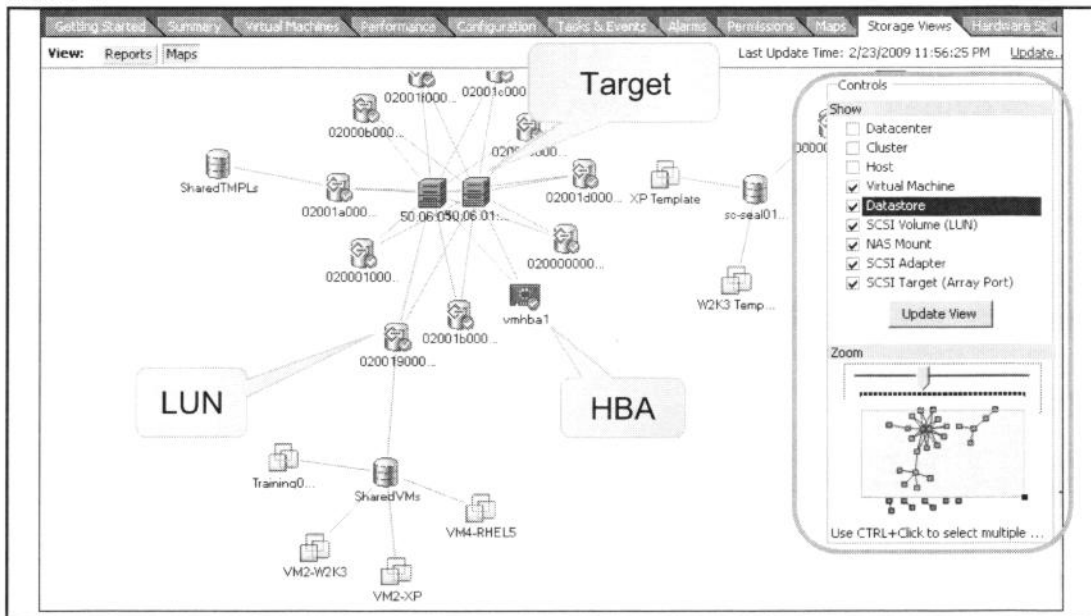
- Datastore to virtual machine or host
- Virtual machine/host/cluster to datastore
- Virtual machine to SCSI volume, path, adapter, or target

The reports provided are searchable, and the views are customizable in that you can choose what pieces of information to display by right-clicking the header bar of the report and selecting the desired values to display.

Reports are automatically updated every 30 minutes. You can manually update the reports by clicking the **Update** link.

Viewing Fibre Channel Storage Maps

Slide 6-24



Storage maps are an easy way to visually represent relationships between selected inventory objects and storage. For example, you can view what targets a virtual machine can see, or how many paths a virtual machine has to a storage device. Maps can assist in troubleshooting by showing problem entities.

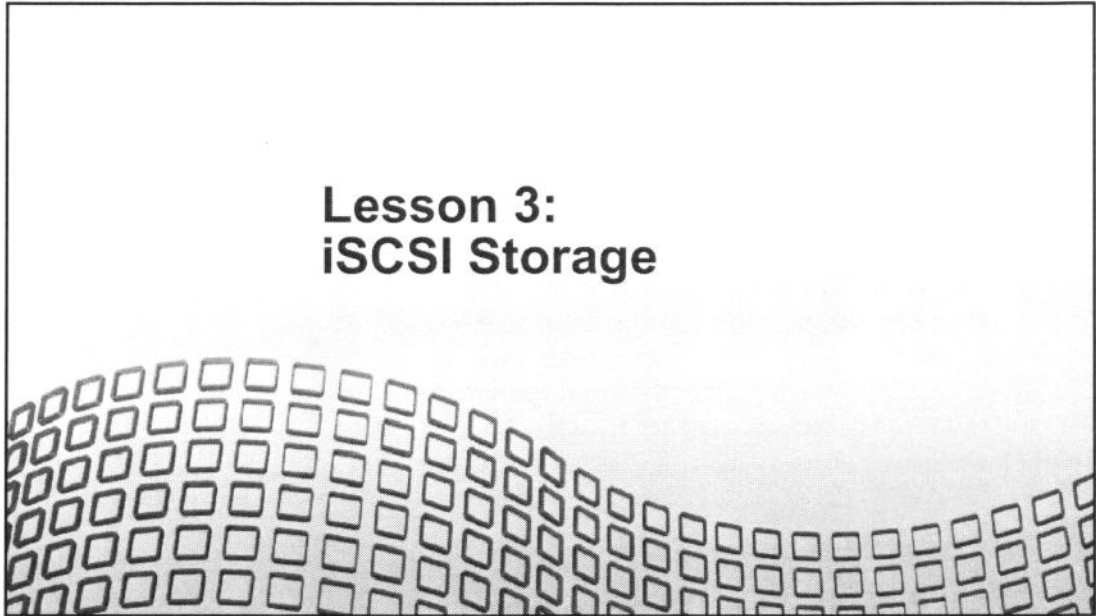
Lesson Summary

Slide 6-25

- Fibre Channel storage devices can be used to hold VMFS datastores or raw data.
- Clicking the **Rescan** link allows the ESX/ESXi host to rescan all HBAs for new storage devices.
- Fibre Channel storage information is available from the reports provided in the **Storage Views** tab.

Lesson 3: iSCSI Storage

Slide 6-26



Lesson Objectives

Slide 6-27

- > Describe uses of iSCSI storage with ESX/ESXi
- > Describe iSCSI components and addressing
- > Configure iSCSI initiators
- > View iSCSI storage information

Using iSCSI with ESX/ESXi

Slide 6-28

Uses of iSCSI SAN LUNs:

- > VMFS datastores to hold virtual machines, ISO images, and templates
- > RDMs to hold a virtual machine's raw data
- > Supports vSphere features such as VMotion, VMware HA, and DRS
- > To boot ESX from a SAN LUN (hardware initiator only)

ESX/ESXi supports:

- > iSCSI over a 10GbE interface

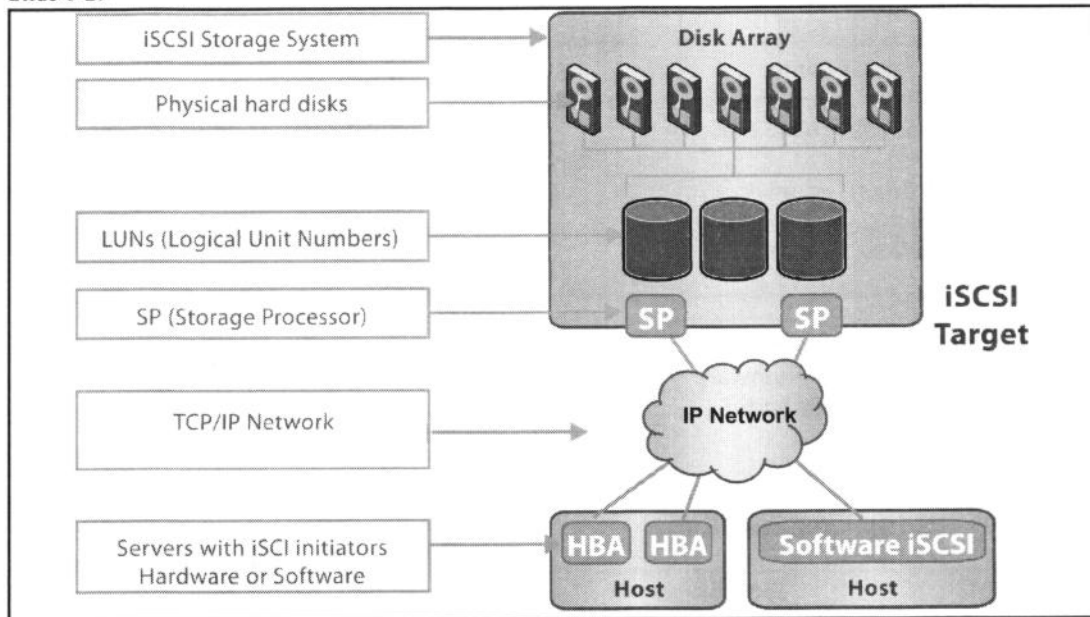
iSCSI storage is commonly used for VMFS datastores. VMFS datastores are used to hold virtual machines' files, ISO images, templates, and RDMs that point to raw iSCSI volumes.

VMFS datastores on an iSCSI SAN can be shared across multiple ESX/ESXi hosts. As a result, iSCSI can play an important role in supporting vSphere features like VMotion, VMware HA, DRS, and Consolidated Backup.

Installing and booting an ESX host from iSCSI storage is supported.

iSCSI Components

Slide 6-29



An iSCSI SAN consists of an iSCSI storage system, which contains one or more LUNs and one or more SPs. Communication between the host and the storage array occurs over a TCP/IP network.

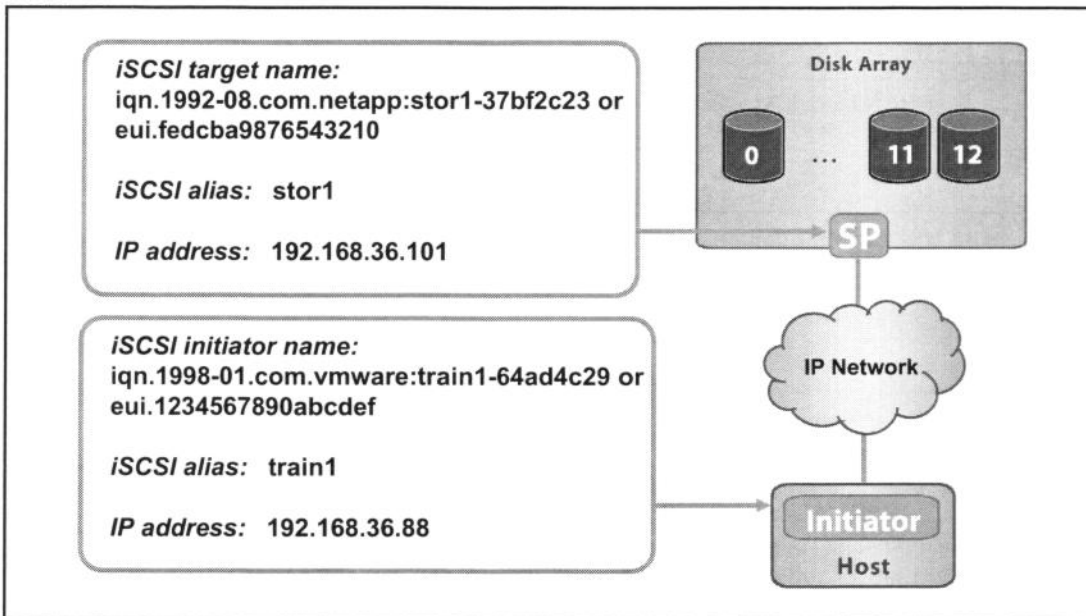
The ESX/ESXi host is configured with an iSCSI initiator. An initiator can be hardware-based, in which case the initiator is an iSCSI HBA. Or it can be software-based, known as the iSCSI software initiator.

An initiator transmits SCSI commands over the IP network. A target receives SCSI commands from the IP network. You can have multiple initiators and targets in your iSCSI network. iSCSI is SAN-oriented in that the initiator finds one or more targets, a target presents LUNs to the initiator, and the initiator sends it SCSI commands. An initiator resides in the ESX/ESXi host, while targets reside in the storage arrays supported by the ESX/ESXi host.

LUN masking is also available in iSCSI and works as it does in Fibre Channel. Ethernet switches do not implement zoning like Fibre Channel switches. Instead, you can create zones using VLANs.

iSCSI Addressing

Slide 6-30



The main addressable, discoverable entity in iSCSI is an iSCSI node. An iSCSI node can be an initiator or a target. An iSCSI node requires a name for the purpose of identification, so that iSCSI storage resources can be managed regardless of location (address).

The iSCSI name can use one of the following formats: IQN and extended unique identifier (EUI).

The IQN can be up to 255 characters long. The naming convention is as follows:

- The prefix “iqn”
- A date code specifying the year and month in which the organization registered the domain or subdomain name used as the naming authority string
- The organizational naming authority string, which consists of a valid, reversed domain or subdomain name
- Optionally, a colon (:), followed by a string of the assigning organization’s choosing, which must make each assigned iSCSI name unique

The EUI naming convention is as follows:

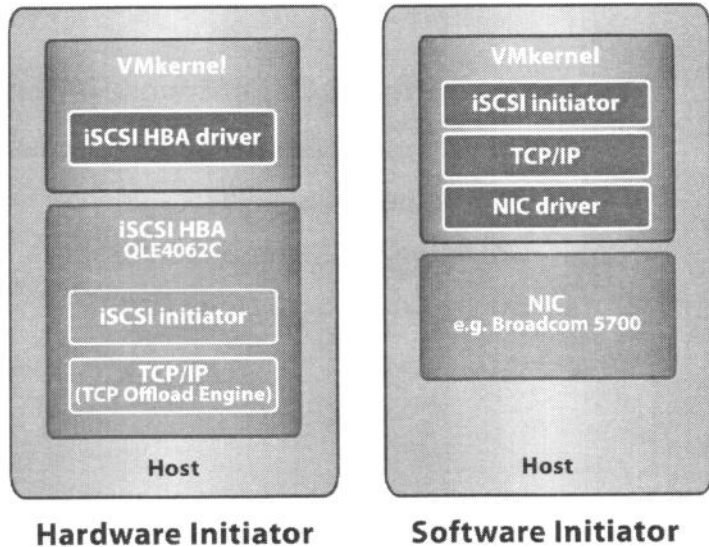
- The prefix “eui”
- A 16-character name. The name includes 24 bits for company name assigned by the IEEE and 40 bits for a unique ID, such as a serial number.

iSCSI Initiators

Slide 6-31

ESX/ESXi hosts use iSCSI initiators to access remote targets.

- **Hardware initiator:** An iSCSI HBA responsible for all iSCSI processing and management
- **Software initiator:** Code built into the VMkernel that allows ESX/ESXi to connect to the iSCSI storage device



The hardware-based iSCSI initiator allows you to use a third-party adapter capable of accessing iSCSI storage over TCP/IP. This iSCSI initiator handles all iSCSI processing and management for your ESX/ESXi host. The hardware initiator off-loads the iSCSI network traffic load from the VMkernel's networking stack. You must install and configure the hardware iSCSI adapter before you set up a datastore that resides on an iSCSI storage device.

The software-based iSCSI initiator allows you to use a standard network adapter to connect your ESX/ESXi host to a remote iSCSI target on the IP network. The software iSCSI initiator built into the ESX/ESXi host facilitates this connection communicating with the network adapter through the network stack.

For both initiators, hardware and software, the guest operating system never specifically sees iSCSI network traffic. Because the guest operating system is not aware of the underlying storage, it sees only virtual disk SCSI I/O traffic.

An ESX/ESXi host does not support both hardware and software initiators running simultaneously.

For a list of iSCSI storage arrays supported for iSCSI software and hardware initiators, see *Storage/SAN Compatibility Guide* at <http://www.vmware.com/support/pubs>.

Steps to Configure Software iSCSI

Slide 6-32

To configure the iSCSI software initiator:

1. Configure a VMkernel port for accessing IP storage.
2. Enable the iSCSI software adapter.
3. Configure iSCSI target addresses.
4. Configure iSCSI security (CHAP).

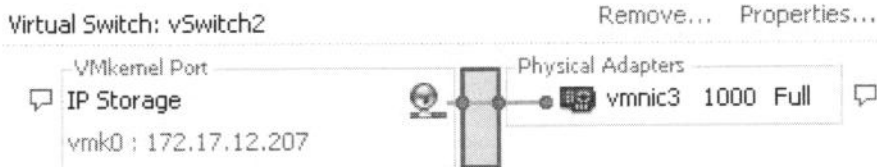
To configure the iSCSI software initiator

1. Create a VMkernel port, which is used by the ESX/ESXi host to access iSCSI storage.
2. Enable the software iSCSI initiator so that your ESX/ESXi host can use it.
3. Configure one or more target discovery addresses so that the iSCSI initiator can determine which storage resource on the network is available for access.
4. Configure Challenge Handshake Authentication Protocol (CHAP) to verify the legitimacy of initiators that access targets on the network.

Configuring Network for Software iSCSI

Slide 6-33

Create a VMkernel port on a vSwitch for access to IP storage (for example, iSCSI and NFS).



To optimize your vSphere networking setup:

- Separate network services like iSCSI and NFS access.
 - Physical separation is preferred.
 - If not possible, use VLANs.

Networking configuration for software iSCSI involves creating a VMkernel port on a virtual switch (standard or distributed) that would handle your iSCSI traffic.

Depending on the number of physical adapters you want to use for the iSCSI traffic, networking setup can be different:

- If you have one physical network adapter, you create one VMkernel port on a virtual switch.
- If you have two or more physical network adapter for iSCSI, you can use these adapters for host-based multipathing. Multipathing is discussed in a later module.

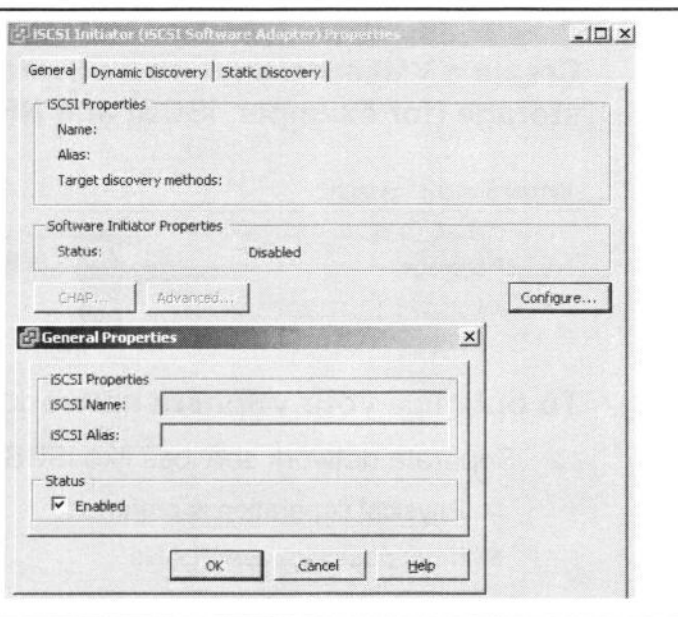
To add a VMkernel port to a virtual switch, go to the host's **Configuration** tab and select **Networking** from the **Hardware** panel.

It is a best practice to isolate your iSCSI network from other networks for performance and security reasons. Physically separate the networks. If that is not possible, logically separate them from each other on a single virtual switch using VLANs.

Enabling the iSCSI Software Adapter

Slide 6-34

In the Storage Adapters link of the ESX/ESXi host's Configuration tab, click Properties.



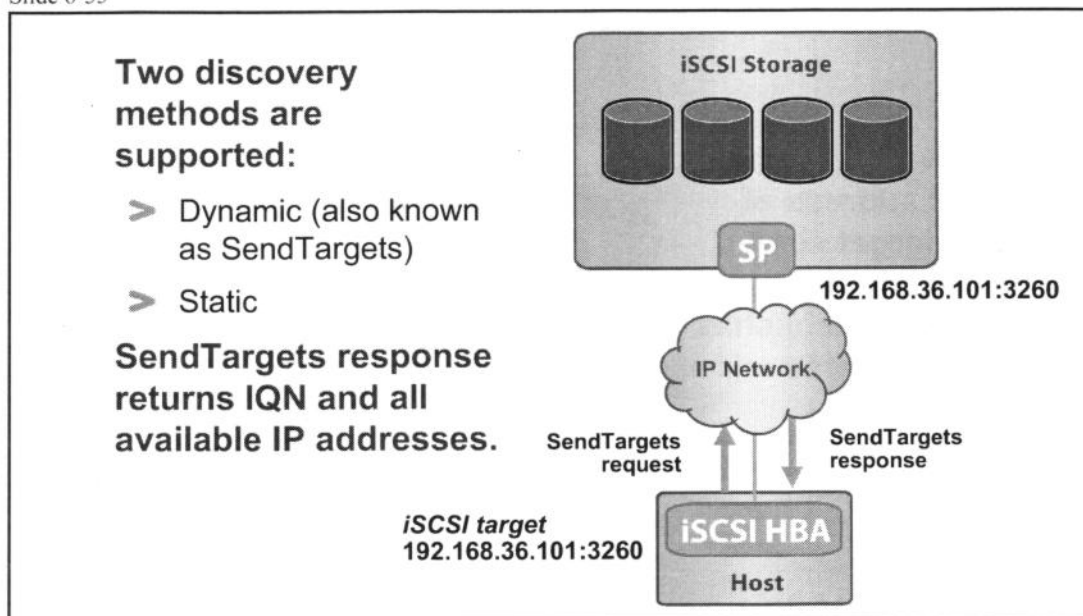
Enable the iSCSI software initiator so that your ESX/ESXi host can use it. To do this, go to the **Storage Adapters** link in your host's **Configuration** tab. Select **iSCSI Software Adapter** from the **Device** list, then click the **Properties** link in the **Details** pane below. The iSCSI Initiator Properties dialog box appears.

The iSCSI Initiator Properties dialog box displays the status of the software initiator. Click **Configure**. In the General Properties dialog box, select the **Enabled** check box.

By enabling the software initiator, a default iSCSI name is chosen for you which follows the IQN naming convention.

iSCSI Target-Discovery Methods

Slide 6-35



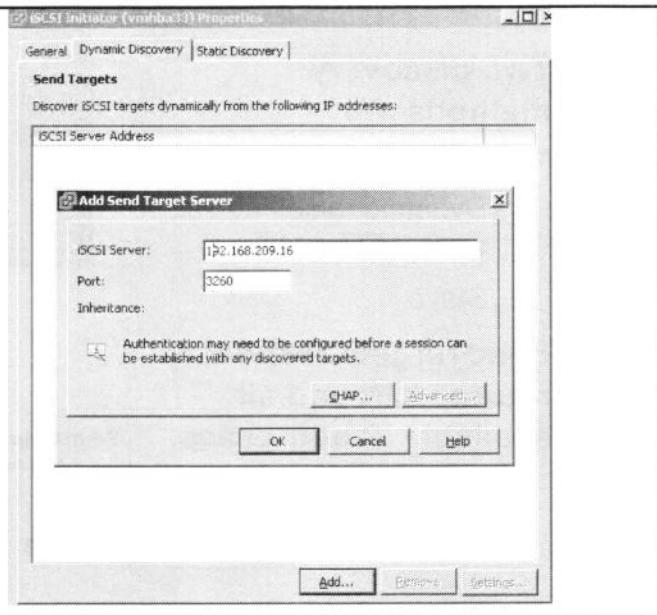
The ESX/ESXi host supports these discovery methods:

- Dynamic discovery – Also known as SendTargets discovery. Each time the initiator contacts a specified iSCSI server, it sends the SendTargets request to the server. The server responds by supplying a list of available targets to the initiator. The names and IP addresses of these targets appear on the **Static Discovery** tab. If you remove a static target added by dynamic discovery, the target might be returned to the list the next time a rescan happens, the HBA is reset, or the host is rebooted.
- Static discovery – The initiator does not need to perform any discovery. The initiator in advance knows all targets it will be contacting and uses their IP addresses and domain names to communicate with them.

Configuring iSCSI Target Addresses

Slide 6-36

In the **Dynamic Discovery** tab, enter the IP address of each target server for which the initiator establishes a discovery session.



To configure iSCSI target addresses, in the iSCSI Initiator Properties dialog box, click the **Dynamic Discovery** tab. Click **Add** and enter the IP address of an iSCSI target. Port 3260 is used to receive transactions from your iSCSI storage devices.

The target address will appear in both the **Dynamic Discovery** tab and **Static Discovery** tab.

You cannot change the IP address, iSCSI name, or port number of an existing target. If you need to make any changes, remove the existing target and add a new one.

iSCSI Security: CHAP

Slide 6-37

iSCSI initiators can use Challenge Handshake Authentication Protocol (CHAP) for authentication purposes.

ESX/ESXi supports unidirectional and bidirectional CHAP authentication.

- Unidirectional – Target authenticates initiator, but initiator does not authenticate target.
- Bidirectional (or mutual) – Target authenticates initiator, and initiator authenticates target.

ESX/ESXi also supports per-target CHAP authentication.

- This enables you to configure different credentials for each target.

Because the IP networks that the iSCSI technology uses to connect to remote targets do not encrypt the data they transport, it is necessary to ensure security of the connection. It is a best practice that all devices on the network implement CHAP for a secure connection.

ESX/ESXi supports the following CHAP authentication methods:

- One-way CHAP – In one-way, or unidirectional, CHAP authentication, the target authenticates the initiator, but the initiator does not authenticate the target. You must specify the CHAP secret so that your initiators can access the target.
- Mutual CHAP (software iSCSI only) – In mutual, or bidirectional, CHAP authentication, an additional level of security enables the initiator to authenticate the target. You must specify different target and initiator secrets.

CHAP uses a three-way handshake algorithm to verify the identity of your host and, if applicable, of the iSCSI target when the host and target establish a connection. The verification is based on a predefined private value, or CHAP secret, that the initiator and target share.

ESX implements CHAP as defined in RFC 1994.

Configuring iSCSI Security: CHAP

Slide 6-38

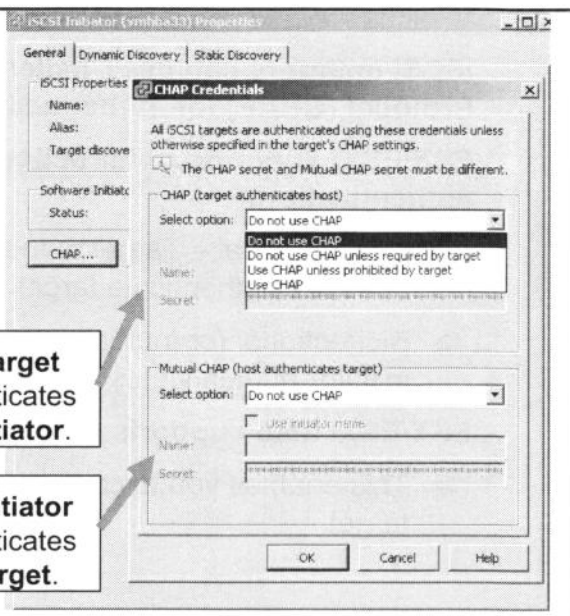
By default, CHAP is not configured.

CHAP options:

- Do not use CHAP
- Do not use CHAP unless required by target
- Use CHAP unless prohibited by target
- Use CHAP

The **target** authenticates the **initiator**.

The **initiator** authenticates the **target**.



ESX/ESXi supports CHAP authentication at the adapter level. In this case, all targets receive the same CHAP secret from the iSCSI initiator. For software iSCSI, ESX/ESXi also supports per-target CHAP authentication.

To configure CHAP on the ESX/ESXi host at the adapter level, in the iSCSI Initiator Properties dialog box, go to the **General** tab and click **CHAP** to display the CHAP Credentials dialog box.

When you set the CHAP parameters, you select a CHAP option:

- **Do not use CHAP** – The host does not use CHAP authentication. Select this option to disable authentication if it is currently enabled.
- **Do not use CHAP unless required by target** – The host prefers a non-CHAP connection, but allows a CHAP connection if the target requires it (iSCSI software initiator only).
- **Use CHAP unless prohibited by target** – The host prefers CHAP, but uses non-CHAP connections when the target prohibits it.
- **Use CHAP** – The host requires successful CHAP authentication (iSCSI software initiator only). Also, you must select this option in order to configure mutual CHAP.

Before configuring CHAP, check whether CHAP is enabled at the iSCSI storage system and check the CHAP authentication method the system supports. If it is enabled, you need to enable it for your initiators, making sure that the CHAP authentication credentials match the credentials on the iSCSI storage.

Steps to Configure Hardware iSCSI

Slide 6-39

To configure the iSCSI hardware initiator:

1. Install the iSCSI hardware adapter.
2. Modify iSCSI name and configure iSCSI alias.
3. Configure iSCSI target addresses.
4. Configure iSCSI security (CHAP).

The steps to configure the iSCSI hardware initiator are the following:

- Before you begin configuring the hardware iSCSI initiator, make sure that the iSCSI HBA is successfully installed and appears on the list of initiators available for configuration (host's **Configuration** tab, **Storage Adapters** link). If the initiator is installed, you can view its properties.
- If necessary, modify the iSCSI name and configure an iSCSI alias. Make sure that the iSCSI name is formatted properly. Otherwise, some storage devices might not recognize the hardware initiator. If you change the iSCSI name, it will be used for new iSCSI sessions. For existing sessions, new settings will not be used until logout and a subsequent login.
- Configure one or more target discovery addresses so that the iSCSI initiator can determine which storage resource on the network is available for access.
- Configure CHAP to verify the legitimacy of initiators that access targets on the network. Only one-way CHAP is available for hardware initiators.

The steps to configure the target discovery addresses and CHAP security are the same for the hardware initiator as they are for the software initiator.

Viewing iSCSI Information

Slide 6-40

Storage link in the Configuration tab

Storage Adapters link in the Configuration tab

View: Datastores Devices

Datastores

Identification	Status	Device	Capacity	Free	Type	Last Update
Local06	Normal	Local VMware Disk...	136.25 GB	122.08 GB	vmfs3	2/1/2009 11:06:15 AM
SharedVMs	Normal	DGC Fibre Channel...	99.75 GB	79.35 GB	vmfs3	2/1/2009 11:06:15 AM
iSCSILUN	Normal	IET iSCSI Disk (t...	1.75 GB	1.47 GB	vmfs3	2/1/2009 11:06:15 AM

Storage Adapters

Device	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:sc-rat01-5f7f8b6f

Details

vmhba33

Model: iSCSI Software Adapter

ISCSI Name: iqn.1998-01.com.vmware:sc-rat01-5f7f8b6f

ISCSI Alias:

Connected Targets: 1 Devices: 1 Paths: 1

View: Devices Paths

Name	Runtime Name	LUN	Type	Transport	Capacity	Owner
IET iSCSI Disk (t10.945445000000...	vmhba33:C0:T0:L1	1	disk	iSCSI	2.00 GB	NMP

The **Storage** link and **Storage Adapters** link in the **Configuration** tab display all storage devices available to the selected ESX/ESXi host. The **Storage** link lists local and networked storage that the host accesses using storage adapters. It also lists the datastore names carved on those storage. The **Storage Adapters** link lists all available adapters, their types, such as Fibre Channel, SCSI, or iSCSI storage.

Another way to view iSCSI storage information (not shown above) is to view the various reports in your host's **Storage Views** tab.

Lab 6

Slide 6-41

In this lab, you will configure access to an iSCSI datastore.

1. Create a VMkernel port on the standard switch, vSwitch0.
2. Configure the iSCSI software adapter.
3. View iSCSI storage information.

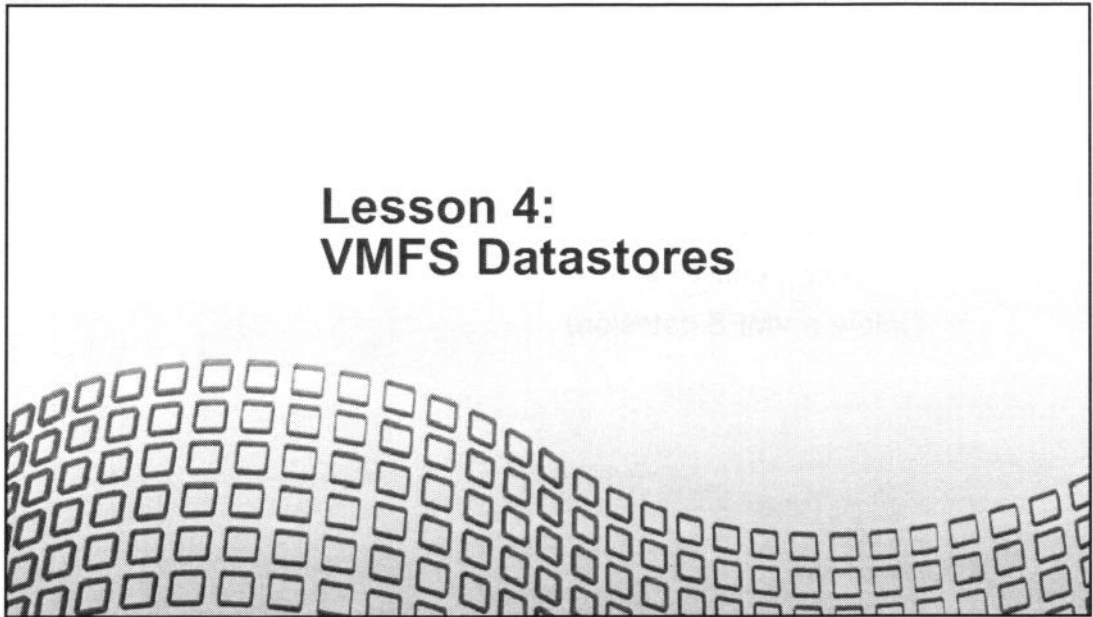
Lesson Summary

Slide 6-42

- > ESX/ESXi hosts support both hardware initiators and software initiators.
- > For the iSCSI software initiator, a VMkernel port on a distributed switch or standard switch must be configured.
- > iSCSI security is achieved by isolating the iSCSI network from other networks as well as by configuring CHAP.

Lesson 4: VMFS Datastores

Slide 6-43



Lesson Objectives

Slide 6-44

- > Create a VMFS datastore
- > Grow a VMFS datastore
 - Using Volume Grow
 - Using Extent Grow
- > Delete a VMFS datastore

Using a VMFS with ESX/ESXi

Slide 6-45

Use VMFS datastores whenever possible:

- > VMFS is optimized for storing and accessing large files.
- > A VMFS can have a maximum volume size of 64TB.
- > NFS datastores are great for storing virtual machines. However, some functions are not supported.
- > Use RDMs if your virtual machine
 - Is performing SAN snapshotting
 - Is clustered to a physical machine using Microsoft Cluster Service (MSCS)
 - Has large amounts of data that you do not want to convert into a virtual disk

VMFS datastores primarily serve as repositories for virtual machines' files. A VMFS is optimized for storing and accessing large files such as virtual disks and memory images of suspended virtual machines. The maximum size of a VMFS is 64TB.

You can certainly use an NFS datastore to store your virtual machines. However, not all functions are supported. For example, you cannot store an RDM on an NFS datastore (an RDM must be located on a VMFS), and you cannot cluster a virtual machine that resides on an NFS datastore using Microsoft Cluster Service.

As for RDMs, choose RDMs over VMFS datastores if a virtual machine is using SAN snapshot applications, a virtual machine is clustered with a physical machine using Microsoft Cluster Service, or you want to keep the virtual machine's data on a raw disk instead of converting it to a virtual disk because, for example, the data disk is very large. Otherwise, use a VMFS datastore to store your virtual machines to take advantages of features like template deployment as well as for portability.

Creating a VMFS

Slide 6-46

To create a VMFS, use the Add Storage wizard.

Add Storage

Select Disk/LUN

Select a LUN to create a datastore or expand the current one

Select Disk/LUN

Current Disk Layout

Properties

Formatting

Ready to Complete

Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c...

Name	Path ID	LUN	Capacity	VMFS Label
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L1	1	10.00 GB	
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L12	12	10.00 GB	

Select LUN.

Specify datastore name.

Specify datastore size – use full or partial LUN

To create a VMFS datastore, select your host in the inventory, then click the **Configuration** tab. Select **Storage** from the **Hardware** panel. Click the **Add Storage** link. The Add Storage wizard guides you through the configuration steps.

First, select **Disk/LUN** as the storage type. Then provide the following information for your VMFS, shown above:







- Select a device to use for your datastore. Select the device that does not have a datastore name displayed in the **VMFS Label** column. The name present in the **VMFS Label** column indicates that the device contains a copy of an existing VMFS datastore.
- The Current Disk Layout page opens. If the disk you are formatting is blank, the Current Disk Layout page presents the entire disk space to you for storage configuration. If the disk is not blank, you can choose to use the entire device or just use the free space on the device.
- Enter a datastore name. Choose a descriptive name, one that reflects the purpose or function of the datastore, or if desired, the hardware characteristics of the device itself.
- Specify the maximum size of the VMFS datastore.

After the VMFS is created, view its properties by selecting the VMFS in the **Storage** list (on the host's **Configuration** tab).

Viewing VMFS Datastores

Slide 6-47

Storage link in the Configuration tab

View: Datastores Devices						
Datastores						
Identification	Status	Device	Capacity	Free	Type	Last Update
 nfs_iso_library...	 Normal	nfs-goose-a:/iso	5.77 GB	2.43 GB	NFS	1/29/2009 10:05:36 AM
 Local06	 Normal	Local VMware Disk ...	136.25 G	124.08 G	vmfs3	1/29/2009 10:05:36 AM
 SharedVMs	 Normal	DGC Fibre Channel ...	99.75 GB	78.85 GB	vmfs3	1/29/2009 10:05:36 AM

Storage Views tab

View: Reports Maps					
Show all Datastores ▾					
Datastore	File system type	Connectivity Status	Multipathing Status	Capacity	Free Space
nfs_iso_library		Up		5.77 GB	2.43 GB
SharedTMPLs (2)		Up	Partial/No Redundancy	35.75 GB	15.77 GB
Local06		Up	Partial/No Redundancy	136.25 GB	124.08 GB

There are a couple of ways to view information about your VMFS datastores. One way is to use the **Storage** link in your host's **Configuration** tab.

Another way is to view the Show all Datastores report in your host's **Storage Views** tab.

Browsing Datastore Contents

Slide 6-48

Right-click the datastore in either the host's Summary tab or the Storage link in the Configuration tab.

Datastores

Identification	Status	Device
nfs_iso_library...	Normal	nfs-goose-a:/iso
Local06	Normal	Local VMware Dis
SharedV...		

Datastore Browser - [Local06]

esxconsole-4978234c...
Greg06-1
GregTemplate
SampleVM06

Name	Size	Type	Path
esxconsole-4978234c...		Folder	[Local06] esxconsole-4978234c-cda...
Greg06-1		Folder	[Local06] Greg06-1
GregTemplate		Folder	[Local06] GregTemplate
SampleVM06		Folder	[Local06] SampleVM06

The **Datastores** pane of the **Configuration** tab lists all datastores currently configured for the ESX/ESXi host. To display the **Datastores** pane, select your host in the inventory, click the **Configuration** tab, then click the **Storage** link. From the **Datastores** pane you can also browse the contents of a datastore. To do this, right-click the datastore, then choose **Browse Datastore**.

In the example above, the contents of the VMFS datastore named Local06 are displayed. The contents are the virtual machines' files, where each virtual machine's files are located in its own folder.

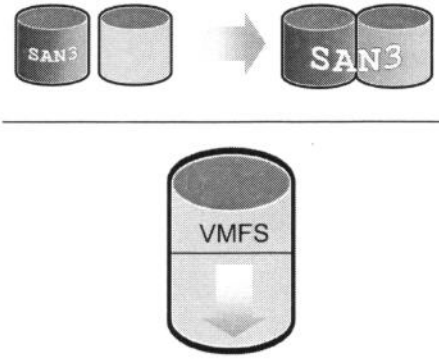
Growing a VMFS

Slide 6-49

Grow a VMFS to give it more space or possibly to improve performance.

Two ways to grow a VMFS:

- > **Extent Grow** – This feature allows you to dynamically add a new extent to a VMFS.
- > **Volume Grow** – This feature allows you to dynamically expand a VMFS on the volume partition on which it is located.



The diagram illustrates the process of growing a VMFS. At the top, two cylinders labeled 'SAN3' are shown, with an arrow pointing to a single, larger cylinder also labeled 'SAN3', representing the consolidation of multiple extents into one. Below this, a vertical cylinder labeled 'VMFS' is shown, with a downward-pointing arrow indicating its expansion into the volume partition below it.

You can grow but you cannot shrink a VMFS datastore!

When you need to create new virtual machines on a datastore, or when the virtual machines running on this datastore require more space, you can dynamically increase the capacity of a VMFS datastore.

Use one of the following methods:

- **Extent Grow** – An extent is a partition on a LUN. You can add a new extent to any existing VMFS datastore. The datastore can stretch over multiple extents, up to 32.
- **Volume Grow** – Grow an extent in an existing VMFS datastore. Only extents with free space immediately after them are expandable. As a result, rather than adding the new extent, you can grow the existing extent so that it fills the available adjacent capacity.

Volume Grow versus Extent Grow

Slide 6-50

	Volume Grow	Extent Grow
VM power state	On	On
Newly provisioned LUN	No	Yes
Existing array-expanded LUN	Yes	Yes
Limits	An extent can be grown any number of times, up to 2TB.	A datastore can have up to 32 extents, each up to 2TB.
New partition	No	Yes
VM availability impact	None, if datastore has only one extent.	Introduces dependency on first extent.

Here is a comparison between Volume Grow and Extent Grow:

- There is no need to power off virtual machines when performing Volume Grow or Extent Grow.
- When the LUN is newly provisioned, the administrator cannot perform Volume Grow, but Extent Grow can be utilized to grow VMFS datastore capacity.
- Volume Grow and Extent Grow can both be performed on an existing array that has expanded LUN.
- Each extent can be grown up to a maximum of 2TB. The maximum number of extents on which the datastore can stretch is 32.
- With Volume Grow, no new partition is added. But with extent grow, a new partition is added.
- Virtual machine availability impact refers to what happens to virtual machine availability when Volume Grow and Extent Grow features are used. With Volume Grow, availability is not impacted. However with extents, there is a dependency on the first extent. This first extent contains the metadata for the entire extent set. If that master LUN is lost, it could cause a loss of all data on the entire extent set.

The method you choose to grow your VMFS with depends on what you want to accomplish.

For example, one reason for using Extent Grow instead of Volume Grow is to create a VMFS greater than 2TB in size. The maximum size of a VMFS extent is 2TB. If your VMFS currently

consists of one extent, additional extents must be added if you want to increase the size of your VMFS past 2TB. For example, a 6TB VMFS is made of three extents.

Here is an example of using Volume Grow instead of Extent Grow: Your storage administrator has given you a 50GB LUN on which you format a VMFS. Over time, your VMFS fills up and you ask your storage administrator to grow the LUN to 100GB. After the underlying LUN is increased (using array management utilities), you use Volume Grow to dynamically grow the VMFS to use the newly available space on the LUN. By starting out with a smaller LUN and growing as needed, you can prevent wasting disk space as well as money.

Volume Grow of RDMs is not supported. In other words, if you grow an RDM's underlying LUN on the array, you still have to remove the RDM and re-create it to pick up the new size attributes.

Before Growing a VMFS

Slide 6-51

In general, before making any changes to your storage allocation:

- > Perform a rescan to ensure that your host sees the most current storage.
- > Quiesce I/O on all disks involved.
- > Note the unique identifier of the volume that you want to grow.

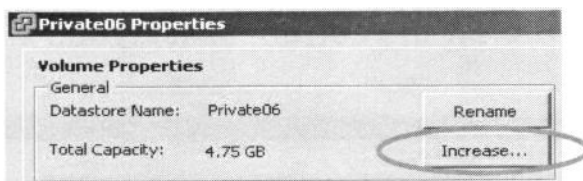
In general, before making any storage allocation changes, such as growing a VMFS, it is a good practice to perform a rescan to ensure that your host sees the most current storage view *before* making any changes. Also, for maximum safety, I/O should be quiesced on all disks involved in extent growth or when resizing a volume using array expansion. Finally, note the unique identifier of the volume you want to grow because you will need that information when prompted by the wizard.

Using Volume Grow: Increase Capacity

Slide 6-52

To grow a VMFS within a LUN, click Properties.

Click Increase to launch the Increase Datastore Capacity wizard.



The selected LUN already contains a datastore, but is also expandable.

Increase Datastore Capacity

Extent Device

Select a LUN to create a datastore or expand the current one

Extent Device

Current Disk Layout:

Extent Size:

Ready to Complete

Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c...

Name	Path ID	LUN	Capacity	Expandable
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L6	6	10.00 GB	No
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L29	29	1.00 GB	No
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L22	22	10.00 GB	No
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L21	21	10.00 GB	Yes
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L27	27	1.00 GB	No
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L28	28	1.00 GB	No

To grow a VMFS using Volume Grow, go to your host's **Configuration** tab and select **Storage** in the **Hardware** panel. Select the VMFS you want to grow and click the **Properties** link in the **Details** pane.

In the VMFS Properties dialog box, click **Increase**. The Increase Datastore Capacity wizard appears.

On the Extent Device page, select the device for which the **Expandable** column reads Yes. Yes indicates that an extent of your datastore is deployed on this device and the extent is adjacent to free space.

Using Volume Grow: View Disk Layout

Slide 6-53

View the current disk layout.

Increase Datastore Capacity

Current Disk Layout
You can either expand an existing extent or partition and format a single block of free space as a new extent.

Extent Device
Current Disk Layout
Extent Size
Ready to Complete

Review the current disk layout:

Device	Capacity	Available	LUN
DGC Fibre Channel Disk (naa.60060160d...) Location /vmfs/devices/disks/naa.60060160d2b02000f24f097ad6b1dd11	10.00 GB	5.00 GB	21

Primary Partitions

	Capacity
✓ VMFS (DGC Fibre Channel Disk (naa.600601...)	4.99 GB
✓ Free space	5.00 GB

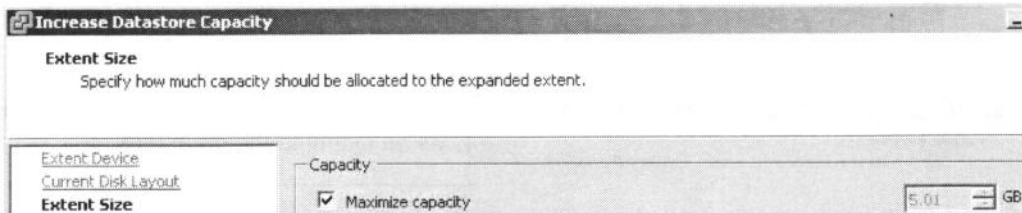
This LUN has a capacity of 10GB, 5GB of which is available.

Continuing with growing a VMFS using Volume Grow, the next page in the Increase Datastore Capacity wizard is Current Disk Layout. On this page, note the current capacity of the device and the available capacity. In the example above, the current capacity of the device is 10GB, of which 5GB is available. The **Primary Partitions** section shows that 4.99GB currently contains a VMFS and the remaining 5GB is free space.

Using Volume Grow: Specify Capacity

Slide 6-54

Select maximize capacity to use all remaining free space, or grow the VMFS by a specific size.



The VMFS Properties dialog box shows the new size.

Continuing with growing a VMFS using Volume Grow, the next page in the Increase Datastore Capacity wizard is Extent Size. To specify the new size, you can do one of the following:

- Leave the **Maximize capacity** check box selected, in which case the remaining free space will be used to grow the VMFS.
- Deselect the **Maximize capacity** check box and enter a specify size to which to grow the VMFS.

After the datastore capacity has been increased, the new size of the VMFS will be reflected in the VMFS Properties dialog box.

Using Extent Grow: Select LUN

Slide 6-55

To grow a VMFS within a LUN, click Properties.

Click Increase to launch the Increase Datastore Capacity wizard.

Increase Datastore Capacity

Extent Device
Select a LUN to create a datastore or expand the current one

Extent Device
Current Disk Layout
Extent Size
Ready to Complete

Name, Identifier, Path ID, LUN, Capacity, Expandable or VMFS Label c...	Name	Path ID	LUN	Capacity	Expandable
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L6	6	10.00 GB	No	
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L29	29	1.00 GB	No	
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L22	22	10.00 GB	No	
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L27	27	1.00 GB	No	
DGC Fibre Channel Disk (naa.60060...	vmhba1:C0:T0:L28	28	1.00 GB	No	

To grow a VMFS using Extent Grow, go to your host's **Configuration** tab and select **Storage** in the **Hardware** panel. Select the VMFS you want to grow and click the **Properties** link in the **Details** pane.

In the VMFS Properties dialog box, click **Increase**. The Increase Datastore Capacity wizard appears.

On the Extent Device page, select a device for which the **Expandable** column reads No.

The remaining pages of the wizard are similar to that of Volume Grow:

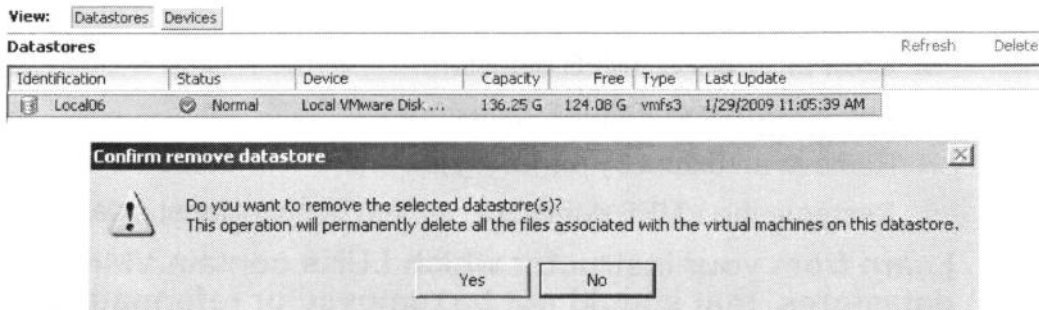
- The Current Disk Layout page allows you to view the total disk capacity and the amount of available capacity.
- The Extent Size page allows you to set the maximum capacity of the extent, whether it is the entire extent or part of the extent.

Deleting a VMFS

Slide 6-56

Use the Storage link in the Configuration tab to delete the VMFS.

Deleting a VMFS permanently deletes all the files associated with the virtual machines on the datastore.



You can delete any type of VMFS datastores, including copies of VMFS datastores that you have mounted without resignaturing. When you delete a datastore, it is destroyed and disappears from all hosts that have access to the datastore.

Before you delete a datastore, stop all virtual machines whose disks reside on the datastore.

To delete a VMFS datastore, click the **Storage** link in the host's **Configuration** tab. Right-click the VMFS datastore, then choose **Delete**. You will be prompted to confirm the datastore removal.

Lab 7

Slide 6-57

In this lab, you will work with VMFS datastores.

1. Display information about your shared storage.
2. View information about existing VMFS datastores.
3. Change the name of your local datastore.
4. Create a VMFS datastore.
5. Grow an existing VMFS datastore.
6. Add an extent to a VMFS datastore.
7. Remove an extent by removing the entire VMFS datastore.
8. Recreate the VMFS datastore, without the additional extent.

Learn from your instructor which LUNs contain VMFS datastores that should not be removed or reformatted.

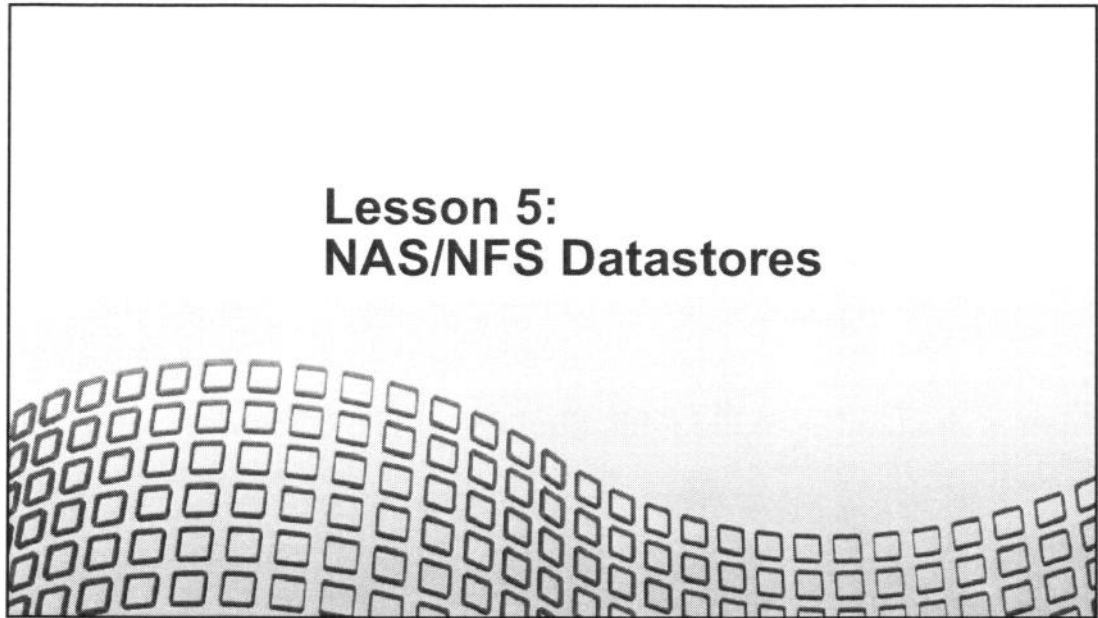
Lesson Summary

Slide 6-58

- Create a VMFS datastore on locally attached storage, a Fibre Channel SAN LUN, or an iSCSI LUN.
- Grow a VMFS within a volume using Volume Grow.
- Grow a VMFS by adding an extent using Extent Grow.
- When you delete a VMFS datastore, all data is destroyed on the datastore.

Lesson 5: NAS/NFS Datastores

Slide 6-59



Lesson Objectives

Slide 6-60

- > Describe NFS components and addressing
- > Create an NFS datastore
- > View the contents of a datastore
- > Unmount an NFS datastore

Using NAS/NFS with ESX/ESXi

Slide 6-61

NAS/NFS storage:

- > Is used to hold virtual machines, ISO images, and templates
- > Supports vSphere features like VMotion, VMware HA, and DRS

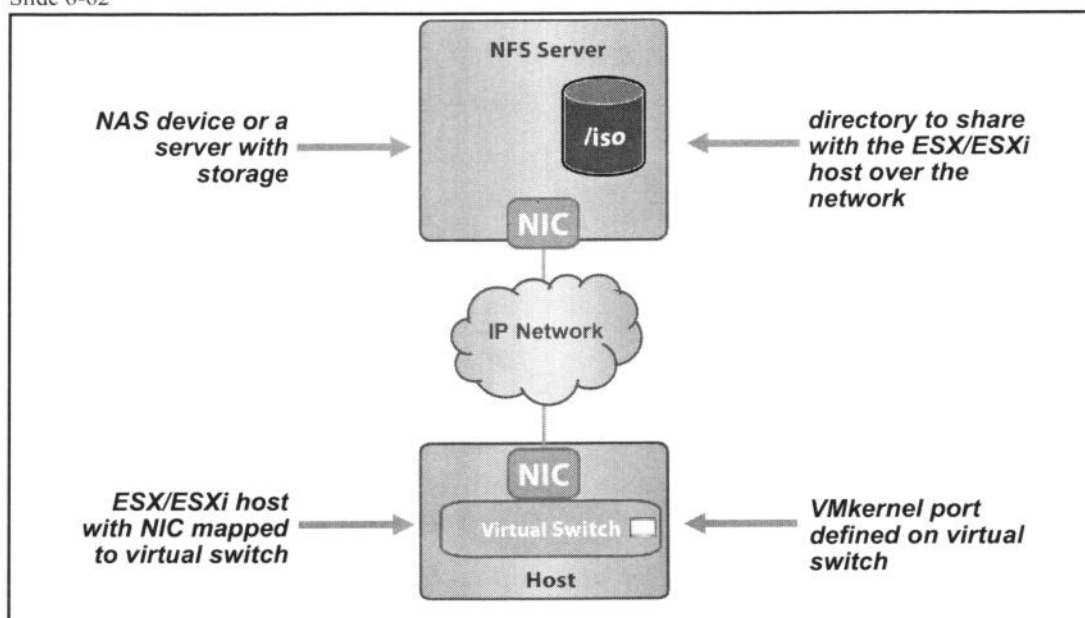
ESX/ESXi supports:

- > Up to 64 NFS volumes
- > NFS over a 10GbE interface
- > NFS in an IPv6 environment

The NFS protocol that ESX supports enables communication between an NFS client and an NFS server. The client issues requests for information from the server, which replies with the result. The NFS client built into ESX/ESXi lets you access the NFS server and use NFS volumes for storing virtual machines' files, ISO images, and templates.

NFS Components

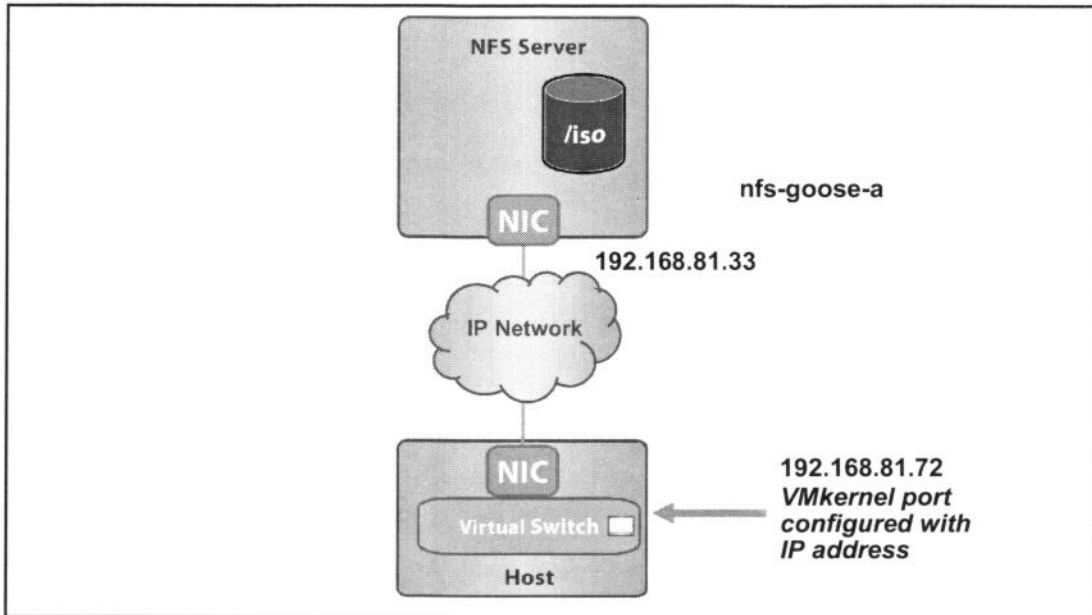
Slide 6-62



An NFS is located on a NAS device. This system is known as the NFS server. The NFS server contains one or more directories that will be shared with the ESX/ESXi host over a TCP/IP network. An ESX/ESXi host accesses the NFS server through a VMkernel port that is defined on a virtual switch.

Addressing and Access Control with NFS

Slide 6-63



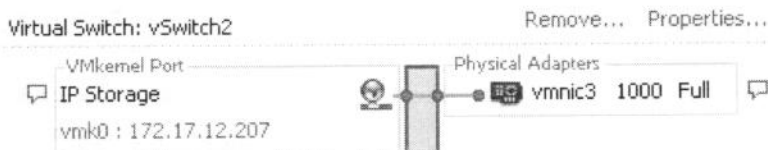
The ESX/ESXi host accesses the NFS server by its IP address or host name. The VMkernel port is configured with an IP address and is connected to a network that has access to the NFS server.

NFS access privileges are assigned to a special user, known as the delegate user. By default, the delegate user for the ESX/ESXi host is `root`. However, having `root` as the delegate user might not work for all NFS volumes. To protect NFS volumes from unauthorized access, the NFS administrator exports the volumes with the `root squash` option turned on. When `root squash` is on, the NFS server treats access by the `root` user as access by any unprivileged user and might refuse the ESX/ESXi host access to virtual machine files stored on the NFS volume.

Configuring Networking for NFS Access

Slide 6-64

Create a VMkernel port on a vSwitch for access to IP storage (for example, iSCSI and NFS).



To optimize your vSphere networking setup:

- > Separate network services like iSCSI and NFS access.
 - Physical separation is preferred.
 - If not possible, use VLANs.

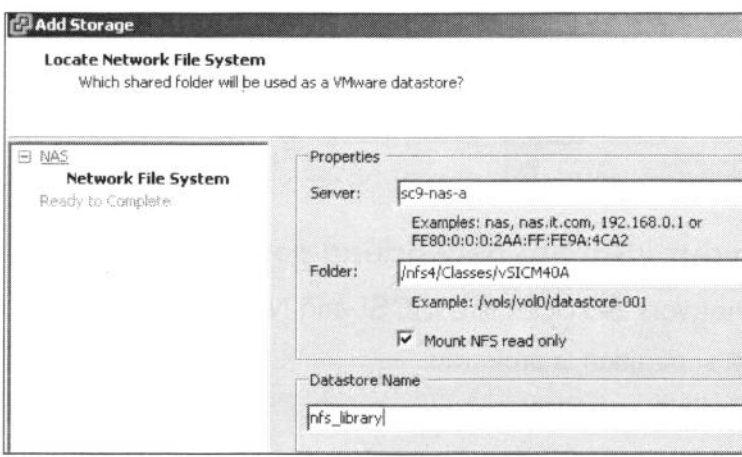
For the ESX/ESXi host to access the NFS datastore over the network, a VMkernel port must be configured on a virtual switch. The name of this port can be anything you want. In the example above, it is named IP Storage. The VMkernel port can be created as either another connection on an existing virtual switch or as a new connection on a new virtual switch.

For performance and security reasons, it is a best practice to isolate your NFS networks from the other networks, such as your iSCSI network and your virtual machine networks.

Creating an NFS Datastore

Slide 6-65

In the Add Storage wizard, enter the following information:



- > IP address or host name of NFS server
- > The shared folder on the NFS server
- > Whether to mount NFS read-only
- > The name of the datastore

To create an NFS datastore, click the **Storage** link in your host's **Configuration** tab. Click the **Add Storage** link and then select **Network File System** as the storage type. Enter the properties of your NFS datastore:

- Host name or IP address of the NFS server
- The path to the folder on the NFS server that you want this datastore to correspond to
- Whether you want to mount the NFS read-only
- Mount an NFS as a read-only file system if you want the NFS to be a library of read-only files, such as ISO images; you do not want this file system to be space for users to place their personal files; or you have a limited amount of space in the NFS and you do not want users accidentally filling up the NFS file system.
- The name of the datastore

Viewing NFS Datastore: Storage Tab

Slide 6-66

The NFS volume is displayed in the Datastores pane of the Configuration tab.

Browse the NFS datastore to display its contents.

View: Datastores Devices

Datastores

Identification	Status	Device	Capacity	Free	Type	Last Update
SAN	Alert	DGC Fibre Channel...	79.75 GB	3.84 GB	vmfs3	4/29/2009 8:41:10 PM
SharedVMs	Normal	DGC Fibre Channel...	99.75 GB	91.42 GB	vmfs3	4/29/2009 8:41:10 PM
Storage1	Normal	Local VMware Disk...	67.00 GB	49.77 GB	vmfs3	4/29/2009 8:41:10 PM
NFS_Library (read only)	Normal	sc9-nas-a:/nfs4/C...	1,008.38 G	629.75 GB	NFS	4/29/2009 8:41:10 PM
iSCSILUN		Browse Datastore...	4.75 GB	1.47 GB	vmfs3	4/29/2009 8:41:10 PM
Private04		Alarm	4.75 GB	4.45 GB	vmfs3	4/29/2009 8:41:10 PM

Datastore Details

NFS_Library (Readonly)

Server: sc9-nas-a

Capacity

Copy to Clipboard Ctrl+C

After creation, the NFS datastore appears in the **Datastores** pane of the host's **Configuration** tab. From this pane, you can also display the contents of the datastore by right-clicking the datastore and choosing **Browse Datastore**.

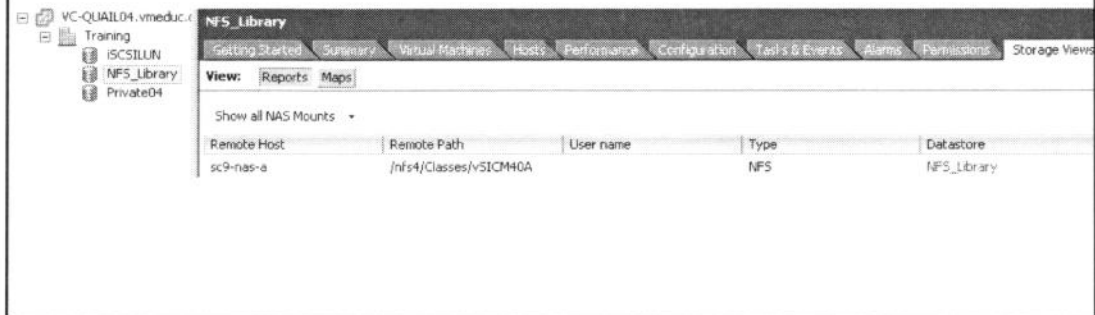
Viewing NFS Datastore: Storage Views Tab

Slide 6-67

The Datastores inventory view includes NFS volumes.

The Storage Views tab shows information about all NAS mounts (NFS datastores):

- NFS server, shared folder, datastore type, and datastore name



To display information about your NFS datastores, go to your host's **Storage Views** tab and display the **Show all NAS Mounts** report.

Unmounting an NFS Datastore

Slide 6-68

Use the Storage link in the Configuration tab to unmount an NFS datastore.


Unmounting an NFS datastore makes the files in the shared folder inaccessible to the host.

View: **Datastores** Devices

Datastores Refresh Delete

Identification	Status	Device	Capacity	Free	Type	Last Update
SharedVMs	Normal	DGC Fibre Channel...	99.75 GB	91.42 GB	vmfs3	4/29/2009 9:00:20 PM
Storage1	Normal	Local VMware Disk...	67.00 GB	49.77 GB	vmfs3	4/29/2009 9:00:20 PM
NFS_Library (read only)	Normal	sc9-nas-a:/nfs4/C...	1,008.38 G	629.75 GB	NFS	4/29/2009 9:00:20 PM
iSCSILUN	Normal	IET iSCSI Disk (t...	1.75 GB	1.47 GB	vmfs3	4/29/2009 9:00:20 PM
Private04	Normal	DGC Fibre Channel...	4.75 GB	4.45 GB	vmfs3	4/29/2009 9:00:20 PM

Confirm remove datastore

 The files on this datastore will be inaccessible once it is unmounted. Virtual machines that depend on these files will not be able to power on. Are you sure you want to unmount this datastore?

To unmount an NFS datastore, click the **Storage** link in the host's **Configuration** tab. Right-click the NFS datastore, then choose **Unmount**. The NFS file system will be unmounted and the files on the datastore will be inaccessible. In addition, virtual machines that depend on files on this datastore will not be able to power on.

Therefore, before you unmount the datastore, stop all virtual machines whose disks reside on this datastore.

Lab 8

Slide 6-69

In this lab, you will configure access to an NFS datastore.

1. Verify that a VMkernel port exists for NFS access.
2. Create an NFS datastore and view its contents.

Lesson Summary

Slide 6-70

- > When you create an NFS datastore, you must specify the NFS server host name and the shared folder on the NFS server.
- > The VMware vSphere Client allows you to browse the contents of a VMFS or NFS datastore.
- > When you unmount an NFS datastore, all files in the shared folder are inaccessible to the ESX/ESXi host.

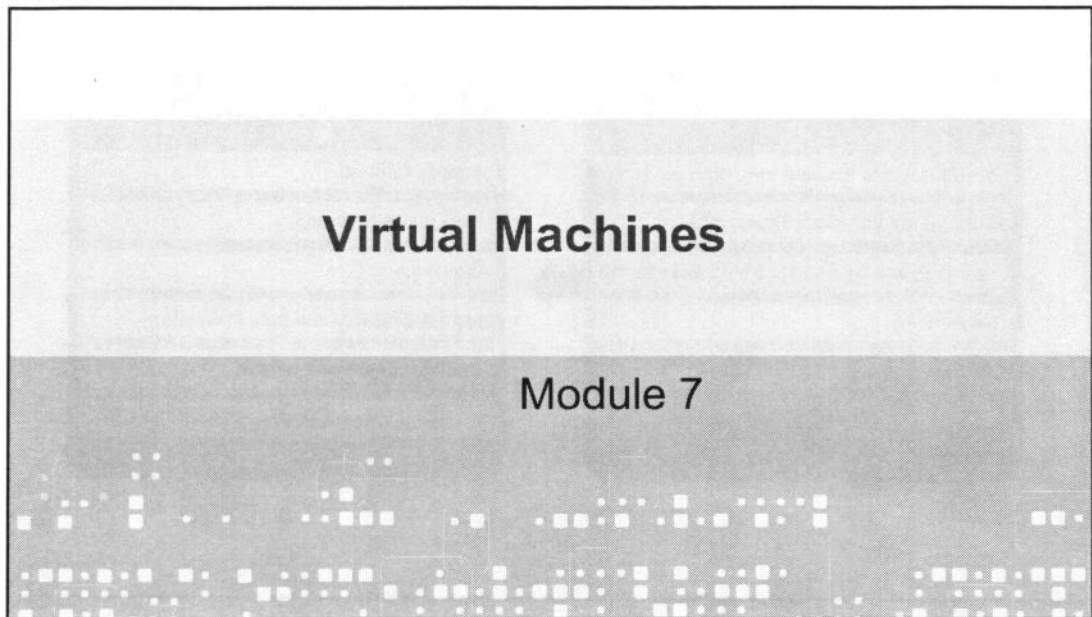
Key Points

Slide 6-71

- > Whenever possible, use VMFS datastores to hold virtual machines' files.
- > NFS datastores make a great repository for ISO images.
- > Shared storage is integral to vSphere features like VMware HA, DRS, and VMotion.

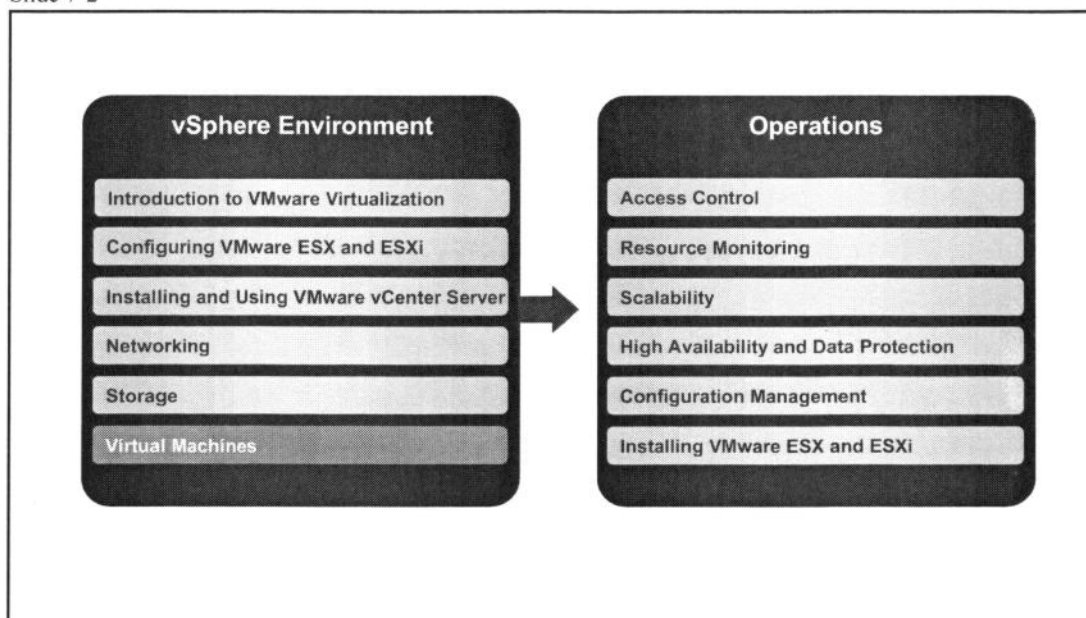
Virtual Machines

Slide 7-1



You Are Here

Slide 7-2



Importance

Slide 7-3

- > There are a number of ways to create a virtual machine. Choosing the correct method can help you save time and make the deployment process manageable and scalable.

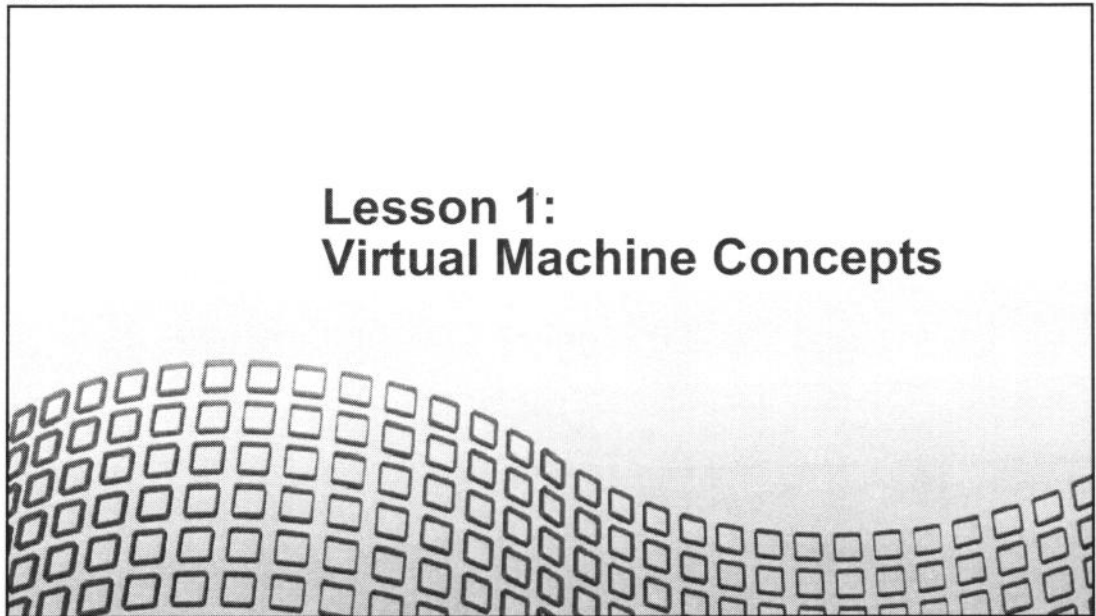
Module Lessons

Slide 7-4

- Lesson 1: Virtual Machine Concepts**
- Lesson 2: Creating a Virtual Machine**
- Lesson 3: Creating Templates and Clones**
- Lesson 4: VMware vCenter Converter**
- Lesson 5: vCenter Guided Consolidation**
- Lesson 6: Modifying Virtual Machines**
- Lesson 7: Managing Virtual Machines**

Lesson 1: Virtual Machine Concepts

Slide 7-5



Lesson Objectives

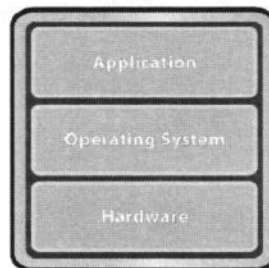
Slide 7-6

- > Describe a virtual machine
- > List the virtual machine hardware
- > Display a virtual machine's files

What Is a Virtual Machine?

Slide 7-7

- > It is a set of virtual hardware on which a supported guest operating system and its applications run.
- > It is a set of discrete files.
- > A virtual machine's configuration file describes the virtual machine's configuration, including its virtual hardware.
 - Avoid using special characters and spaces in the virtual machine's name.



Virtual Machine

MyVM.vmx

```
guestOS = "winnetstandard"  
displayName = "MyVM"  
(etc.)
```

A virtual machine is configured with a set of virtual hardware on which a supported guest operating system and its applications run. The virtual machine is a set of discrete files. The virtual machine's configuration file describes the virtual machine's configuration, which includes the virtual hardware, such as CPU, memory, disk, network interface, CD-ROM drive, and floppy drive.

When naming virtual machines, it is a best practice to avoid using special characters, including spaces, in the virtual machine name. The virtual machine name is used to name the files that make up the virtual machine.

What Files Make Up a Virtual Machine?

Slide 7-8

File name	Description
<VM_name>.vmx	Virtual machine configuration file
<VM_name>.vmdk	File describing virtual disk characteristics
<VM_name>-flat.vmdk	Preallocated virtual disk file that contains the data
<VM_name>.nvram	Virtual machine BIOS
vmware.log	Virtual machine log file
vmware-#.log (where # is number starting with 1)	Files containing old virtual machine log entries
<VM_name>.vswp	Virtual machine swap file
<VM_name>.vmsd	File that describes virtual machine's snapshots
Additional files can exist if snapshots are taken or raw disk mappings are added (to be discussed later).	

The table above lists the files that make up a virtual machine. Except for the log files, the name of each file starts with the virtual machine's name (<VM_name>). A virtual machine consists of the following files:

- A configuration file (.vmx)
- One or more virtual disk files (first virtual disk has files <VM_name>.vmdk and <VM_name>-flat.vmdk; subsequent virtual disks are named <VM_name>_#.vmdk and <VM_name>_#-flat.vmdk, where # is the next number in the sequence, starting with 1)
- A file containing the virtual machine's BIOS (.nvram)
- A log file (.log)
- A set of files used to archive old log entries (-#.log) (six of these files are maintained at any time)
- A swap file (.vswp)
- A snapshot description file (.vmsd) (this file is empty if the virtual machine has no snapshots)

A virtual machine can have additional files if one or more snapshots have been taken or if raw disk mappings have been added. This is discussed later in the module.

If the virtual machine has more than one disk file, the file pair for the second disk file and on is named <VM_name>_#.vmdk and <VM_name>_#-flat.vmdk, where # is the next number in

sequence, starting with 1. For example, if the virtual machine named Test01 has two virtual disks, then this virtual machine will have the files Test01.vmdk, Test01-flat.vmdk, Test01_1.vmdk, and Test01_1-flat.vmdk.

Regarding the archive log files, six of these files are maintained at any time. For example, -1.log to -6.log might exist at first. The next time an archive log file is created (for example, when the virtual machine is powered off and powered back on), -2.log to -7.log are maintained (-1.log is deleted), then -3.log to -8.log, and so forth.

Displaying a Virtual Machine's Files

Slide 7-9

Click the Storage link in the Configuration tab.

Right-click a datastore to browse its files.

The screenshot shows the VMware vSphere Client interface. At the top, the 'View' tab is set to 'Datastores'. Below this is a table of datastores:

Identification	Status	Device	Capacity
SharedVMs	Normal	DGC Fibre Channel...	99.75 GB
Storage1	Normal	Local VMware Disk...	67.00 GB
NFS_Library (re...			1,008.38 G
ISCSILUN			1.75 GB
Private04			4.75 GB

A right-click context menu is open over the 'Storage1' datastore, with the 'Browse Datastore...' option selected. Below the table, the 'Datastore Browser - [Storage1]' window is open, showing a tree view of folders on the left and a list of files in the center. The tree view shows folders like 'esxconsole-49f626e', 'VM-for-StudentA', 'VM-for-StudentB', 'VM Template', '.dvsData', and 'vSauce04-1'. The file list shows files like 'VM-for-StudentA.vmdk', 'VM-for-StudentA.vmx', 'VM-for-StudentA.vmsd', 'VM-for-StudentA.nvram', 'vmware-1.log', 'vmware.log', and 'VM-for-StudentA-a45fdc09.vswp'.

A virtual machine's files are located in either a VMware® vStorage VMFS datastore or an NFS datastore. You can display a virtual machine's files using the VMware vSphere™ Client if you know the datastore on which the virtual machine is located.

To find out what datastores your virtual machine is using, select your virtual machine in the inventory and view its **Summary** tab. The list of datastores used by the virtual machine is shown in the **Resources** section.

To display the virtual machine's files on a datastore, select your VMware ESX™/ESXi host from the inventory and then click its **Summary** tab. The list of datastores accessible by the ESX/ESXi host is shown in the **Resources** section. You right-click a datastore and then select **Browse Datastore** from the drop-down menu. The contents of the datastore are displayed. Double-click into any virtual machine's folder to display its files.

Displaying Files Using the Storage Views Tab

Slide 7-10

Click the Storage Views tab.

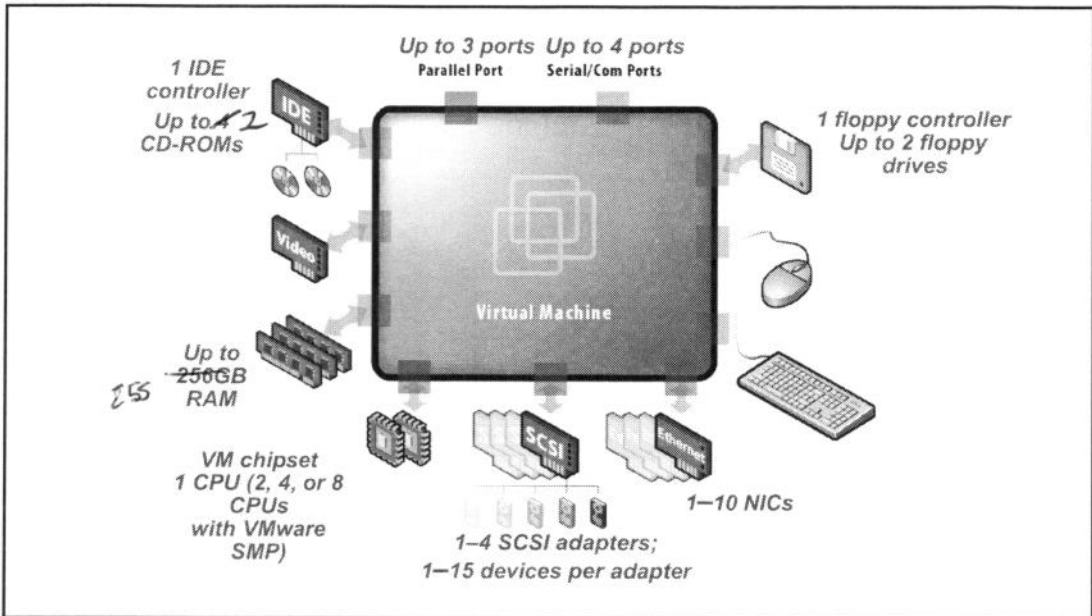
Select Show All Virtual Machine Files from the menu.

View: Reports Maps		Last Update Time:		
Show all Virtual Machine Files ▾		Name, Path or File type contains		
Name	Path	File type	Datastore	Size
vmware-1.log	[Storage1] VM-for-StudentA/vmware-1.log	Log	Storage1	40.04
VM-for-StudentA.vmdk	[Storage1] VM-for-StudentA/VM-for-StudentA.vmdk	Disk Descriptor	Storage1	507.0
VM-for-StudentA.vmsd	[Storage1] VM-for-StudentA/VM-for-StudentA.vmsd	Snapshot List	Storage1	0.00 B
VM-for-StudentA.vmx	[Storage1] VM-for-StudentA/VM-for-StudentA.vmx	Extended Configuration	Storage1	270.0
vmware.log	[Storage1] VM-for-StudentA/vmware.log	Log	Storage1	54.79
VM-for-StudentA-flat.vmdk	[Storage1] VM-for-StudentA/VM-for-StudentA-flat.vmdk	Disk Extent	Storage1	3.00 G
VM-for-StudentA-a45fdc09...	[Storage1] VM-for-StudentA/VM-for-StudentA-a45fdc09...	Swap	Storage1	256.0
VM-for-StudentA.nvram	[Storage1] VM-for-StudentA/VM-for-StudentA.nvram	NVRAM	Storage1	8.48 K
VM-for-StudentA.vmx	[Storage1] VM-for-StudentA/VM-for-StudentA.vmx	Configuration	Storage1	2.56 K

You can also use the host's **Storage Views** tab to display a virtual machine's files. To do this, select a virtual machine in the inventory, then click the **Storage Views** tab. Display the Show all Virtual Machine Files report to view all the files for the virtual machine selected.

Virtual Machine Hardware

Slide 7-11



A virtual machine uses virtual hardware. Each guest operating system sees ordinary hardware devices—it does not know that these devices are virtual. Furthermore, all virtual machines have uniform hardware (except for a small number of variations that the system administrator can apply). This makes virtual machines uniform and portable across platforms.

Virtual machines on ESX/ESXi hosts have most devices. One device that is not supported is a sound adapter.

Each virtual machine has a total of six virtual PCI slots. One is used for the virtual video adapter. Therefore, the total number of virtual adapters—SCSI plus Ethernet—cannot be greater than five. The virtual chipset is an Intel 440BX-based motherboard with an NS338 SIO chip. This chipset ensures compatibility for a wide range of supported guest operating systems (including legacy operating systems like Windows NT). A virtual machine can have up to two IDE controllers, which means that up to four CD-ROM drives are supported per virtual machine.

CPU and Memory

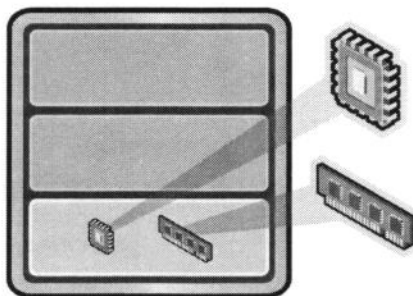
Slide 7-12

Up to eight virtual CPUs (VCPUs)

- > Virtual SMP license required
- > Also depends on number of licensed CPUs on a host and the number of processors supported by a guest operating system

Maximum memory size (up to 256GB)

- > Amount the guest operating system will be told it has



Virtual Machine

Although the vSphere Client interface can provide a default memory size for your virtual machine at the time of creation, you should understand the memory needs of your application and guest operating system and size accordingly. The maximum memory size allowed for any virtual machine is 256GB. Memory size is the maximum amount of physical memory that the virtual machine can use.

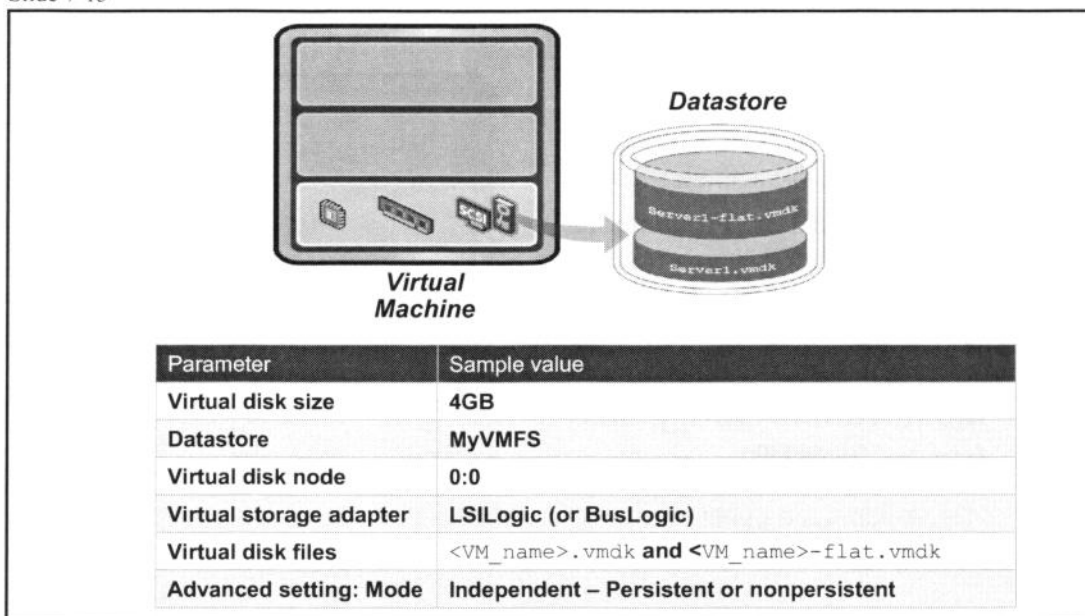
VMware Virtual SMP allows you to take advantage of configuring a virtual machine with up to eight virtual CPUs, allowing larger CU-intensive workloads to run on ESX/ESXi hosts. It is also possible to assign any integer number of virtual CPUs between one and eight to a virtual machine.

Many guest operating system/application combinations are not enhanced by the additional CPU. Multi-VCPU virtual machines should be created only in the comparatively infrequent instances where they are of benefit and not as a standard configuration.

Not every computer can host virtual machines with multiple virtual CPUs. In a later module, we will discuss the relationship between a virtual machine's number of virtual CPUs and the physical processors on the computer that hosts it.

Virtual Disk

Slide 7-13



A virtual machine should have at least one virtual disk. Adding the first virtual disk implicitly adds a virtual SCSI adapter for it to be connected. The ESX/ESXi host offers a choice of either a virtual LSILogic adapter or a virtual BusLogic adapter. The Virtual Machine Creation wizard in the vSphere Client automatically selects the type of virtual SCSI adapter, based on the choice of guest operating system.

You select a VMFS to hold the new, blank virtual disk, and specify the disk's size. Choose a descriptive filename for the virtual disk. You can also site the disk at a specific virtual SCSI target ID and LUN. Finally, choose the appropriate disk mode. You can change the disk mode any time the virtual machine is powered off.

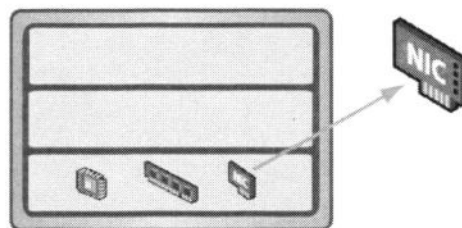
ESX/ESXi host virtual disks are monolithic and pre-extended. In other words, if you make a 6GB virtual disk, the result will be a single 6GB file.

Virtual NIC

Slide 7-14

The following network adapters might be available for your virtual machine:

- > vlane – Also called PCNet32, supported by most 32-bit guest operating systems
- > vmxnet – Provides significantly better performance than vlane
- > Flexible – Can function as either a vlane or vmxnet adapter
- > e1000 – High-performance adapter available only for some guest operating systems
- > Enhanced vmxnet – vmxnet adapter with enhanced performance
- > vmxnet3 – Builds on the Enhanced vmxnet adapter



Virtual Machine

There are several virtual network adapters available to the virtual machine:

- vlane – Supported only on legacy virtual machines. A vlane adapter uses the stock driver that the guest operating system provides and does not require that VMware Tools be installed in the virtual machine. vlane is supported by most 32-bit guest operating systems (except Windows Vista).
- vmxnet – Supported only on legacy virtual machines. It usually provides significantly better performance than a vlane adapter, but it requires that VMware Tools be installed.
- Flexible – Supported on virtual machines that were created on ESX 3.x or greater and that run 32-bit guest operating systems. The Flexible adapter functions as a vlane adapter if VMware Tools is not installed in the virtual machine. It functions as a vmxnet adapter if VMware Tools is installed in the virtual machine.
- e1000 – Emulates the functioning of an e1000 network card. It is the default adapter type for virtual machines that were created on ESX 3.x or greater and that run 64-bit guest operating systems.
- Enhanced vmxnet – An upgraded version of the vmxnet adapter, Enhanced vmxnet provides some high-performance features commonly used on modern networks, such as jumbo frames. It requires that VMware Tools be installed in the virtual machine.

- vmxnet3 – The third-generation virtual NIC emulation (after vmxnet and enhanced vmxnet) available through VMware Tools. vmxnet features include message signaled interrupts subject to guest kernel support, receive-side scaling (supported in Windows 2008), IPv6 checksum and TCP segmentation off-loading (TSO) over IPv6, VLAN off-loading, and support for VMDirectPath I/O technologies.

Other Devices

Slide 7-15

CD-ROM drive

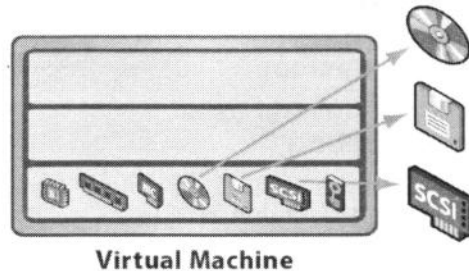
- > Connect to CD-ROM or ISO image.

Floppy drive

- > Connect to floppy or floppy image.

Generic SCSI devices (such as tape libraries)

- > Can be connected to additional SCSI adapters



Virtual CPU and virtual memory are your minimum required virtual hardware. Having a virtual hard disk and virtual NICs will make the virtual machine more useful. Additional virtual hardware that you can add to your virtual machine are a virtual CD/DVD-ROM drive, a virtual floppy drive, and generic virtual SCSI devices. The virtual CD/DVD-ROM drive or floppy drive can point to either the CD/DVD-ROM drive or floppy drive located on the ESX/ESXi host, a CD/DVD ISO image (.iso) or floppy (.flp) images, or even the CD/DVD-ROM or floppy drive on your local system.

You can map the virtual machine's CD/DVD-ROM drive either to a physical drive or to an ISO file for your CD/DVD-ROM drive. An ISO file is a CD/DVD-ROM that has been "ripped": its file system is copied byte-for-byte to the disk surface. These virtual CDs/DVDs can be accessed remotely and are usually faster than physical CDs/DVDs.

Virtual Machine Console

Slide 7-16

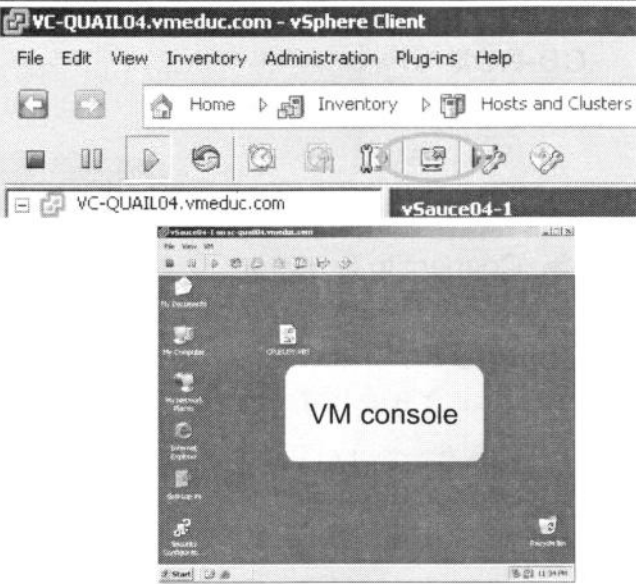
Send power changes to virtual machine.

Access virtual machine's guest operating system.

Send Ctrl+Alt+Del to guest operating system.

➤ Press Ctrl+Alt+Ins in virtual machine console.

Press Ctrl+Alt to release cursor from virtual machine console.



The screenshot shows the vSphere Client interface. The top bar indicates the connection to 'VC-QUAIL04.vmeduc.com - vSphere Client'. The main menu includes File, Edit, View, Inventory, Administration, Plug-ins, and Help. The breadcrumb trail shows 'Home > Inventory > Hosts and Clusters'. The left sidebar lists various icons for managing virtual machines. The main pane displays the console for a virtual machine named 'vSource04-1'. The console window shows a Windows desktop environment with a watermark that reads 'VM console'.

The virtual machine's console, available in the vSphere Client, provides the mouse, keyboard, and screen functionality. To install an operating system, you must use the virtual machine's console. The virtual machine console allows access to the BIOS of the virtual machine and offers the ability to power the virtual machine on and off and to reset it.

The virtual machine console is normally not used to connect to the virtual machine for daily tasks. Tools like Remote Desktop Connection, Citrix, or Virtual Network Connection, for example, are normally used to connect to the virtual machine. The virtual machine console is used for tasks like power cycling, configuring hardware, and troubleshooting network issues.

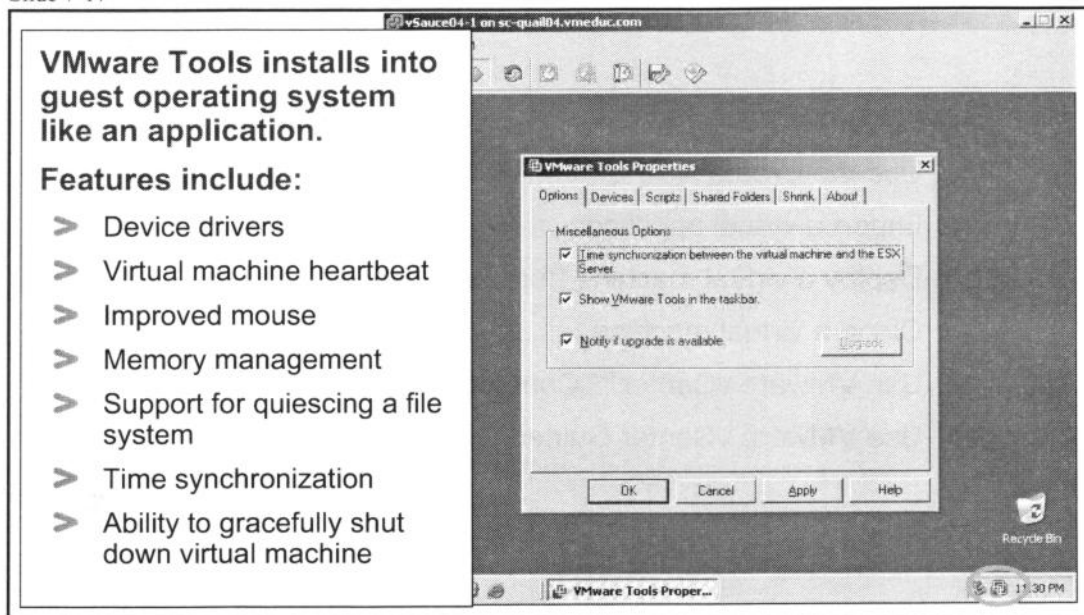
The virtual machine console allows you to send the Ctrl+Alt+Del key sequence specifically to the virtual machine. This is accomplished by pressing Ctrl+Alt+Ins in the virtual machine console or by selecting **VM** in the virtual machine console menu bar and choosing **Send Ctrl+Alt+Del** from the drop-down menu.

Likewise, to release the cursor from the virtual machine console so that you can use it in other windows, press Ctrl+Alt.

To view the virtual machine's console, right-click your virtual machine in the inventory, then choose **Open Console**.

VMware Tools

Slide 7-17



VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.

Installing VMware Tools in the guest operating system is vital. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience. When you install VMware Tools, you install the following:

- The VMware Tools service. This service synchronizes the time in the guest operating system with the time in the host operating system.
- A set of VMware device drivers, including an SVGA display driver, the vmxnet networking driver for some guest operating systems, the BusLogic SCSI driver for some guest operating systems, the memory control driver for efficient memory allocation between virtual machines, the sync driver to quiesce I/O for VMware Consolidated Backup, and the VMware mouse driver.
- The VMware Tools control panel, which enables you to modify settings and connect and disconnect virtual devices.
- A set of scripts that helps you to automate guest operating system operations. The scripts run when the virtual machine's power state changes, if you configure them to do so.
- The VMware user process, which enables you to copy and paste text between the guest operating system and the managed host operating system.

Provisioning a Virtual Machine

Slide 7-18

Several methods for creating virtual machines:

- > Use the Create New Virtual Machine wizard.
- > Import a virtual appliance.
- > Deploy a virtual machine from template.
- > Clone a virtual machine.
- > Use VMware vCenter™ Converter.
- > Use VMware vCenter Guided Consolidation.

There are several methods available to you for creating, or provisioning, virtual machines. These methods will be discussed in detail in this module.

VMware Products for Provisioning Virtual Machines

Slide 7-19

VMware Stage Manager

- > Quickly and consistently transitions service configurations through the stages of the release process – integration, testing, staging, and user acceptance testing – into production.

VMware vCenter Lifecycle Manager

- > Provides a consistent, automated process for managing the life cycle of virtual machines in the datacenter, from provisioning to operation to retirement

VMware Lab Manager

- > Allows you to create and manage a library of commonly used configurations and dynamically provision them in seconds

Several VMware products act as front ends to vCenter Server to enable you to provision and manage virtual machines:

- VMware Stage Manager – Uses a simple user interface as a global view of all services under management, organizes multimachine service configurations by the IT service they support, defines the stages of the release process and customizes them for specific services, and associates resource pools from vCenter Server with services and life-cycle stages.
- VMware vCenter Lifecycle Manager – Allows user to easily request virtual machines and determine request status through a self-service portal, allows an approver to approve or reject requests, and allows IT staff to complete approved requests and decide where virtual machines will be placed within the environment.
- VMware Lab Manager – Allows users to create, deploy, and share complex system configurations with multiple physical and virtual network connections from a self-service portal controlled by IT; maintains a complete library of commonly used system environments for on-demand use; pools and shares server, networking, storage, and other resources among users (teams and individuals).

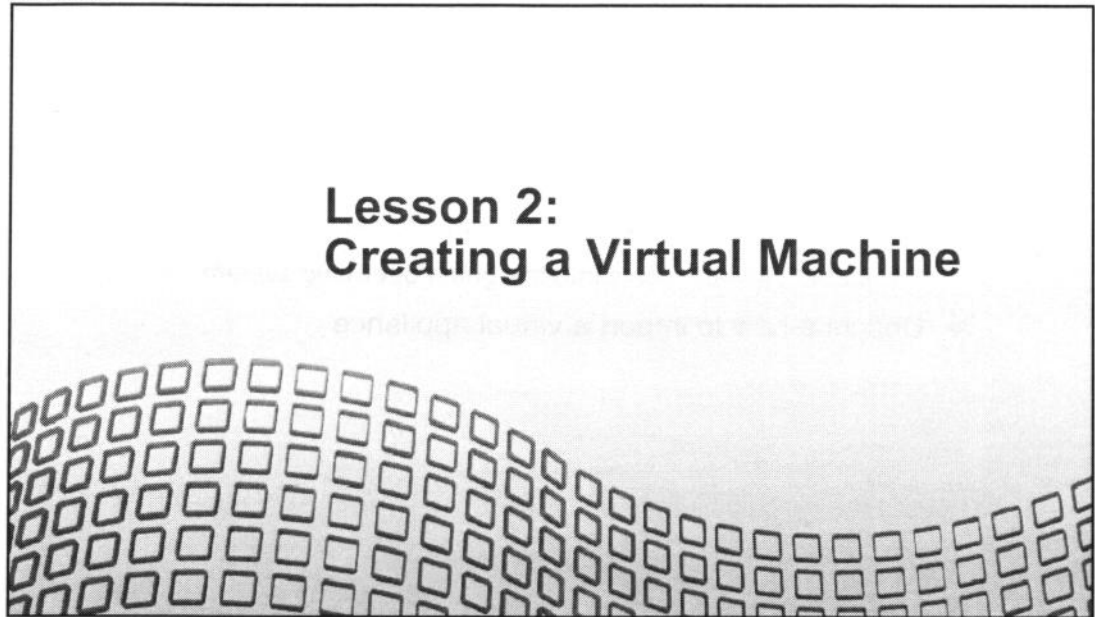
Lesson Summary

Slide 7-20

- > A virtual machine is a discrete set of files that is located in a datastore.
- > Display a virtual machine's files using the host's **Configuration** tab or **Storage Views** tab.
- > VMware Tools provides features such as enhanced device drivers, improved mouse movement, and a virtual machine heartbeat.

Lesson 2: Creating a Virtual Machine

Slide 7-21



Lesson Objectives

Slide 7-22

- > Provision a virtual machine
 - Create the virtual machine
 - Install the guest operating system into the virtual machine
 - Install VMware Tools into the guest operating system
- > Describe how to import a virtual appliance

Creating a Virtual Machine: Launch Wizard

Slide 7-23

Create a new virtual machine in the VMware vCenter Server inventory.

- > In the Hosts and Clusters view, select a datacenter, cluster, or host.
- > In the VMs and Templates view, select a folder.

Launch the Create New Virtual Machine wizard.

- > Perform a “typical” or “custom” configuration.



To create a virtual machine, navigate to either the Hosts and Clusters view or the VMs and Templates view.

In the Hosts and Clusters view, right-click the datacenter, cluster, or host, then choose **New Virtual Machine**. The Create New Virtual Machine wizard is launched. In the VMs and Templates view, right-click the datacenter or folder, if one exists.

The wizard asks whether you want to perform a “typical” or “custom” configuration. The typical path shortens the process by skipping some choices that rarely need changing from their defaults. The custom path provides more flexibility and options.

Choosing the Typical Configuration

Slide 7-24

Information needed for a typical configuration:

- > Virtual machine name and inventory location
- > Location in which to place the virtual machine (cluster, host, resource pool)
- > Datastore on which to store virtual machine's files
- > Guest operating system and version
- > Disk parameters for creating a new virtual disk:
 - Disk size
 - Disk-provisioning settings:
 - **Allocate and commit space on demand (Thin Provisioning)**
 - **Support clustering features such as Fault Tolerance**

If you choose the typical configuration, the New Virtual Machine wizard prompts you for information such as the virtual machine name, where in the vCenter Server inventory to place the virtual machine, the datastore on which to locate the virtual machine's files, and the guest operating system to be installed into the virtual machine.

You will also be prompted for the size of the virtual disk and an option to choose disk provisioning settings:

- **Allocate and commit space on demand (Thin Provisioning)** – If you do not select this check box, the virtual disk file will be expanded to the specified size now. If you select the check box, the virtual disk file will grow as the virtual machine is used.
- **Support clustering features such as Fault Tolerance** – If you select this check box, then this virtual machine can take advantage of the VMware Fault Tolerance feature (discussed in a later module).

Choosing the Custom Configuration

Slide 7-25

Additional information needed for a custom configuration:

- > Virtual machine version
- > Number of CPUs and size of memory
- > Number of NICs, network to connect to, and network adapter type
- > SCSI controller type
- > Whether to create a new disk, use an existing disk, use an RDM, or use no disk
- > Additional disk-provisioning settings:
 - Store virtual disk with virtual machine or in a different datastore
 - Virtual device node (for example, SCSI(0:0))
 - Mode-independent (persistent and nonpersistent)

You can also edit the virtual machine settings before completing the creation task.

- > For example, attach an ISO image to the virtual CD-ROM device.

If you choose the custom configuration, the New Virtual Machine wizard prompts you for additional information like the virtual machine version (always choose the latest version to take advantage of the newer features) and specifics about the virtual hardware to add.

The wizard also gives you the choice of creating a new virtual disk, using an existing virtual disk, creating an RDM, or using no disk at all. Specify whether you want to store the virtual disk file on the same datastore as the virtual machine files, or whether you want to store the virtual disk file on a separate datastore.

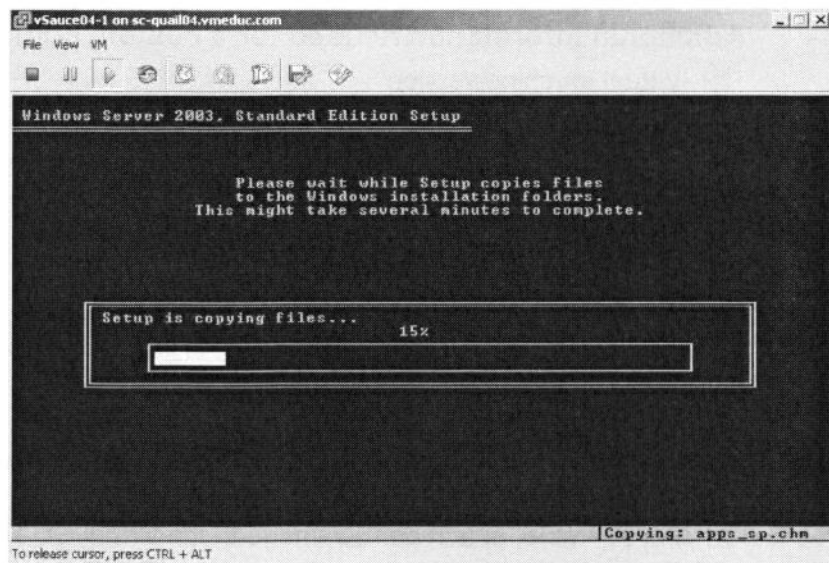
You can also set advanced options, such as selecting a virtual device node for a disk or raw device mapping. You can also enable and configure independent mode for disks. Select **Independent Persistent** if you want changes to be immediately and permanently written to the disk. Select **Independent Nonpersistent** to discard changes when the virtual machine is powered off or reverted to a snapshot. In most cases, you do not need to change the advanced options for virtual disks.

You can perform additional configuration before completing the virtual machine. For example, you can attach an ISO image to the virtual CD-ROM device once the virtual machine is created.

Installing the Guest Operating System

Slide 7-26

Install the guest operating system into the virtual machine.



Installing a guest operating system inside your virtual machine is essentially the same as installing it on a physical computer.

To install the guest operating system, interact with the virtual machine through the virtual machine console, accessible in the vSphere Client. Also, using the vSphere Client, you can attach a CD-ROM or ISO image containing the install image to the virtual CD-ROM drive.

In the example above, the Windows Server 2003 guest operating system is being installed.

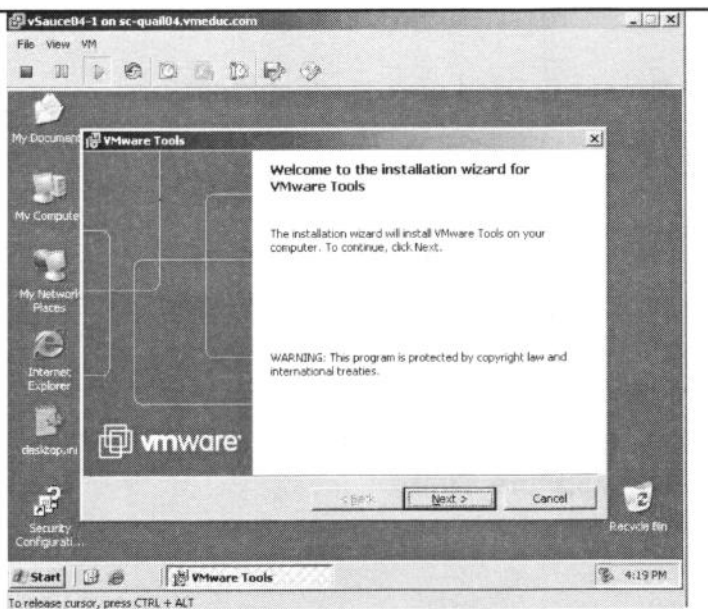
For details on the supported guest operating systems, see *Guest Operating System Installation Guide* at http://www.vmware.com/pdf/GuestOS_guide.pdf.

Installing VMware Tools

Slide 7-27

Install VMware Tools.

- Right-click virtual machine in the inventory, then choose **Guest > Install/Update VMware Tools**.



The installers for VMware Tools for Windows, Linux, Solaris, and NetWare guest operating systems are built into ESX/ESXi as ISO image files. You do not use an actual CD-ROM disc to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file.

When you choose to install VMware Tools, vCenter Server temporarily connects the virtual machine's first virtual CD-ROM disk drive to the ISO image file that contains the VMware Tools installer for your guest operating system.

To install VMware Tools in a virtual machine, you right-click on the virtual machine name in the inventory and select **Install/Upgrade VMware Tools**. The virtual machine must be powered on and you must be logged in with an administrative or root-level account.

Virtual Appliances

Slide 7-28

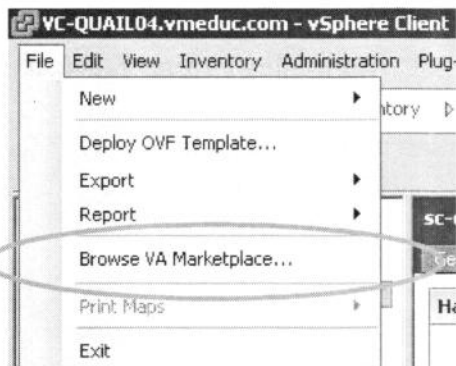
Preconfigured virtual machines:

- > Usually designed for a single purpose (for example, a safe browser or firewall)
- > Deployed as an OVF template

Available from the VMware Virtual Appliance Marketplace

- > <http://www.vmware.com/appliances>

Upload into vCenter Server using the vSphere Client.



A virtual appliance is a preconfigured virtual machine that typically includes a preinstalled guest operating system and other software. It is usually designed for a specific purpose; for example, to provide a secure Web browser, a firewall, or a backup/recovery utility.

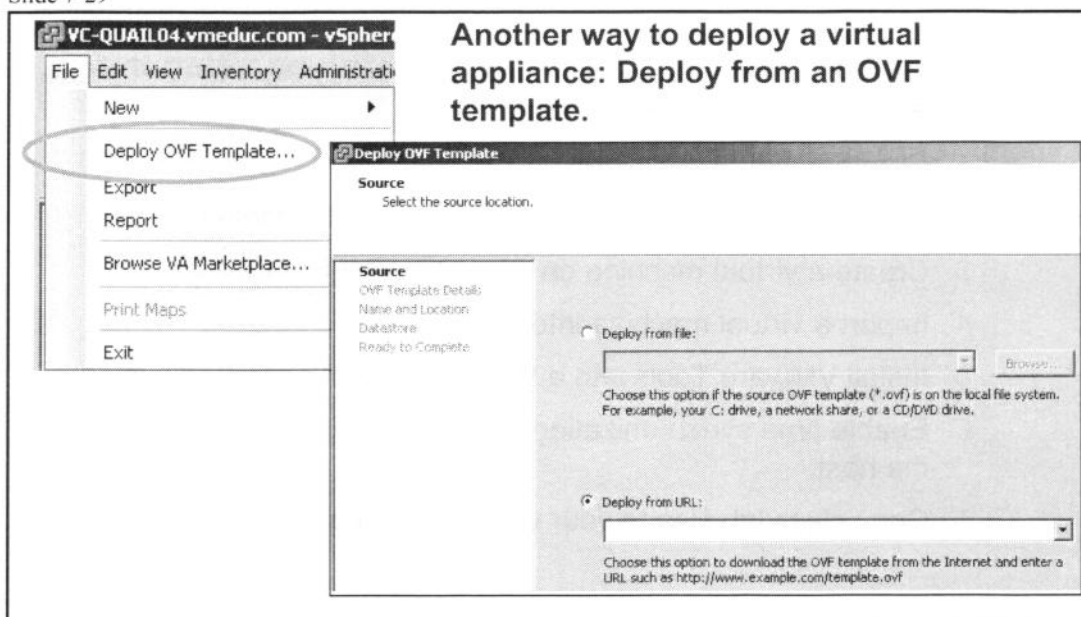
A virtual appliance can be added, or imported, to your vCenter Server or ESX/ESXi inventory. The concept of importing a virtual appliance is similar to deploying a virtual machine from a template. Virtual appliances can be imported from Web sites like the VMware Virtual Appliance Marketplace at <http://www.vmware.com/appliances/>.

To import a virtual appliance to your vCenter Server from the VMware Virtual Appliance Marketplace, use the vSphere Client. In the menu bar, select **File > Browse VA Marketplace**. The Deploy OVF Template wizard launches and steps you through the process of choosing the virtual appliance, downloading it to an ESX host, and adding it to the vCenter Server inventory.

Virtual appliances are deployed as an Open Virtual Machine (OVF) template. OVF is a platform-independent, efficient, extensible, and open packaging and distribution format for virtual machines. OVF files are compressed, allowing for faster downloads. The vSphere Client validates an OVF file before importing it and ensures that it is compatible with the intended destination server. If the appliance is incompatible with the selected host, it cannot be imported.

Deploy OVF Template

Slide 7-29



Another way to deploy a virtual appliance: Deploy from an OVF template.

In addition to virtual appliances, the vSphere Client allows you to import and export any file in OVF format.

To import a virtual appliance, select the host or cluster in the inventory that you plan to run the appliance, then choose **File > Deploy OVF Template**. This launches the Deploy OVF Template wizard. The wizard allows you to specify the OVF filename from which to import. If you are importing an OVF file from the Internet, you can also specify the URL pointing to the file itself.

Exporting virtual machines allows you to create virtual appliances that can be imported by other users. You can use the export function to distribute preinstalled software as a virtual appliance, or as a means of distributing template virtual machines to users, including users who cannot directly access and use the templates in your vCenter Server inventory.

To export a virtual machine, select the virtual machine in the inventory. The virtual machine you select must be powered off and must not have connections to local devices like CD-ROMs. From the menu bar, choose **File > Export > Export OVF Template**.

Lab 9

Slide 7-30

In this lab, you will create a virtual machine using the Create Virtual Machine wizard.

1. Create a virtual machine.
2. Install a guest operating system in a virtual machine.
3. Create a virtual machine on an iSCSI VMFS datastore.
4. Import a virtual machine into the inventory.
5. Install VMware Tools into a Windows guest operating system.
6. Enable time synchronization between the virtual machine and the host.
7. Copy class lab files to your virtual machine.

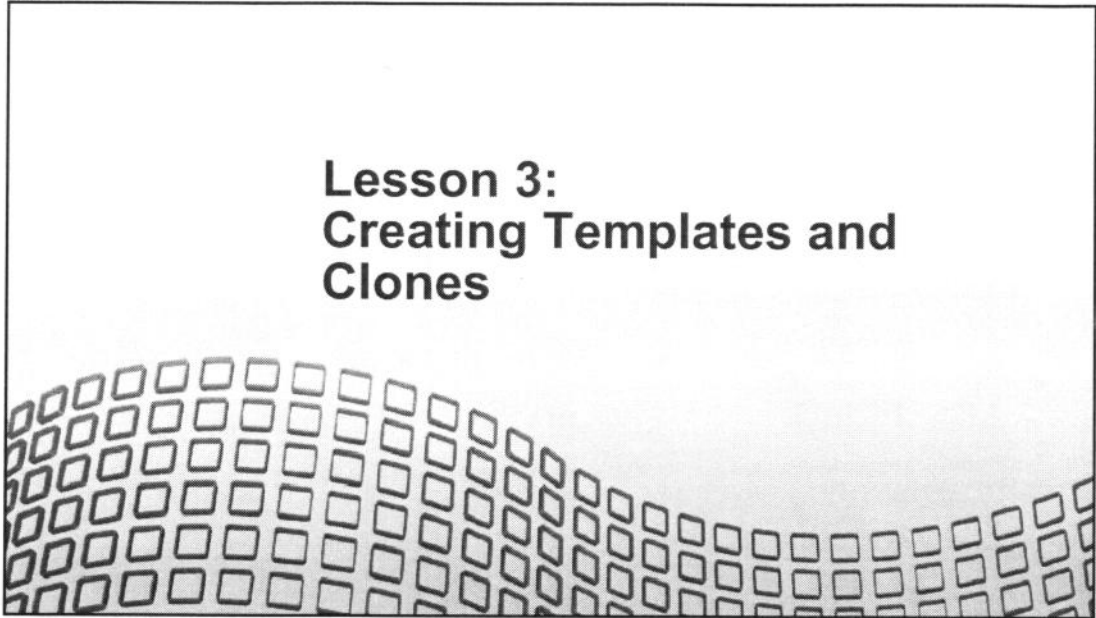
Lesson Summary

Slide 7-31

- > Using the Create Virtual Machine wizard is one way to create a virtual machine.
- > Always install VMware Tools into a virtual machine.
- > Virtual appliances are preconfigured virtual machines and can be imported from Web sites like the Virtual Appliance Marketplace.

Lesson 3: Creating Templates and Clones

Slide 7-32



Lesson Objectives

Slide 7-33

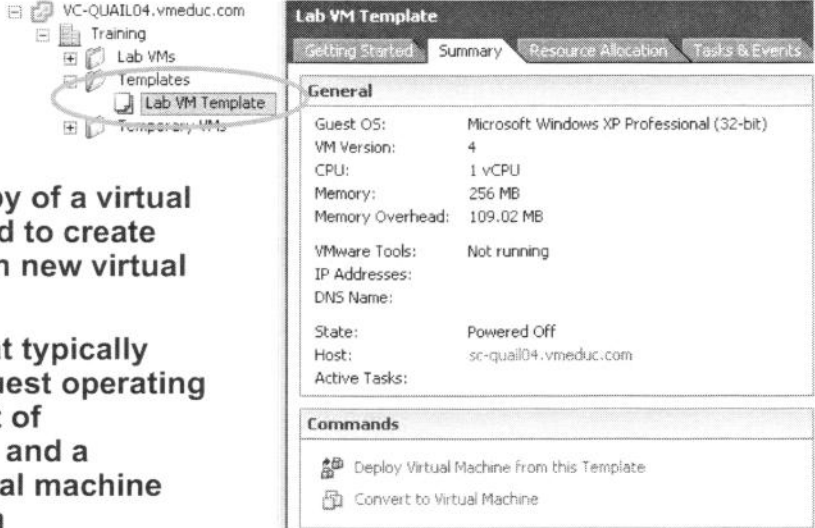
- > Create a template
- > Deploy a virtual machine from a template
- > Clone a virtual machine
- > Allow guest operating system customization by vCenter Server

What Is a Template?

Slide 7-34

A master copy of a virtual machine used to create and provision new virtual machines

An image that typically includes a guest operating system, a set of applications, and a specific virtual machine configuration



The screenshot displays the VMware vSphere interface. On the left, a folder tree shows the hierarchy: VC-QUAIL04.vmeduc.com > Training > Lab VMs > Templates > Lab VM Template. The 'Lab VM Template' folder is selected and circled. On the right, the 'Lab VM Template' configuration window is open, showing the 'General' tab. The configuration details are as follows:

General	
Guest OS:	Microsoft Windows XP Professional (32-bit)
VM Version:	4
CPU:	1 vCPU
Memory:	256 MB
Memory Overhead:	109.02 MB
VMware Tools:	Not running
IP Addresses:	
DNS Name:	
State:	Powered Off
Host:	sc-quail04.vmeduc.com
Active Tasks:	

Below the configuration details, the 'Commands' section lists two actions:

- Deploy Virtual Machine from this Template
- Convert to Virtual Machine

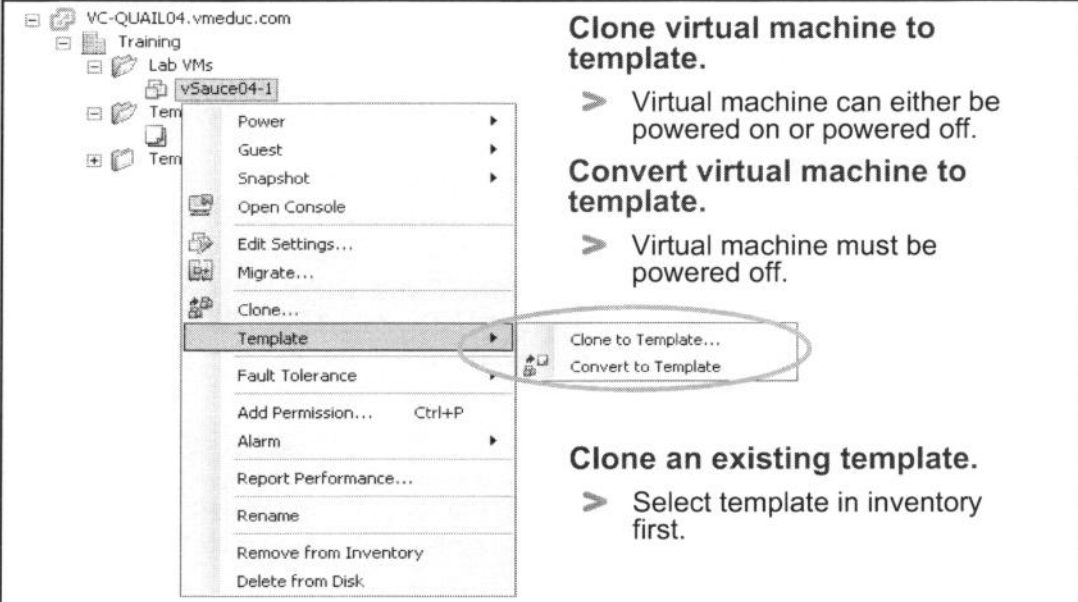
A template is a master copy of a virtual machine that can be used to create and provision new virtual machines. This image includes a guest operating system, a set of applications, and a configuration that provides virtual counterparts to hardware components.

Templates coexist with virtual machines at any level within the template and virtual machine domain. You can order collections of virtual machines and templates into arbitrary folders and apply a variety of permissions both to virtual machines and templates. Virtual machines can be transformed into templates without requiring a full copy of the virtual machine files and the creation of a new object.

You can use templates to create new virtual machines by deploying the template as a virtual machine. When complete, the deployed virtual machine is added to the folder chosen by the user when the template was created.

Creating a Template

Slide 7-35



Clone virtual machine to template.

- > Virtual machine can either be powered on or powered off.

Convert virtual machine to template.

- > Virtual machine must be powered off.

Clone an existing template.

- > Select template in inventory first.

There are three ways to create a template:

- Clone a virtual machine to a template
- Convert a virtual machine to a template
- Clone an existing template

When you clone a virtual machine to template, the original virtual machine is retained. When you convert a virtual machine to a template, the original virtual machine goes away. When you clone an existing template, you make a copy of a template that has already been created.

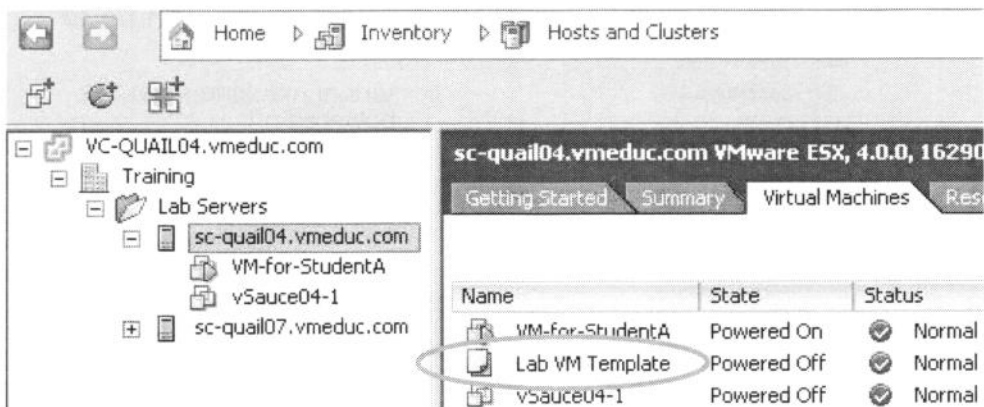
The **Clone to Template** option offers the choice between normal and compact disk (compressed) format. The **Convert to Template** option leaves the virtual machine's disk file intact (which uses normal disk format).

Viewing Templates

Slide 7-36

Use the VMs and Templates inventory view.

In the Hosts and Clusters view, use the Virtual Machines tab.



To view all templates, navigate to the VMs and Templates inventory view. You can also view templates from the Hosts and Clusters view by selecting a container object (root, datacenter, cluster, or folder) and clicking its **Virtual Machines** tab.

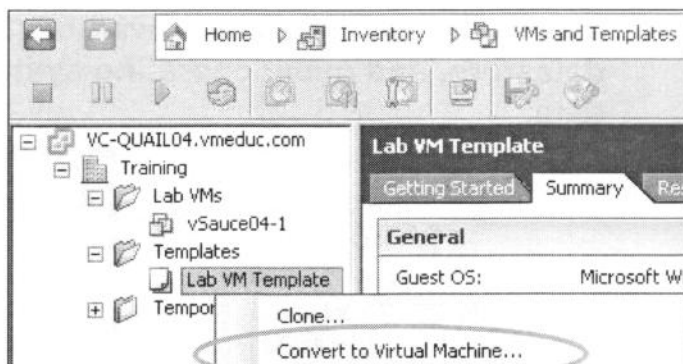
Templates are distinguished from virtual machines by their icon.

Updating a Template

Slide 7-37

To update a template:

1. Convert the template to a virtual machine.
2. Place the virtual machine on an isolated network to prevent user access.
3. Make appropriate changes to the virtual machine.
4. Convert the virtual machine back to a template.



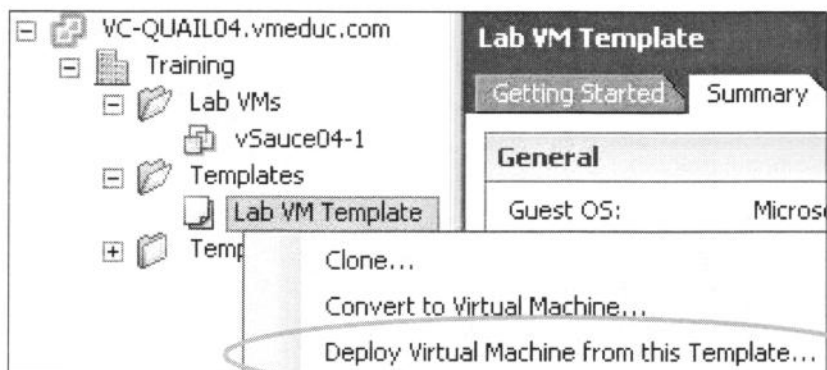
If you need to update your template to include new patches or software, you do not have to create a brand-new template. Instead, first convert the template back to a virtual machine. This allows you to power on the virtual machine. For added security, place the virtual machine on an isolated network to prevent users from accessing it while you are updating the virtual machine. Log in to the virtual machine's guest operating system and apply the patch or install additional software—whatever is necessary. When that is done, convert the virtual machine back to a template.

To convert a template back to a virtual machine, navigate to the VMs and Templates inventory view. Right-click the template, then choose **Convert to Virtual Machine**.

Deploying a Virtual Machine from Template

Slide 7-38

To deploy a virtual machine, provide such information as virtual machine name, inventory location, host, datastore, and guest operating system customization data.



To deploy a virtual machine from a template, navigate to the VMs and Templates inventory view. Right-click the template, then choose **Deploy Virtual Machine from this Template**. The Deploy Template wizard asks you for virtual machine deployment information. You also have the option of having vCenter Server customize the guest operating system for you.

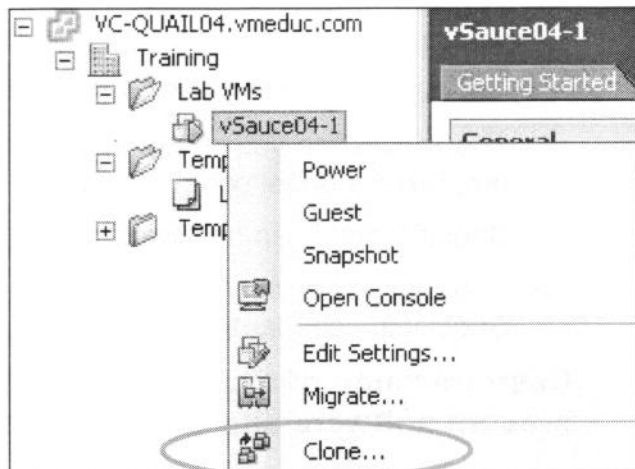
Cloning a Virtual Machine

Slide 7-39

Cloning is an alternative to deploying a virtual machine.

A clone is an exact copy of the virtual machine.

The virtual machine being cloned can either be powered on or powered off.



Cloning a virtual machine is an alternative to deploying a virtual machine from a template. As when deploying from template, when you clone, you have the option of customizing the guest operating system in the clone. The virtual machine can either be powered on or powered off.

To clone a virtual machine, right-click your virtual machine in the inventory, then choose **Clone**.

Customizing the Guest Operating System

Slide 7-40

During cloning or deploying from template, you have the option of running the Guest Customization wizard.

- > The wizard lets you create a specification you can use to prepare the guest operating systems of virtual machines.
- > Specifications can be stored in the database.
- > You can edit existing specifications using the Customization Specifications Manager.

Customization of a clone's guest is recommended to prevent software and network conflicts.

The Guest Customization wizard allows you to create specifications that you can use to prepare the guest operating systems of virtual machines to function in a target environment.

You can store specifications in the database to customize the guest operating system of a virtual machine during the cloning or deploying process. Use the Customization Specification Manager to manage customization specifications that you create with the Guest Customization wizard.

To enable guest operating system customization, vCenter Server must first be configured for this task.

To customize Windows virtual machines, you install Microsoft sysprep files on the vCenter Server system.

For example, for Windows 2003:

- Retrieve the installer for Microsoft Windows 2003 sysprep from the Microsoft Web site.
- Copy the files from the .cab file, `WindowsServer2003-KB892778-SP1-DeployTools-x86-ENU.cab`, to `C:\Documents and Settings\ALLUSERSPROFILE\Application Data\VMware\VMware VirtualCenter\sysprep\svr2003`.

For more details on how to prepare for guest customization, see *vSphere Basic System Administration Guide* at <http://www.vmware.com/support/pubs>.

Deploying Virtual Machines Across Datacenters

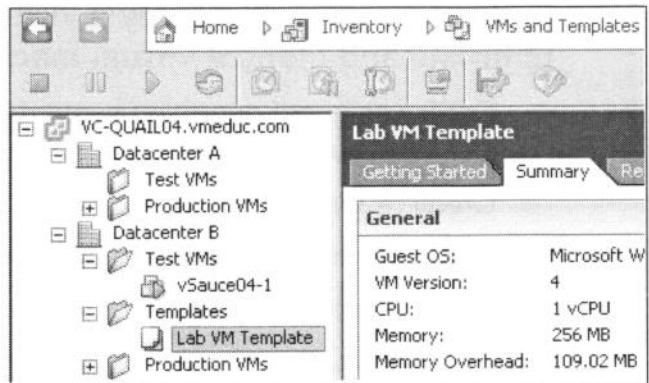
Slide 7-41

Virtual machine deployment is allowed across datacenters.

- > Clone a virtual machine from one datacenter to another.
- > Deploy from a template located in one datacenter to a virtual machine in a different datacenter.

For example:

- > Clone Prod01 from Datacenter A to Datacenter B.



vCenter Server allows you to provision virtual machines across datacenters. Administrators can clone a virtual machine from one datacenter to another datacenter. Administrators can also create a template in one datacenter and then deploy a virtual machine from that template, placing the virtual machine in a different datacenter.

In the example above, an administrator can clone the virtual machine named Prod01, which is located in Datacenter A, to a host in Datacenter B.

Lab 10

Slide 7-42

In this lab, you will deploy a virtual machine from a template and clone a virtual machine.

1. Configure guest operating system customization on vCenter Server system.
2. Create a template.
3. Deploy a virtual machine from a template.
4. Clone a virtual machine that is powered on.

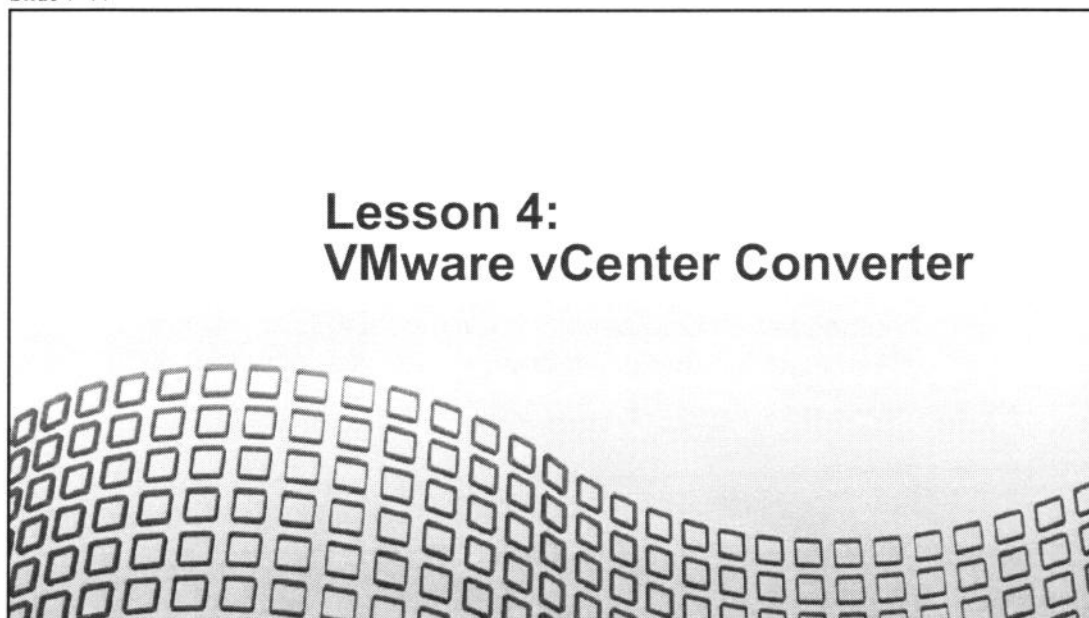
Lesson Summary

Slide 7-43

- > A template is a master copy of a virtual machine used to create and provision new virtual machines.
- > Deploying a virtual machine from template should be the preferred method for provisioning virtual machines, over creating a virtual machine using the Create Virtual Machine wizard.
- > Another way to provision a virtual machine is to clone a virtual machine that is either powered on or powered off.

Lesson 4: VMware vCenter Converter

Slide 7-44



Lesson Objectives

Slide 7-45

- Describe the capabilities of vCenter Converter
- Import a system into vCenter Server
- Describe hot cloning and cold cloning

vCenter Converter Capabilities

Slide 7-46

vCenter Converter is a vCenter Server additional module used to import, export, or reconfigure physical or virtual machines or system images.

- Convert the following types of systems to virtual machines and import them into vCenter Server:
 - Physical machines
 - Virtual machines, such as VMware Workstation, Microsoft Virtual Server 2005, and Windows Server 2008 Hyper-V
 - Third-party backups or disk images
- Restore VMware Consolidated Backup images to virtual machines.
- Export vCenter Server virtual machines to other VMware virtual machine formats.
- Customize virtual machines (for example, change the host name or network settings).

A standalone version of vCenter Converter is also available.

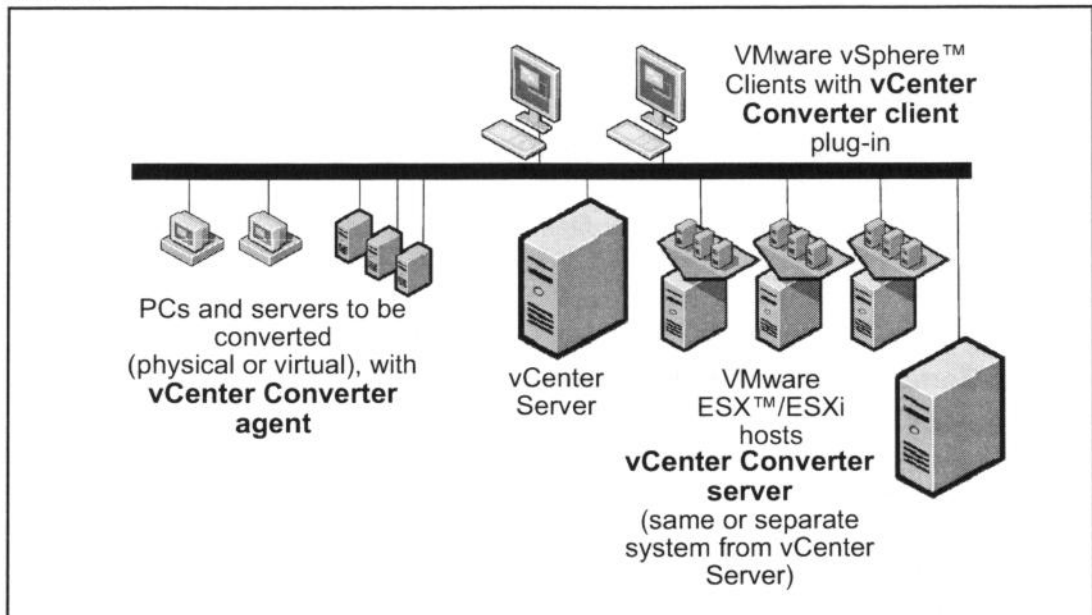
Migration with VMware vCenter Converter involves cloning the source machine or image and exporting it to a destination. You can convert virtual machines that vCenter Server manages to different VMware virtual machine formats and export those virtual machines for use with other VMware products. You can use vCenter Converter to perform the following tasks:

- Convert physical machines to virtual machines and import the virtual machines to vCenter Server
- Convert and import virtual machines, such as VMware Workstation or Microsoft Virtual Server 2005 to vCenter Server
- Convert third-party backup or disk images to vCenter Server virtual machines
- Restore VMware Consolidated Backup images to vCenter Server virtual machines
- Export vCenter Server virtual machines to other VMware virtual machine formats
- Reconfigure vCenter Server virtual machines so that they are bootable
- Customize vCenter Server machines (for example, change the host name or network settings)

A standalone version of vCenter Converter is available. VMware vCenter Converter Standalone has similar functionality, but it is not integrated into vCenter Server.

vCenter Converter Components

Slide 7-47



Depending on the vCenter Converter component you install, you can perform hot or cold cloning, use a command-line interface, or use the vCenter Converter wizard from within vSphere Client. vCenter Converter includes the following components:

- **vCenter Converter server** – Enables the import and export of virtual machines using the vSphere Client or the vCenter Converter CLI. Install the vCenter Converter server on vCenter Server or on an independent machine with access to vCenter Server.
vCenter Converter CLI – Provides a command-line interface to operate the vCenter Converter server. You can install the vCenter Converter CLI on the same machine as a vCenter Converter server or on another machine that has access to a vCenter Converter server.
- **vCenter Converter agent** – Prepares a physical machine for import from a remote machine running a vCenter Converter server. The vCenter Converter server installs the agent on physical machines only to import them as virtual machines. You can choose to automatically remove the vCenter Converter agent from the physical machine after the importation is complete.
- **vCenter Converter client** – Works with the vCenter Converter server. The client component consists of the vCenter Converter client plug-in, which provides access to the vCenter Converter Import, Export, and Reconfigure wizards from within a vSphere Client.
- **vCenter Converter boot CD** – Enables cold cloning of physical machine.

vCenter Converter Requirements

Slide 7-48

Install vCenter Converter on the vCenter Server system or on a separate system.

Allocate disk space for the various vCenter Converter components:

- > vCenter Converter server files, vCenter Converter CLI, vCenter Converter agent files, vCenter Converter client files, and the installers
- > Approximately 300MB of disk space is needed for all components.

Memory requirements depend on whether hot or cold cloning is performed

- > Hot cloning – 350MB of memory is required on source physical machine.
- > Cold cloning – At least 264MB of memory is required on source physical machine; 364MB or more is preferred.

vCenter Converter supports installation on a variety of platforms. The installation space requirements differ, depending on the vCenter Converter components that you install. vCenter Converter requires a connection to vCenter Server. You can install vCenter Converter on the same computer as vCenter Server or on another computer that has access to vCenter Server. You can install vCenter Converter on a number of Microsoft Windows operating systems.

During installation you can choose which vCenter Converter components to install. Individual components have different disk space requirements for installation.

The vCenter Converter client is installed as a plug-in for vSphere Client. You access the Import, Export, and Reconfigure wizards from the client to setup your migrations.

The operating system on which you install vCenter Converter server determines which virtual machines and third-party images you can import, export, and reconfigure.

Memory requirements differ, depending on the type of cloning you are performing. For hot cloning, vCenter Converter requires 350MB of free space on the source physical machine. For cold cloning with the vCenter Converter boot CD, the source physical machine must also meet certain memory requirements.

For details on the vCenter Converter system requirements, see the *vCenter Converter Administration Guide* at <http://www.vmware.com/support/pubs>.

Importing a Physical System

Slide 7-49

Cloning and system reconfiguration steps are used to create and reconfigure the virtual machine.

- Cloning – Create a cloned disk, where the cloned disk is a virtual disk that is an exact copy of the source physical disk.
- System reconfiguration – Adjust the migrated operating system to enable it to function on virtual hardware.

vCenter Converter supports hot cloning and cold cloning:

- Hot cloning – Clone a source machine while the operating system is running. The source machine can be accessed remotely.
- Cold cloning – Clone the source machine when the operating system is not running. Cloning can be performed locally, where Converter runs on the source machine.

vCenter Converter uses cloning and system reconfiguration to create virtual machines that are compatible with ESX/ESXi hosts.

Cloning is the process of creating a cloned disk, where the cloned disk is a virtual disk that is an exact copy of the source physical disk. This involves copying the data on the source machine's hard disk and transferring that data to a target virtual disk (the new cloned disk).

System reconfiguration is the process of adjusting the migrated operating system to enable it to function on virtual hardware. This adjustment is performed on the target virtual disk after cloning and enables the target virtual disk to function as a bootable system disk in a virtual machine.

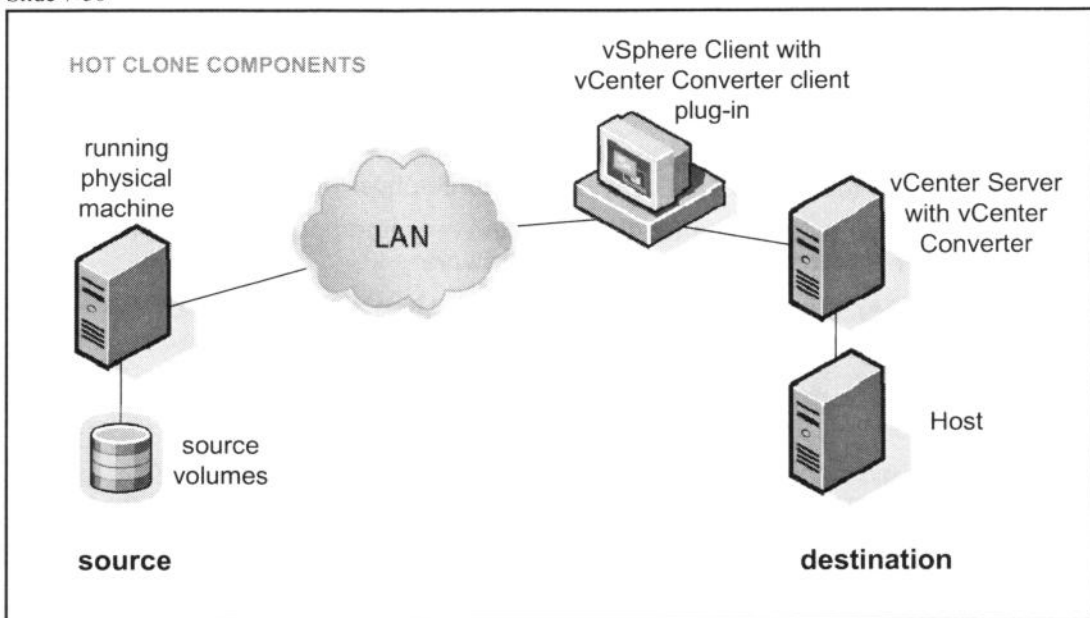
The process is nondestructive, so you can continue to use the original source machine after the import completes. If you plan to run an imported virtual machine on the same network as the source physical machine, modify the network name and IP address on one of the machines so that the physical and virtual machines can coexist properly.

Hot cloning, also called live cloning or online cloning, entails cloning the source machine while it is running its operating system.

Cold cloning, also called offline cloning, entails cloning the source machine when it is not running its operating system. With cold cloning, the user reboots the source machine from the vCenter Converter boot CD.

Remote Hot Cloning of a Physical Machine

Slide 7-50



Hot cloning is usually performed remotely. With remote cloning, the source machine can be accessed via an agent without having to physically touch it, as long as it is running and network-accessible. Remote cloning installs, uses, and then uninstalls an agent.

Four stages occur during a hot-cloning operation. All stages are performed by vCenter Converter without user involvement after the user has created and initiated the task.

The first stage is to prepare the source machine for conversion. vCenter Converter server installs the vCenter Converter agent on the source machine. The agent then takes a snapshot of the source volumes.

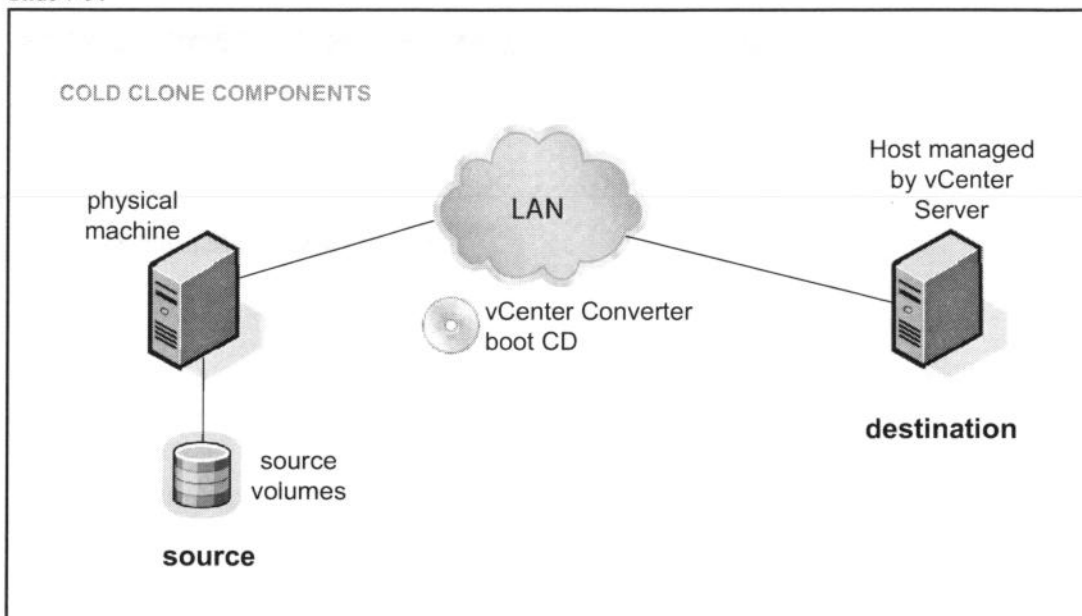
The second stage is to prepare the virtual machine on the destination machine. vCenter Converter server creates a new virtual machine on the destination ESX/ESXi host. The vCenter Converter agent copies volumes from the source machine to the destination host.

The third stage is to complete the conversion process. vCenter Converter agent installs required drivers to allow the operating system to boot in the virtual machine. vCenter Converter agent customizes the virtual machine; for example, it changes IP information.

The fourth stage is to clean up. The agent removes all traces from the source machine. The snapshot created in stage 1 is deleted, and the vCenter Converter agent is uninstalled from the source machine. You have the option of uninstalling the agent automatically or manually.

Local Cold Cloning of a Physical Machine

Slide 7-51



Cold cloning is usually performed locally. With *local cloning*, the migration is performed using the vCenter Converter boot CD running on the source machine.

Four stages occur during a cold-cloning operation. After the user boots from the vCenter Converter boot CD and uses the wizard to set up and run the task, vCenter Converter performs the remaining steps without user involvement.

The first stage is to prepare the source machine image. The user boots the source machine from the vCenter Converter boot CD and uses vCenter Converter to define and start the migration. vCenter Converter copies the source volumes into a RAM disk.

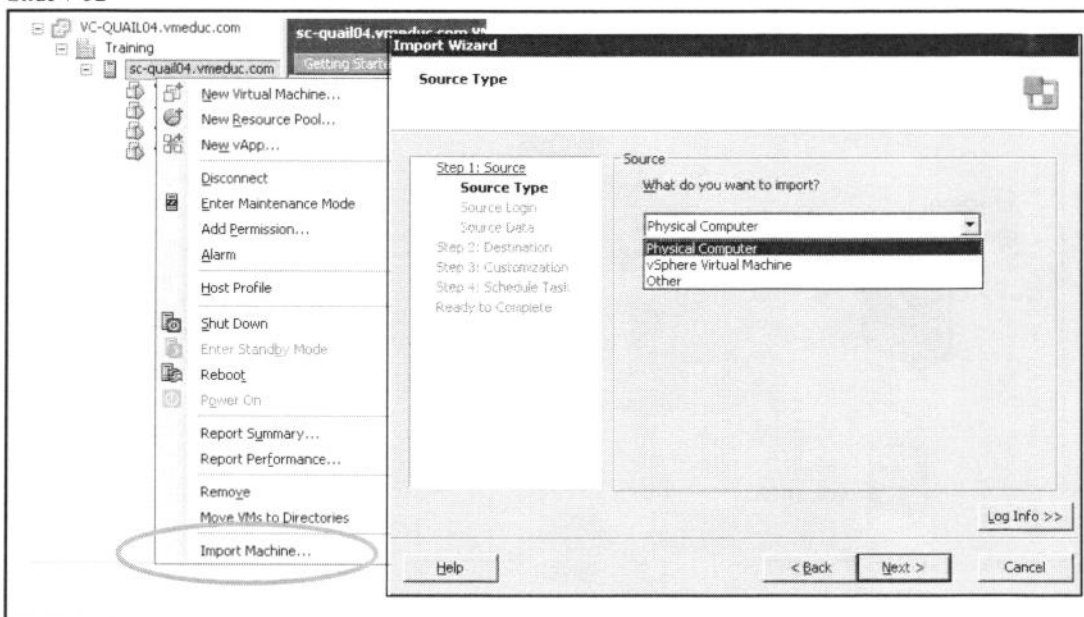
The second stage is to prepare the virtual machine on the destination machine. vCenter Converter creates a new virtual machine on the destination machine. vCenter Converter copies volumes from the source machine to the destination machine.

The third stage is to complete the conversion process. vCenter Converter installs the required drivers to allow the operating system to boot in a virtual machine. vCenter Converter customizes the virtual machine; for example, it changes the IP configuration.

The fourth stage is to clean up. The user removes the boot CD and reboots the source physical machine into its own operating system. The virtual machine is ready to run on the destination machine.

Importing a Physical System

Slide 7-52



The vCenter Converter Import wizard allows you to import physical machines, virtual machines, or backup/disk images. It is used during both hot cloning and cold cloning.

To launch the import wizard, right-click your ESX/ESXi host in the inventory, then choose **Import Machine**. The Import Machine selection is available only if you download and install the vCenter Converter plug-in into the vSphere Client.

The Import wizard prompts you for information about the source and destination machines and to select the task parameters for the conversion. The wizard is context-sensitive. You must complete the steps in the wizard to start an import task.

Cloning Modes: Disk-Based and Volume-Based

Slide 7-53

Disk-based cloning

- > Transfers all sectors from all disks and preserves all volume metadata. It supports all basic and dynamic disks.
- > Used for cold cloning and importing existing virtual machines

Volume-based cloning

- > Creates all volumes in the destination virtual machine as basic volumes, regardless of type of corresponding source volume
- > Used for hot and cold cloning and for importing existing virtual machines
- > Performed at the file or block level, depending on your size selections

vCenter Converter supports two cloning modes: disk-based cloning and volume-based cloning.

vCenter Converter supports disk-based cloning for cold cloning and for importing existing virtual machines. Disk-based cloning transfers all sectors from all disks and preserves all volume metadata. The destination virtual machine receives the same volumes of the same type as the volumes of the source virtual machine. Disk-based cloning supports all basic and dynamic disks.

vCenter Converter supports volume-based cloning for hot and cold cloning and for importing existing virtual machines. In volume-based cloning, all volumes in the destination virtual machine are basic volumes, regardless of the type in the corresponding source volume. Volume-based cloning is performed at the file level or block level, depending on your size selections:

- Volume-based cloning at the file level is performed when you specify a size smaller than the original volume.
- Volume-based cloning at the block level is performed when you specify the same or a larger volume size.

Depending on the cloning mode, some types of source volumes might not be supported:

- Cold cloning with the vCenter Converter boot CD supports all types of dynamic volumes and Windows NT 4 with mirrored volumes. Windows NT 4 fault-tolerant volumes are not supported.

- Virtual machine importing supports basic volumes and all types of dynamic volumes, except RAID. It does not support Windows NT 4 fault-tolerant volumes. It does support Windows NT 4 with mirrored volumes. Only master boot record (MBR) disks are supported. GUID partition table (GPT) disks are not supported.
- Hot cloning supports all types of source volumes that Windows recognizes.

Changes to Virtual Hardware

Slide 7-54

Most applications function correctly.

Watch for applications that depend on:

- > Specific hardware characteristics
- > Different serial numbers
- > Software licensed to MAC addresses
- > Special graphics cards

Most applications should function correctly in the virtual machine because their configuration and data files have the same location as they did on the source virtual machine. However, applications might not work if they depend on specific characteristics of the underlying hardware, such as the serial number or the device manufacturer, or on devices that are not available within the virtual machine.

When troubleshooting after virtual machine migration, notice the following potential hardware changes:

- The CPU model and serial numbers (if activated) can be different after the migration. They correspond to the physical computer hosting the VMware virtual machine.
- The Ethernet adapter can be different (AMD PCNet or vmxnet) with a different MAC address. Each interface's IP address must be individually reconfigured.
- The graphics card can be different (VMware SVGA card).
- The numbers of disks and partitions are the same, but each disk device can have a different model and different manufacturer strings.
- The primary disk controllers can be different from the source machine's controllers.

Settings that remain identical include operating system configuration, computer name, SID, user accounts, profiles, preferences, applications and data files, and the volume serial number of each disk partition.

Lab 11 and eLearning Activity

Slide 7-55

In this lab, you will use vCenter Converter to create a virtual machine from an existing system.

1. Prepare a system for hot cloning.
2. Hot-clone a system.

In this eLearning activity, you will view a self-paced demonstration on how to convert a physical machine to a virtual machine using the vCenter Converter boot CD.

➤ <http://mylearn.vmware.com/register.cfm?course=38260>

Lesson Summary

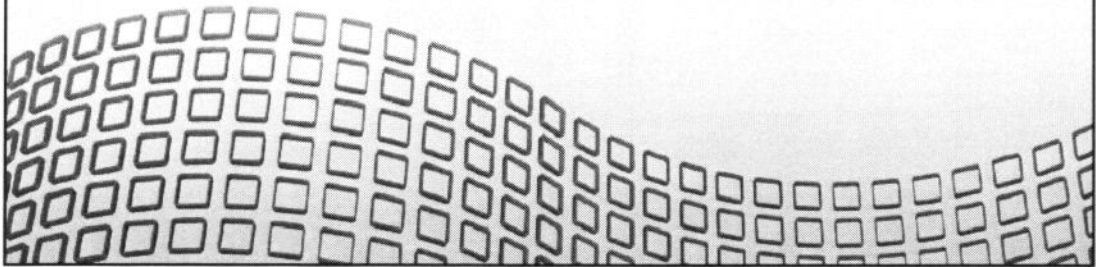
Slide 7-56

- > vCenter Converter is a vCenter Server additional module used to import, export, or reconfigure physical or virtual machines or system images.
- > vCenter Converter can also be used to restore Consolidated Backup images to virtual machines.
- > Cloning of a physical machine can be done in a hot mode, while the physical machine continues to run.

Lesson 5: vCenter Guided Consolidation

Slide 7-57

Lesson 5: vCenter Guided Consolidation



Lesson Objectives

Slide 7-58

- > Describe the Guided Consolidation architecture
- > Understand how Guided Consolidation works
 - Find physical systems
 - Analyze physical systems
 - Convert physical systems to virtual machines

Guided Consolidation

Slide 7-59

Guided Consolidation enables you to streamline your datacenter by transforming your physical machines, running business applications, into virtual machines.

- Recommended for small IT environments

Consolidating your datacenter involves the following:

- Find – Search for and select physical systems that you want analyzed.
- Analyze – Analyze the physical systems and collect performance data.
- Consolidate – Compare performance to available host resources, convert physical systems to virtual machines, and import virtual machines into vCenter Server.

VMware vCenter Guided Consolidation, recommended for smaller IT environments, enables you to streamline your datacenter by moving business applications, spread across multiple disparate physical systems, into a centrally managed virtual environment.

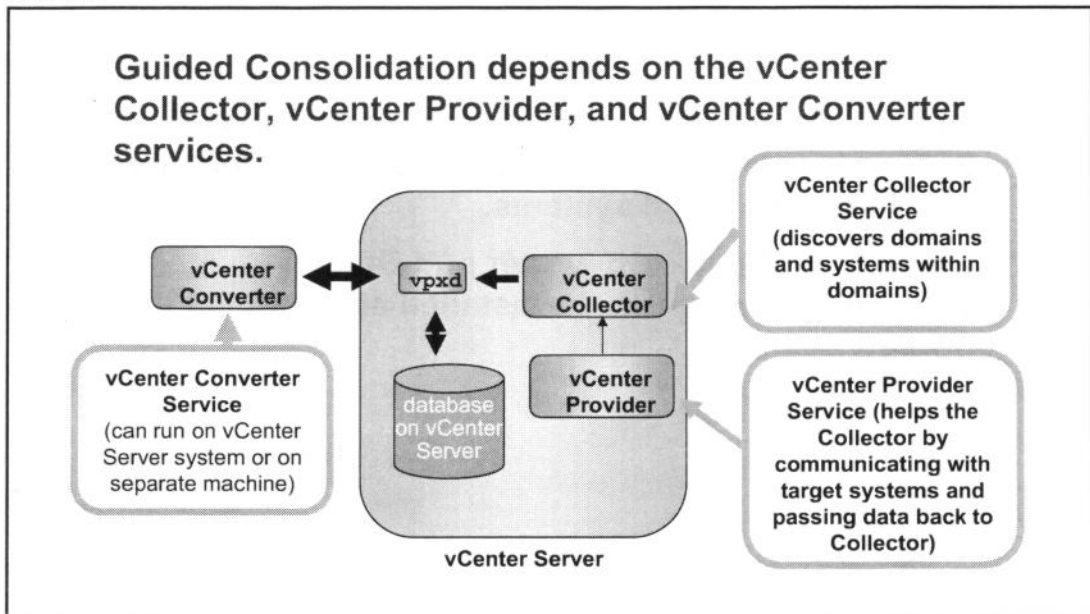
In the virtualized environment, the physical systems that run your business applications are transformed into virtual machines. Multiple virtual machines can be hosted on a single physical system, enabling more efficient use of computing resources. Consolidating your datacenter involves the following process:

- Find – You search for and select the physical systems in your datacenter that you want analyzed.
- Analyze – Selected physical systems are analyzed and performance data on each selected system is collected. Generally, the longer the duration of the analysis phase, the higher the confidence in vCenter Server recommendations.
- Consolidate – Performance data is compared to the resources available on the virtual machine host systems. The selected physical systems are converted to virtual machines and imported into vCenter Server on the recommended hosts, where they are managed along with other components of your virtual environment.

Use the consolidation feature to start building your virtual environment or to further consolidate your datacenter as it grows.

Guided Consolidation Architecture

Slide 7-60



Guided Consolidation can be installed together with vCenter Server, or it can be installed on a separate system. For best performance, install Guided Consolidation on a separate system.

Guided Consolidation include the following services:

- vCenter Collector Service – Discovers domains and systems within domains. Collects performance data on those systems.
- vCenter Provider Service – Helper service to vCenter Collector Service. Communicates with target systems and passes the data back to vCenter Collector Service.
- vCenter Guided Consolidation – Coordinates all communication among Guided Consolidation components. Saves the performance data collected by the vCenter Collector Service. Analyzes the data and generates placement recommendations. Also communicates with vCenter Server to perform conversion. Runs inside a generic servlet container labeled VMware vCenter Management Webservices. The services of other vCenter Server features and extensions might also be present inside that servlet container.

Guided Consolidation Prerequisites

Slide 7-61

Guided Consolidation requires that your VMware vSphere is populated and that you provide credentials to the target physical systems.

Ensure that vCenter Converter and Guided Consolidation plug-ins are installed and enabled in the vSphere Client.

Guided Consolidation requires that your vSphere is populated and requires that you provide credentials to the target physical systems. This section lists the prerequisites for using the feature. Guided Consolidation can convert systems configured to any locale. Before you use the feature, ensure that the following prerequisites are met:

- Guided Consolidation must be installed and enabled on the vSphere Client.
- During installation, you must provide credentials that have administrator and Log on as service privileges on the system where Guided Consolidation is installed. If Active Directory is deployed on your network, the provided credentials must also have sufficient privileges to query the Active Directory database.
- At least one datacenter inventory object exists.
- At least one host is registered with vCenter Server.
- Guided Consolidation also requires administrator access to the systems selected for analysis. Specifically, the vCenter Collector Service uses these credentials to connect to and retrieve configuration and performance data from the physical systems under analysis.
- Ensure that the Guided Consolidation extension is installed and enabled in the vSphere Client.

For further details on the Guided Consolidation prerequisites, see the *vSphere Basic System Administration Guide* at <http://www.vmware.com/support/pubs>.

Finding Physical Systems to Consolidate

Slide 7-62

Click **Start Analysis** to find systems on the network to analyze.

Guided Consolidation
Which physical computers should you virtualize to best consolidate your physical computer virtualization. Click Start Analysis to add computers to analysis.

Start Analysis

Search for systems by computer name or IP address, or within a domain.

Add to Analysis
Enter the physical computers to consider for consolidation. Click Add to Analysis to begin analyzing these computers and to determine if they are good candidates for consolidation.

☒ Manually specify the computers.

Computer Name(s):
IP Address(es):
(example: hostname.domain.com, a.b.c.d, 192.168.1.1)

IP Range:
(example: a.b.c.x - a.b.c.y)

File Name:
(list of computer names or IP addresses, one per line)

☐ Select the computers by domain

Domain:

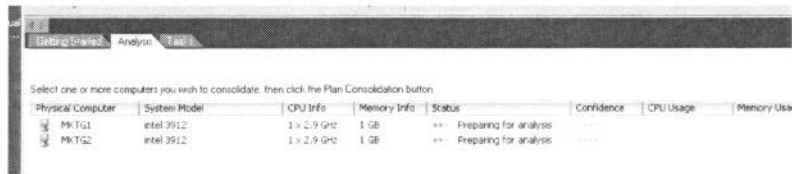
Name or Analysis contains:

The Add to Analysis dialog box enables find systems in your environment and add them for analysis. manually search for physical systems, or to select systems from the list the physical systems found in active domains. You can select systems and add them for analysis.

You can add systems manually by entering a computer name, IP address or range of IP addresses, or file name. Alternatively, you can select a domain—it must be active—and select systems found within that domain. You can analyze up to 100 systems simultaneously.

Analyzing Potential Candidates

Slide 7-63



Select one or more computers you wish to consolidate; then click the Plan Consolidation button.

Physical Computer	System Model	CPU Info	Memory Info	Status	Confidence	CPU Usage	Memory Usage
M1TG1	intel 3912	1 x 2.9 GHz	1 GB	Preparing for analysis
M1TG2	intel 3912	1 x 2.9 GHz	1 GB	Preparing for analysis

Statistics are collected on each host.

- > 10–12 metrics total: CPU, memory, disk, network
- > Columns populated as information obtained

Data is compared to host resources to get recommendation.

Confidence metric is calculated.

- > Refers to the reliability of the recommendation
- > Recommendations based on longer periods of analysis, and therefore more performance data, receive a higher level of confidence

Analysis results are displayed in the **Analysis** tab. When analysis is complete, the following information appears:

- **Physical Computer** – Displays the host name of the physical system being analyzed
- **CPU Info** – Displays the number of CPUs and their clock speed
- **Memory Info** – Displays the amount of RAM on the system
- **Status** – Displays the progress of the analysis
- **Confidence** – Indicates how good a candidate the system is based on the available data
- **CPU Usage and Memory Usage** – Display the system's average CPU and memory usage over time

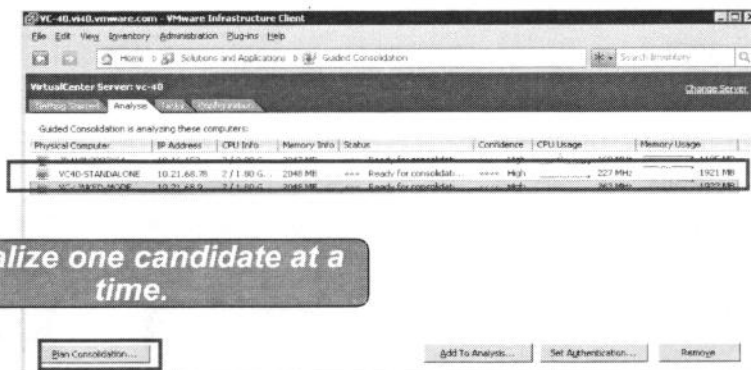
The **Confidence** metric is important. During the analysis phase, performance data about each selected system is collected. This data is used to find a host with resources that match the collected data to determine a recommendation for each candidate.

The recommendation indicates how well suited, based on the collected data, a candidate is to a particular virtual machine host system. Confidence refers to the reliability of the recommendation, and it is a function of the duration of the analysis. Recommendations based on longer periods of analysis—and therefore more performance data—have a higher level of confidence.

Consolidating Candidates

Slide 7-64

After analysis, select the systems you want to convert.
vCenter Server selects appropriate destinations and configuration parameters for each resulting virtual machine.



After the analysis phase, you are ready to plan consolidation. In the **Analysis** tab, you select the systems you want to consolidate and then click the **Plan Consolidation** button (not shown above). A list of analyzed systems is presented. For each system, the candidate destination ESX/ESXi hosts are identified. Each destination is has a star rating.

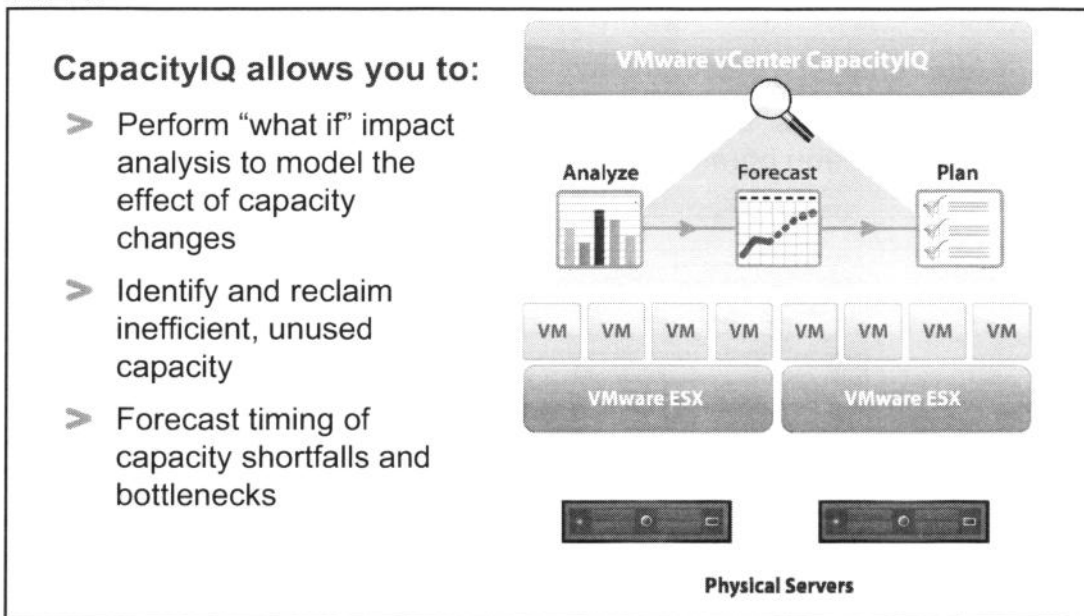
The number of stars displayed in the **Destination Rating** column indicates the degree to which the host system can comfortably accommodate the estimated resource needs of the resultant virtual machine. The rating is based on the average CPU usage, memory usage, and disk space usage of the destination host. The networking check verifies only the number of NICs, not network usage.

The higher the star rating, the better suited that destination host is for consolidation.

When ready, you select the systems to import. For each one, you select the destination host and click the **Consolidate** button. The importation is performed by the vCenter Converter service.

Capacity Planning with vCenter CapacityIQ

Slide 7-65



VMware vCenter CapacityIQ is a planning tool to help you plan your virtualized datacenter capacity.

CapacityIQ allows you to do the following:

- Perform “what if” impact analysis to model the effect of capacity changes – CapacityIQ allows you to model various scenarios to understand the different outcomes. With the right capacity intelligence, you can make informed planning, purchasing, and provisioning decisions for your datacenter.
- Identify and reclaim inefficient, unused capacity – CapacityIQ helps you quickly identify any overallocated, idle, or inactive virtual machines in your datacenter. By right-sizing or decommissioning these virtual machines, you can safely free up any unused capacity to eliminate waste and reduce costs.
- Forecast timing of capacity shortfalls and bottlenecks – CapacityIQ continuously profiles, analyzes and tracks your capacity needs at multiple levels: virtual machine, host, cluster, and datacenter. Based on historical capacity consumption patterns, CapacityIQ trends and forecasts your current and future capacity needs, ensuring that capacity is always available and service levels are met.

eLearning Activity

Slide 7-66

In this eLearning activity, you will view a self-paced demonstration of how to analyze a physical machine and convert the physical machine to a virtual machine using Guided Consolidation.

> <http://mylearn.vmware.com/register.cfm?course=38265>

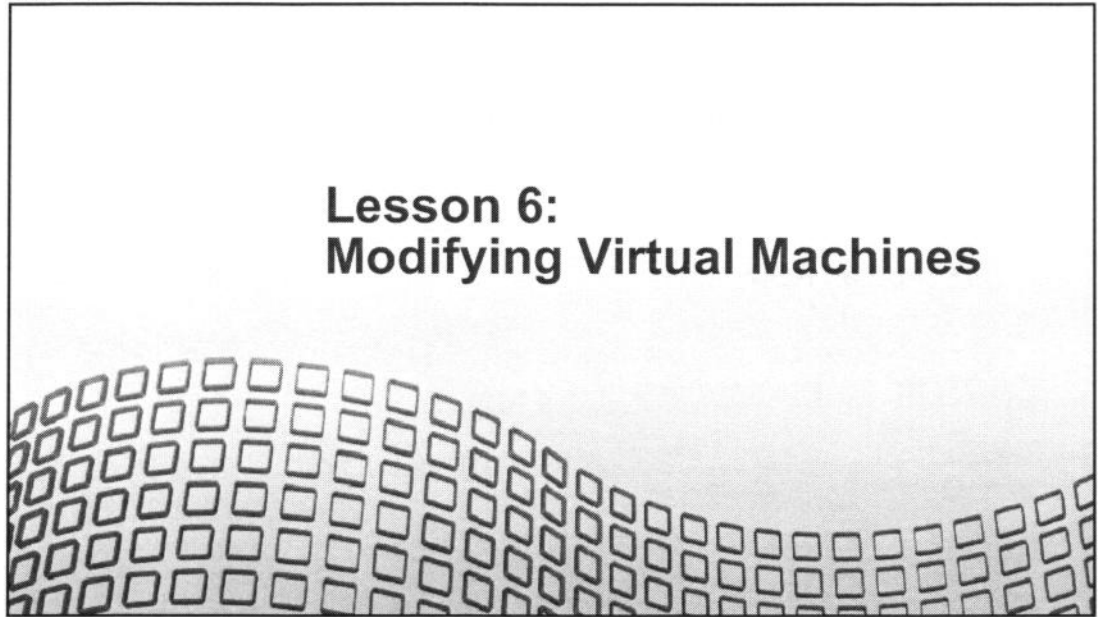
Lesson Summary

Slide 7-67

- Guided Consolidation allows you to consolidate your datacenter by
 - Finding physical systems in one or more domains
 - Analyzing these physical systems for potential consolidation candidates
 - Converting the best candidates to virtual machines and importing them into vCenter Server

Lesson 6: Modifying Virtual Machines

Slide 7-68



Lesson Objectives

Slide 7-69

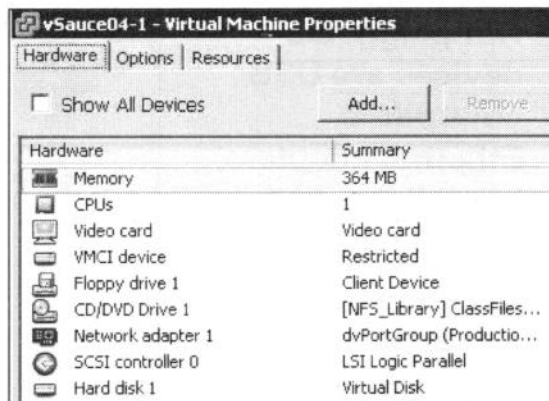
- > Understand the various virtual machine settings and options
- > Add a hot-pluggable device
- > Increase the size of a virtual disk using Hot Extend
- > Add an RDM

Modifying Virtual Machine Settings

Slide 7-70

A virtual machine's configuration can be modified using its Properties dialog box.

- > Add virtual hardware.
 - Some hardware can be added while the virtual machine is powered on.
- > Remove virtual hardware.
- > Set virtual machine options.
- > Control a virtual machine's CPU and memory resources.



It might be necessary to modify a virtual machine's configuration; for example, to add another network adapter or to add another virtual disk. All virtual machine changes can be made while the virtual machine is powered off. However, some hardware changes can be made to the virtual machine while it is powered on.

In addition to adding virtual hardware, you can also remove virtual hardware and set various virtual machine options.

All virtual machine configuration is done using the virtual machine's Properties dialog box. To display a virtual machine's properties, right-click your virtual machine in the inventory, then choose **Edit Settings**. The virtual machine Properties dialog box appears, as shown above.

The **Hardware** tab is used to modify the hardware on the virtual machine.

The **Options** tab is covered later in this lesson.

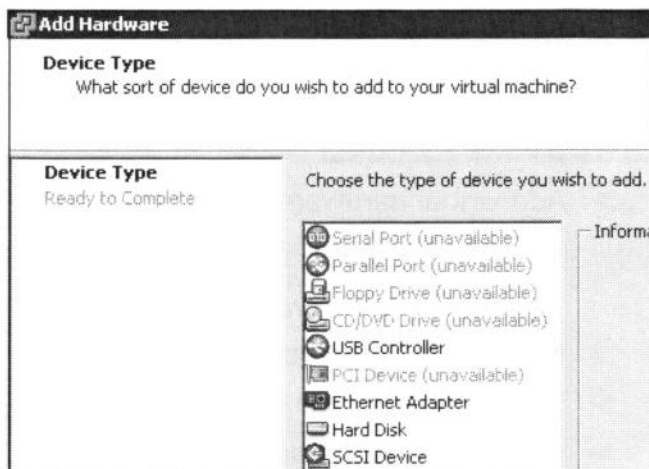
The **Resources** tab is covered in a later module.

Hot-Pluggable Devices

Slide 7-71

Hot-pluggable devices are USB controllers, Ethernet adapters, hard disks, and SCSI devices.

CPU and memory can also be added while the virtual machine is powered on.



To add hardware to your virtual machine, in the virtual machine Properties dialog box, click **Add**. The list of devices you are allowed to add depends on whether the virtual machine you selected is powered on or powered off.

In the example, the virtual machine is powered on. Therefore, the devices you are allowed to add while the virtual machine is powered on are USB controllers, Ethernet adapters, hard disks, and SCSI devices. These devices are known as hot-pluggable devices because they can be added to a virtual machine that is up and running.

Increasing Virtual Disk Size: Hot Extend Feature

Slide 7-72

Hot Extend

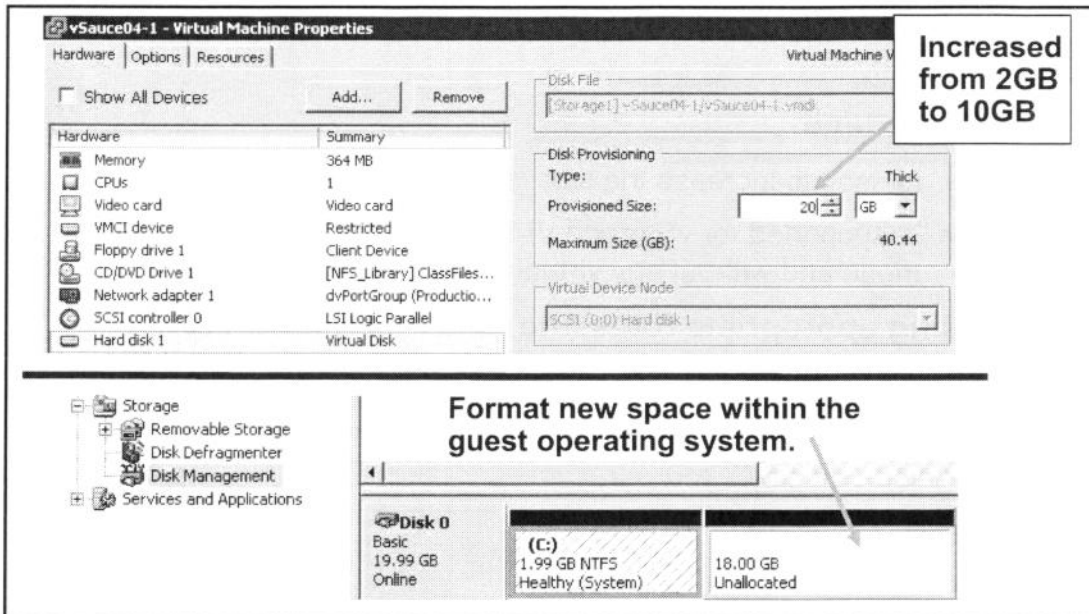
- Is used to increase the size of a virtual disk
- Is supported for vStorage VMFS flat virtual disks in persistent mode and without any virtual machine snapshots.

Using appropriate tools, the guest operating system can dynamically grow the file system to use this new allocated disk space.

With the Hot Extend feature, it is also possible to increase the size of a virtual disk while the virtual machine is up and running. With Hot Extend, you can increase the size of any virtual disk belonging to the virtual machine as long as it is a flat virtual disk in persistent mode and the virtual machine does not have any snapshots.

Hot Extend Example

Slide 7-73



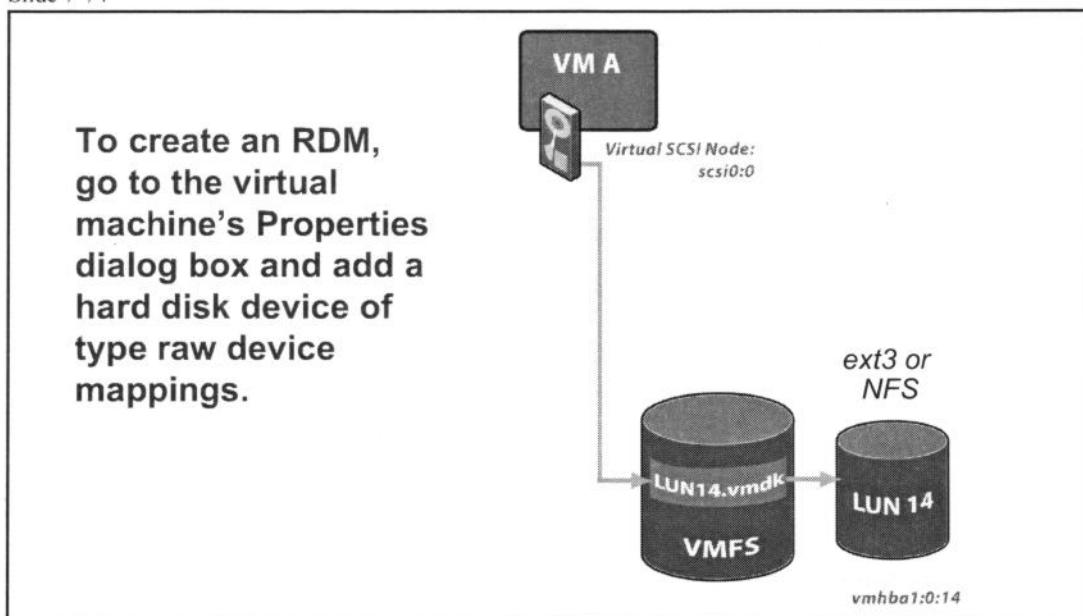
To increase the size of a virtual disk, display the virtual machine's properties (right-click the virtual machine, then choose **Edit Settings**). Select the desired hard disk in the **Hardware** pane. In the resulting **Disk Provisioning** panel, enter the new size for the hard disk.

After you increase the size of a virtual disk, you must use the appropriate tool within the guest operating system itself to allow the file system on this disk to use the newly allocated disk space. For example, use the `diskpart` utility in a Windows 2003 guest operating system.

Creating a Raw Device Mapping

Slide 7-74

USE RARELY



When you map a LUN to a VMFS volume, vCenter Server creates a file that points to the raw LUN. Encapsulating disk information in a file allows vCenter Server to lock the LUN so that only one virtual machine can write to it.

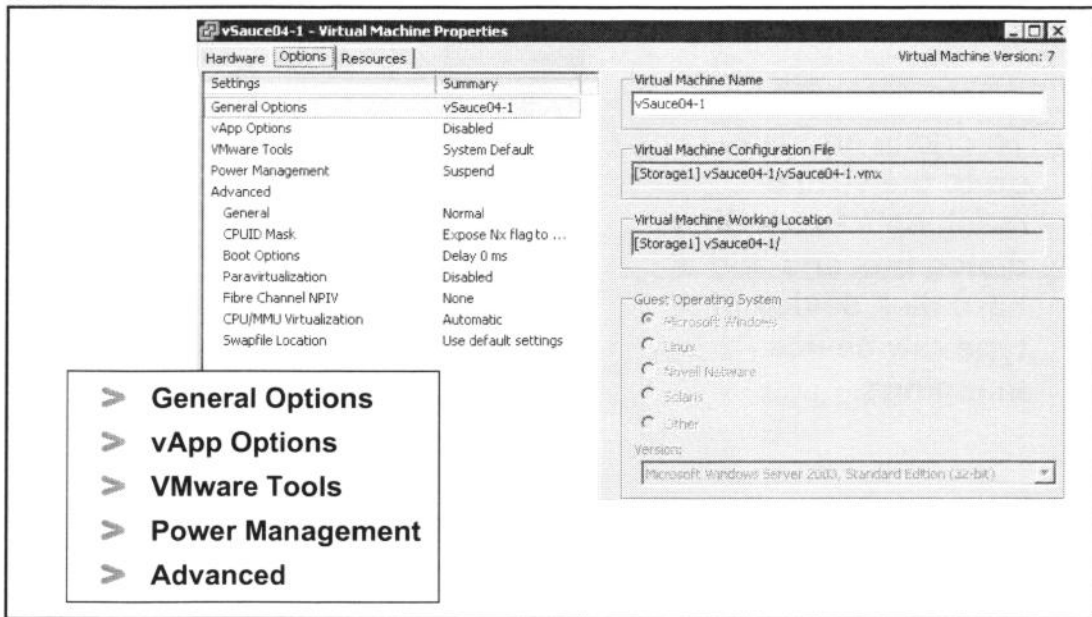
The RDM is a file that has a `.vmdk` extension, but the file contains only disk information describing the mapping to the LUN on the ESX/ESXi host. The actual data is stored on the LUN. Also note that you cannot deploy a virtual machine from a template and store its data on a LUN; you can store its data only in a virtual disk file.

To create an RDM, go to the Virtual Machine Properties dialog box and click **Add**. Add a hard disk of type raw device mappings. Then select the LUN that the RDM will map to. You will also be asked to select a compatibility mode:

- **Physical compatibility mode** – Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications in the virtual machine. However, a LUN configured for physical compatibility cannot be cloned, made into a template, or migrated if the migration involves copying the disk.
- **Virtual compatibility mode** – Allows the virtual machine to use VMware snapshots and other advanced functionality. Virtual compatibility allows the LUN to behave as if it were a virtual disk. When you clone the disk, make a template out of it, or migrate it (if the migration involves copying the disk), the contents of the LUN are copied into a virtual disk (`.vmdk`) file.

Virtual Machine Options

Slide 7-75



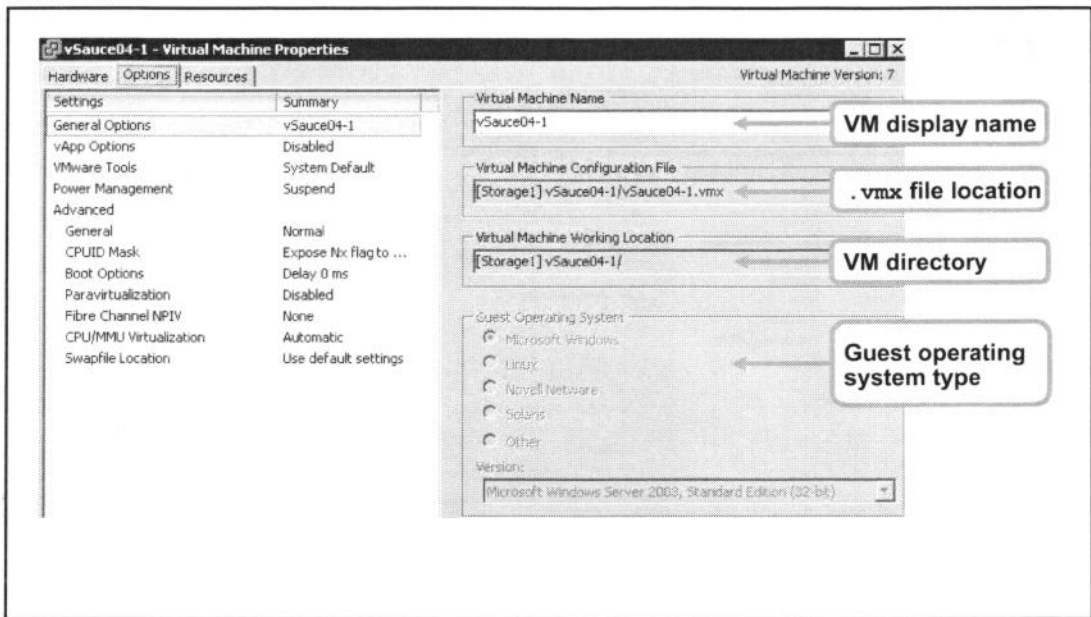
The **Options** tab in the Virtual Machine Properties Editor allows you to change a virtual machine's options. It has several powerful features, which are distributed into four categories:

- **General Options**
- **vApp Options**
- **VMware Tools**
- **Power Management**
- **Advanced**

The next several pages cover some of the important things you can do to modify a virtual machine from the **Options** tab.

Options: General Options

Slide 7-76



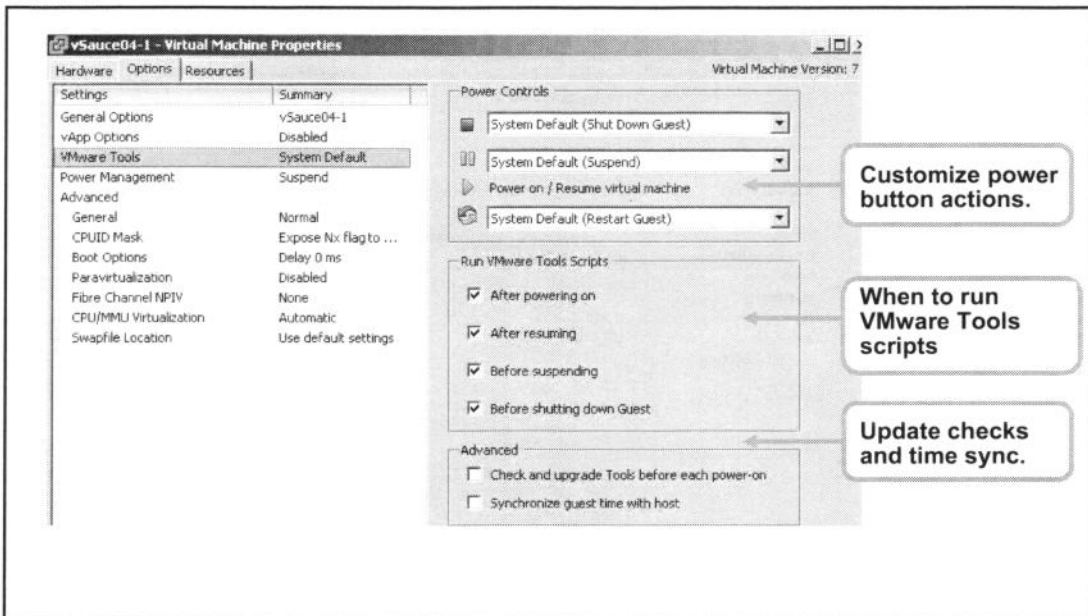
General Options pane can be used to modify things like the display name used for the virtual machine and the type of guest operating system installed. The location and name of the configuration file (.vmx file) is displayed, and the location of the virtual machine's directory is also shown. You can select the text for the configuration file and working location if you need to copy and paste them into a document. But only the display name and the guest operating system type can be modified.

NOTE

If you change the display name, that will not change the names of all of the virtual machine files or the directory the virtual machine is stored in. When a virtual machine is first created, the filenames and the directory name associated with the virtual machine are based on its display name. But changing the display name later does not modify these file and directory names.

Options: VMware Tools

Slide 7-77



The **VMware Tools** pane controls how the VMware Tools in the virtual machine respond to certain external events. You can use these to customize the power buttons on the virtual machine. For example, the red square **Power Off** button for a virtual machine can be set to always perform a guest shutdown. This is far safer for the virtual machine. It is like the difference between using the **Start > Shut Down** command in Windows instead of unplugging the PC.

The VMware Tools program can be set to run certain scripts when specific events (like a power-off) occur. But that has to be set from within the guest operating system by opening the VMware Tools window. Once the scripts are selected and enabled, this window controls when the virtual machine checks to see if scripts should be run. This gives you the advantage of enabling or disabling script operations from outside the virtual machine while it is powered off.

The **Advanced** panel has two important functions. One check box is used to check and possibly update VMware Tools automatically if a newer version becomes available. The other is to enable time synchronization with the host. As a best practice, time synchronization with the host should always be enabled. However, if the virtual machine is forcing its clock to sync to the ESX/ESXi host, you must ensure two other things have been configured:

- The host should have its time synched to some external source, preferably via NTP.
- The guest operating system should *not* be trying to synchronize time on its own. Most Windows systems automatically synchronize to a Windows Active Directory domain controller. Many UNIX and Linux systems are configured to synchronize to external NTP servers. Best practice

is to let VMware Tools synchronize time to the host—and disable these other time synchronization systems within the guest operating system. If you configure the virtual machine to synchronize time to the host and also allow the guest operating system to try to synchronize time to something else, time on the virtual machine will become unstable and erratic.

Options: Power Management

Slide 7-78

vSauce04-1 - Virtual Machine Properties

Hardware | Options | Resources | **Virtual Machine**

Settings	Summary
General Options	vSauce04-1
vApp Options	Disabled
VMware Tools	System Default
Power Management	Suspend

Advanced

General	Normal
CPUID Mask	Expose Nx flag to ...
Boot Options	Delay 0 ms
Paravirtualization	Disabled
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Guest Power Management

How should the virtual machine respond when the guest OS is placed on standby?

- ☒ Suspend the virtual machine
- ☐ Put the guest OS into standby mode and leave the virtual machine powered on

Wake on LAN for virtual machine traffic on:

☒ Network adapter 1 (dyPortGroup)

Suspend or standby the guest operating system gracefully.
Wake on LAN.

The **Power Management** pane allows you to choose how the virtual machine should respond when it is placed in the standby power state. The virtual machine can either be suspended or the guest operating system can be placed in standby mode, leaving the virtual machine powered on.

If you opt for placing the guest operating system in standby mode, you can enable **Wake on LAN**. This is not available on all guest operating systems.

Advanced: Boot Options

Slide 7-79

vSauce04-1 - Virtual Machine Properties

Hardware | Options | Resources

Settings	Summary
General Options	vSauce04-1
vApp Options	Disabled
VMware Tools	System Default
Power Management	Suspend
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Boot Options	Delay 0 ms
Paravirtualization	Disabled
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Power-on Boot Delay

Whenever the virtual machine is powered on, delay the boot for the following number of milliseconds:

0 ms

Force BIOS Setup

☒ The next time the virtual machine boots, force entry into the BIOS setup screen.

Delay power on.

Boot into BIOS.

Advanced options usually do not need to be set.

Advanced options address things that usually do not need to be set for a virtual machine. We cover a few of these options in this lesson.

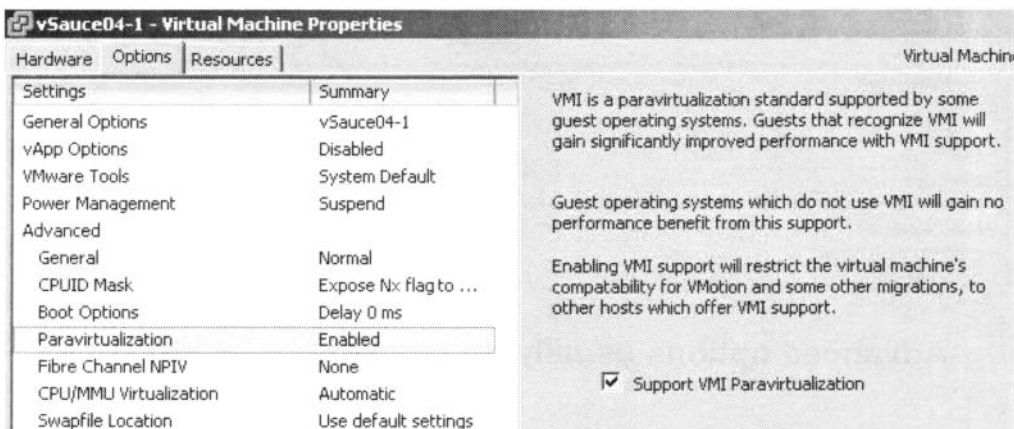
The **Boot Options** pane allows you to do two things. You can use the **Power-on Boot Delay** panel to delay a virtual machine power-on. This can be useful to help stagger virtual machine startups when several virtual machines are being powered on.

You can use the **Force BIOS Setup** panel to make changes to the BIOS settings like forcing a virtual machine to boot from a CD-ROM. The next time the virtual machine powers on, it goes straight into BIOS. This is much easier than powering the virtual machine on, opening a console, and quickly trying to press the F2 key to go into BIOS.

Advanced: Paravirtualization

Slide 7-80

Paravirtualization, supported by some guest operating systems, makes a guest operating system aware that it is running inside a virtual machine rather than on physical hardware.



Paravirtualization is a virtualization enhancement where a guest operating system is aware that it is running inside a virtual machine rather than on physical hardware.

Virtual Machine Interface (VMI) is a paravirtualization standard that enables improved performance for virtual machines capable of utilizing it. This feature is available only for those versions of the Linux guest operating system that support VMI paravirtualization.

Enabling paravirtualization utilizes one of the virtual machine's six virtual PCI slots. Also, enabling paravirtualization can limit how and where the virtual machine can be migrated. Consider the following before enabling this feature:

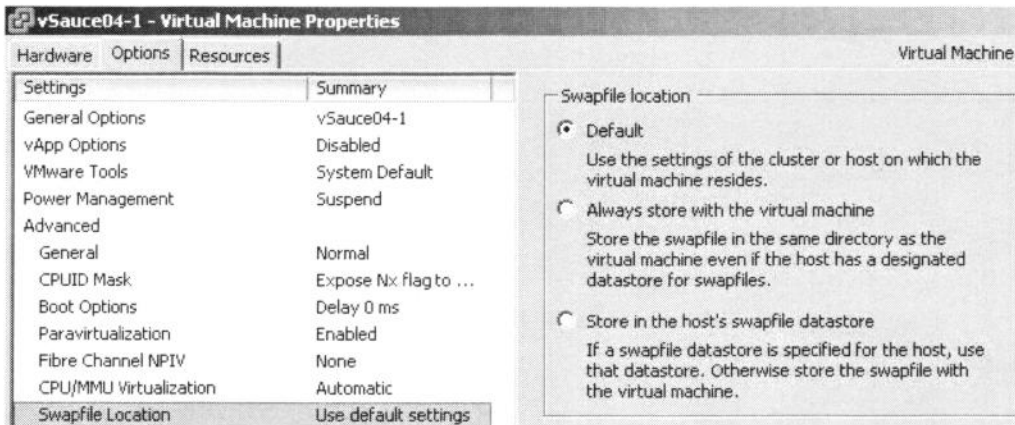
- These hosts support VMI paravirtualization: ESX/ESXi 3.5 and greater, and Workstation 6.0 and greater. Hardware version 4 virtual machines with paravirtualization enabled that are created on ESX hosts can be migrated to VMware Server and Workstation hosts without loss of functionality.
- A virtual machine with paravirtualization enabled and that is powered off can be moved manually to a host that does not support paravirtualization. However, this can result in reduced performance.
- A virtual machine with paravirtualization enabled and that is powered on or in a suspended power state cannot be migrated to a host that does not support paravirtualization.

- Not allowed are automated VMware Distributed Resource Scheduler migrations of virtual machines with paravirtualization enabled to hosts that do not support paravirtualization.

Swap File Location

Slide 7-81

Each host or cluster can have a custom swap file datastore location defined.



Each virtual machine has its own swap file. The swap files are normally stored in the same location as other virtual machine files. However, if the virtual machine's files are stored on a network storage location that has poor performance (such as a slow NFS server), you might see a performance boost by storing the virtual machine's swap file on faster storage. To facilitate this, "swap file datastores" can be defined for each ESX/ESXi host or cluster or both.

There are three choices for the swap file location:

- **Default** – Store the virtual machine swap file at the default location defined by the host or cluster swap file settings.
- **Always store with the virtual machine** – Store the virtual machine swap file in the same folder as the virtual machine configuration file.
- **Store in the host's swapfile datastore** — Store the virtual machine swap file in the swap file datastore defined by the host or cluster swap file settings.

Lab 12

Slide 7-82

In this lab, you will modify a virtual machine's hardware and add a raw LUN to a virtual machine.

1. Modify a virtual machine's disk, memory, and name.
2. Add a raw LUN to an existing virtual machine and verify that the guest operating system sees the new disk.

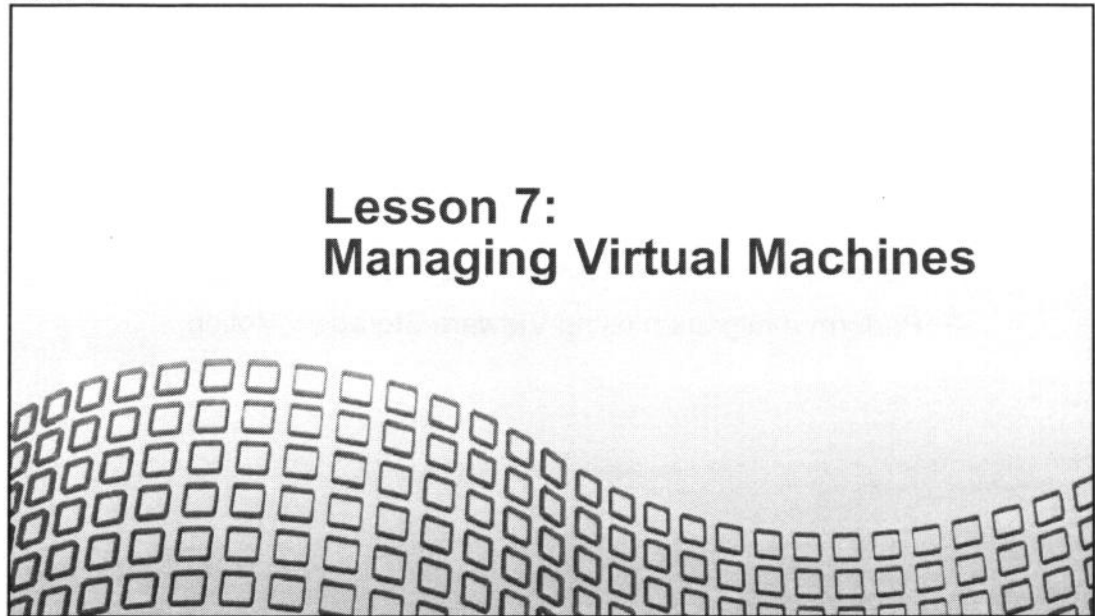
Lesson Summary

Slide 7-83

- > USB controllers, Ethernet adapters, and hard disks can be added to a virtual machine while it is powered on.
- > The size of virtual machine's disk, such as the C: drive, can be increased while the virtual machine is powered on.
- > When a raw LUN is added to a virtual machine, an RDM pointing to the raw LUN is create in the specified VMFS datastore.

Lesson 7: Managing Virtual Machines

Slide 7-84



Lesson Objectives

Slide 7-85

- > Snapshot a virtual machine and manage multiple snapshots
- > Remove a virtual machine from the vCenter Server inventory and completely from disk
- > Describe the different types of migration
- > Perform a migration using VMware Storage VMotion

Virtual Machine Snapshots

Slide 7-86

Snapshots allow you to preserve the state of the virtual machine so that you can return to the same state repeatedly.

For example, if you are testing software, snapshots allow you to back out of these changes.



vCenter Server snapshots allow you to preserve the state of the virtual machine so you can return to the same state repeatedly.

Snapshots are useful when you need to revert repeatedly to the same state but don't want to create multiple virtual machines. With snapshots, you create backup-and-restore positions in a linear process. You can also preserve a baseline before diverging a virtual machine in a process tree.

The relationship between snapshots is like that between a parent and a child. In a linear process, each snapshot has one parent and one child, except for the last snapshot, which has no children. In the example above, the snapshots (Base Image, Security Patch 1.0, Security Patch 1.0.1, and Security Patch 1.0.2) are organized in a linear process.

Another way to organize snapshots is in a process tree, where each snapshot has one parent, but one snapshot can have more than one child. Many snapshots have no children. You can revert to either a parent or a child snapshot.

(can grow to size of original VMDK)

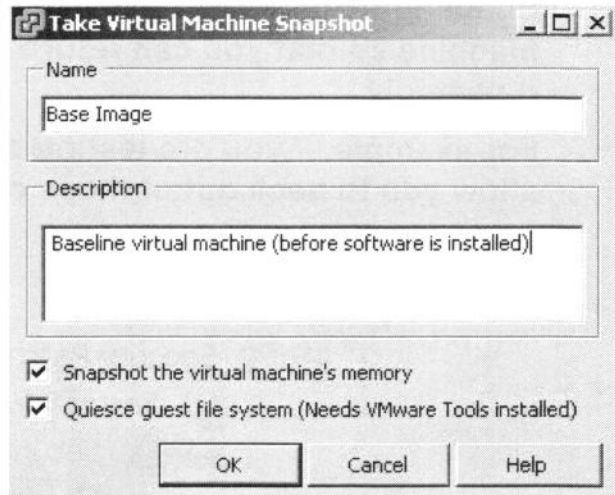
Taking a Snapshot

Slide 7-87

You can take a snapshot while a virtual machine is powered on, powered off, or suspended.

A snapshot captures the entire state of the virtual machine:

- Memory state, settings state, and disk state



A snapshot captures the entire state of the virtual machine at the time you take the snapshot. This includes:

- Memory state – The contents of the virtual machine's memory (captured only if the virtual machine is powered on)
- Settings state – The virtual machine settings
- Disk state – The state of all the virtual machine's virtual disks

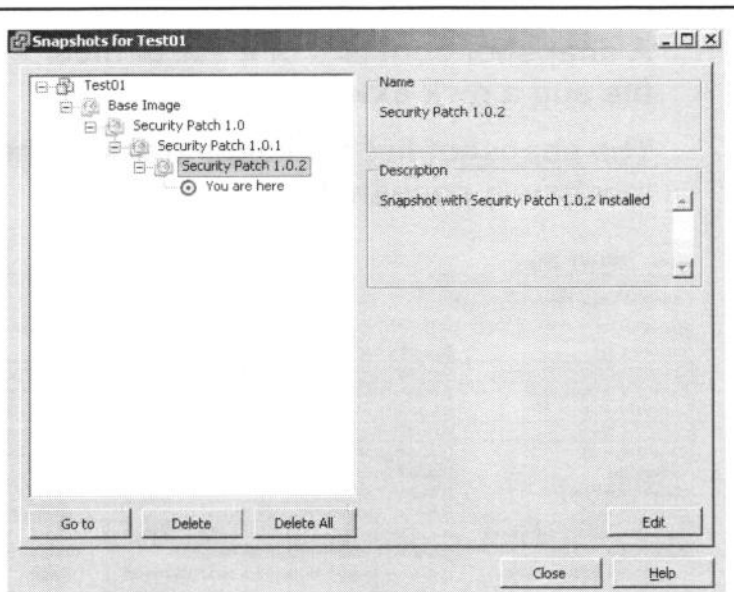
Snapshots of RDM physical compatibility mode disks are not supported.

Managing Snapshots

Slide 7-88

The Snapshot Manager lets you review all snapshots for the active virtual machine and act on them directly.

- Revert to a snapshot.
- Delete one or all snapshots.



The Snapshot Manager window allows you to perform three tasks:

- **Delete** – This task commits the snapshot data to the parent snapshot, then removes the selected snapshot.
- **Delete All** – This task commits all the intermediate snapshots before the current-state icon (“You are here”) to the base disk and removes all existing snapshots for that virtual machine.
- **Go to** – This task allows you to restore, or revert to, a particular snapshot. The snapshot that you restore becomes the current snapshot.

When you revert to a snapshot, you return all these items to the state that they were in at the time you took the snapshot. If you want the virtual machine to be suspended, powered on, or powered off when you launch it, be sure it is in the correct state when you take the snapshot.

To display the Snapshot Manager, right-click virtual machine in the inventory, then choose **Snapshot > Snapshot Manager**.

Virtual Machine Snapshot Files

Slide 7-89

A snapshot consists of a set of files: the snapshot data file and a disk extent file.

The snapshot list file keeps track of the virtual machine's snapshots.

View: Reports Maps

Show all Virtual Machine Files

Name	Path	File type	Datastore	Size
vmware-1.log	[Local06] Carla07-4/vmware-1.log	Log	Local06	148.46 KB
Carla07-4-Snapshot1.vmsn	[Local06] Carla07-4/Carla07-4-Snapshot1.vmsn	Snapshot Data	Local06	381.19 MB
Carla07-4-000001.vmdk	[Local06] Carla07-4/Carla07-4-000001.vmdk	Disk Descriptor	Local06	243.00 B
Carla07-4.vmdk	[Local06] Carla07-4/Carla07-4.vmdk	Disk Descriptor	Local06	443.00 B
Carla07-4.vmsd	[Local06] Carla07-4/Carla07-4.vmsd	Snapshot List	Local06	480.00 B
Carla07-4.vmx	[Local06] Carla07-4/Carla07-4.vmx	Extended Configuration	Local06	264.00 B
vmware.log	[Local06] Carla07-4/vmware.log	Log	Local06	113.99 KB
Carla07-4.nvram	[Local06] Carla07-4/Carla07-4.nvram	NVRAM	Local06	8.48 KB
Carla07-4.vmx	[Local06] Carla07-4/Carla07-4.vmx	Configuration	Local06	2.99 KB
Carla07-4-000001-delta.vmdk	[Local06] Carla07-4/Carla07-4-000001-delta.vmdk	Disk Extent	Local06	16.01 MB
Carla07-4-flat.vmdk	[Local06] Carla07-4/Carla07-4-flat.vmdk	Disk Extent	Local06	1019.00 MB
Carla07-4-a6a81051.vswp	[Local06] Carla07-4/Carla07-4-a6a81051.vswp	Swap	Local06	364.00 MB

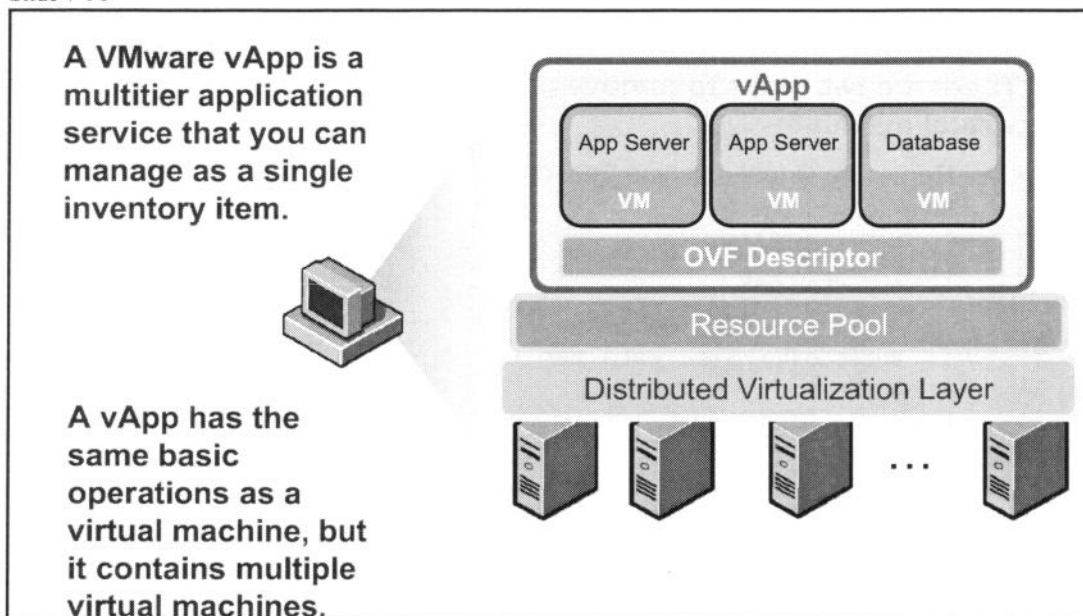
A virtual machine can have one or more snapshots. Each snapshot consists of the following files:

- Snapshot differences file – <VM_name>-00000#-delta.vmdk, where # is the next number in the sequence, starting with 1.
- Snapshot description file – <VM_name>-00000#.vmdk
- Memory state file – <VM_name>-Snapshot#.vmsn. The size of this file is the size of the virtual machine's maximum memory (only if memory is captured—otherwise, the file is much smaller).

<VM_name>.vmsd is a file created at the time the virtual machine is created. It maintains information about all the snapshots (such as name of the snapshot .vmsn file and the name of the virtual disk file) that belong to this virtual machine.

Managing Virtual Machines Using vApp

Slide 7-90



vSphere extends application management to support running and managing multitier application services as a single inventory item. The format in which the applications are packaged and managed is called VMware vApp.

A vApp package includes one or more virtual machines running the applications included in the multi-application service. Each application is already set up and configured to run on the virtual hardware of the virtual machine. Predeploying applications in virtual machines eliminates the complex setup that usually accompanies deploying multitier services. It also gives you the flexibility to change physical resources without affecting the service.

In the vSphere Client, a vApp is represented in both the Hosts and Clusters view and the VMs and Templates view. Each view has a specific **Summary** page with the current status of the service and relevant summary information, as well as operations on the service.

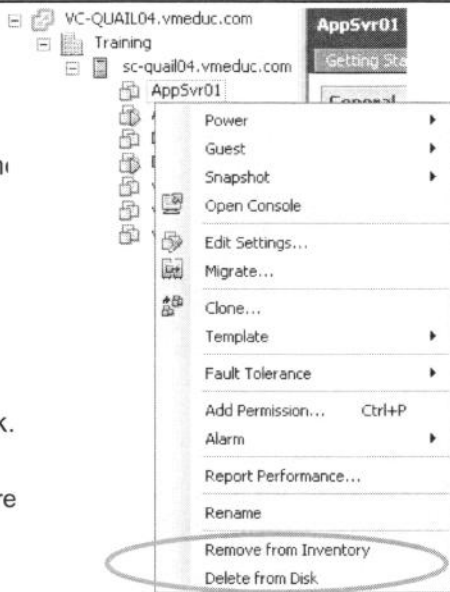
vApps are packaged as OVF files.

Removing a Virtual Machine

Slide 7-91

There are two ways to remove a virtual machine:

- > Remove a virtual machine from the inventory.
 - The virtual machine's files still remain on disk.
 - The virtual machine can be re-added to the inventory at a later time.
- > Delete a virtual machine from disk.
 - The virtual machine is removed from the inventory, and its files are permanently deleted from disk.



There are two ways to remove a virtual machine: from the inventory and from disk.

Removing a virtual machine from the inventory unregisters it from the host and vCenter Server. It does not delete it from the datastore. Virtual machine files remain at the same storage location, and the virtual machine can be re-registered using the datastore browser.

To remove a virtual machine from the inventory, right-click the virtual machine, then choose **Remove from Inventory**.

To re-register the virtual machine in the inventory, go to the Datastores inventory view. Right-click the datastore where the virtual machines are located, then choose **Browse Datastore**. In the left pane of the datastore browser, double-click the folder of the virtual machine you want to re-register. Right-click the virtual machine's configuration file (.vmx file), then choose **Add to Inventory**.

When you remove a virtual machine from a datastore, it is removed from vCenter Server, and all virtual machine files, including the configuration file and virtual disk files, are deleted from the datastore.

To remove a virtual machine from a datastore, right-click the virtual machine, then choose **Delete from Disk**.

Migrating Virtual Machines

Slide 7-92

Migration is the process of moving a virtual machine from one host or storage location to another. Types of migrations:

- Cold – Migrate a virtual machine that is powered off.
- Suspend – Migrate a virtual machine that is suspended.
- VMware VMotion™ – Migrate a virtual machine that is powered on.
- Storage VMotion – Migrate just a virtual machine's files, while the virtual machine is powered on, to a different datastore.

A main use of migration is to improve overall hardware utilization.

VMotion has additional uses:

- It allows continued virtual machine operation while accommodating scheduled hardware downtime.
- It allows VMware Distributed Resource Scheduler to balance virtual machines across hosts.

Migration is the process of moving a virtual machine from one host or storage location to another. Copying a virtual machine creates a new virtual machine. It is not a form of migration. In vCenter Server, you have the following migration options:

- Cold migration – Moving a powered-off virtual machine to a new host. Optionally, you can relocate configuration and disk files to new storage locations. Cold migration can be used to migrate virtual machines from one datacenter to another.
- Migrating a suspended virtual machine – Moving a suspended virtual machine to a new host. Optionally, you can relocate configuration and disk files to new storage location. You can migrate suspended virtual machines from one datacenter to another.
- Migration with VMotion – Moving a powered-on virtual machine to a new host. Migration with VMotion allows you to move a virtual machine to a new host without any interruption in the availability of the virtual machine. Migration with VMotion cannot be used to move virtual machines from one datacenter to another.
- Migration with Storage VMotion – Moving the virtual disks or configuration file of a powered-on virtual machine to a new datastore. Migration with Storage VMotion allows you to move a virtual machine's storage without any interruption in the availability of the virtual machine.

Comparison of Migration Types

Slide 7-93

Migration type	Power state	Change host/ datastore ?	Across datacenters ?	Shared storage required?	CPU compatibility?
Cold	Off	Host or datastore or both	Yes	No	Different CPU families allowed
Suspended VM	Suspended	Host or datastore or both	Yes	No	Must meet CPU compatibility requirements
VMotion	On	Host	No	Yes	Must meet CPU compatibility requirements
Storage VMotion	On	Datastore	No	No	N/A

The table above compares the different migration techniques. A driving factor behind the decision to use a particular migration technique is the actual purpose for performing a migration.

For example, if you need to bring a host down for maintenance yet keep the virtual machine up and running, you would choose to migrate the virtual machine using VMotion instead of performing a cold or suspended virtual machine migration. If you need to move a virtual machine's files to a different datastore to better balance the load, use Storage VMotion for this task.

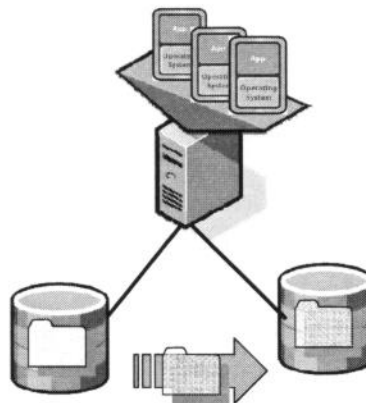
Some migration techniques, such as VMotion, have special hardware requirements that must be met in order to function properly. Other techniques, such as a cold migration or a suspended virtual machine migration, do not have special hardware requirements in order to function properly.

Benefits of Storage VMotion

Slide 7-94

Migration with Storage VMotion:

- > Performing storage maintenance and reconfiguration
- > Redistributing storage load
- > Evacuating physical storage about to be retired
- > Storage tiering
- > Upgrading ESX/ESXi hosts without virtual machine downtime



There are several uses of Storage VMotion:

- Moving virtual machines off a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime
- Manually redistributing virtual machines or virtual disks to different storage volumes to balance capacity and improve performance
- Evacuating physical storage that is about to be retired, such as storage arrays coming off the maintenance and release cycles
- Storage tiering: migrating virtual machines from Fibre Channel to iSCSI or NAS or within or between enclosures; or moving virtual machines to tiered storage with different service levels due to changing business requirements for that virtual machine
- Upgrading VMware Infrastructure without virtual machine downtime. During an upgrade of an ESX/ESXi host from one version to the next, the vSphere administrator can migrate running virtual machines from a VMFS2 datastore to a VMFS3 datastore and upgrade the VMFS2 datastore without any impact on virtual machines. The vSphere administrator can then use Storage VMotion to migrate virtual machines back to the original datastore without any virtual machine downtime.

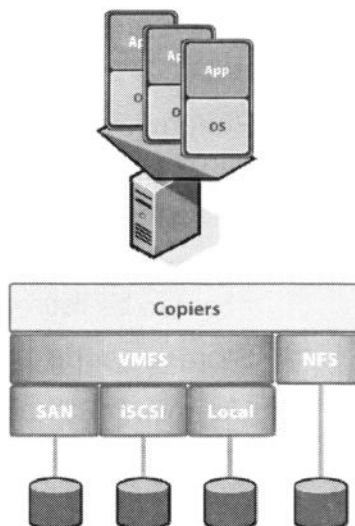
Storage Type Interdependency

Slide 7-95

Storage VMotion is storage type-independent.

- > Virtual machine disks are moved with snapshot technology.
- > Virtual machine home files are copied using a network file copier.
- > Copiers are not storage type-specific, located “above” the file system layer.

Source and destination can be different storage types.



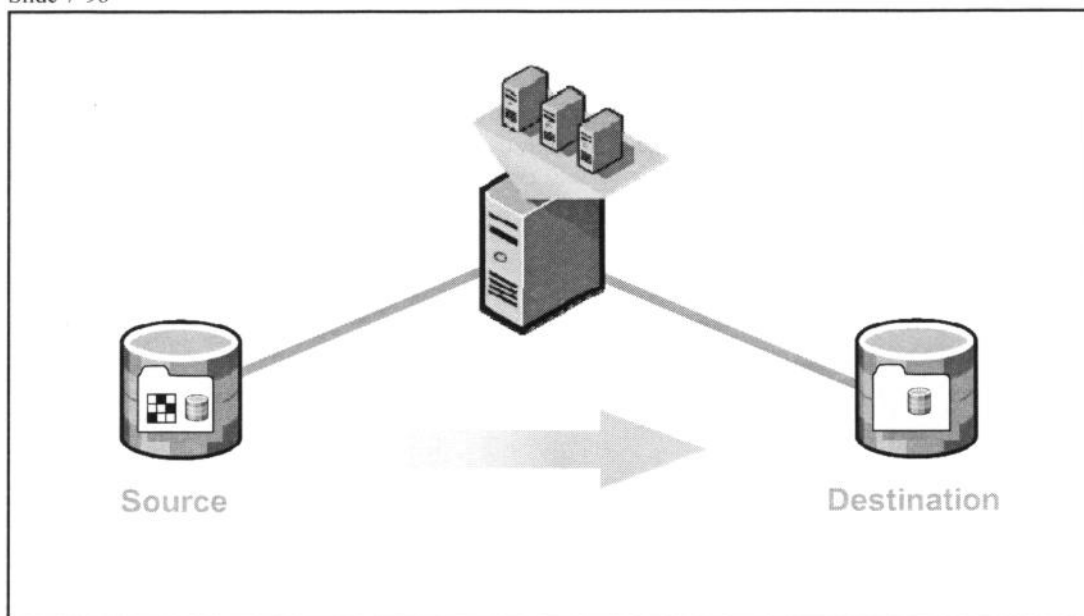
Storage VMotion is storage-type independent. Storage VMotion works across NFS datastores as well as across VMFS datastores on Fibre Channel, iSCSI, and local SCSI storage. In addition, Storage VMotion supports migrating RDMs to RDMs, provides the option to convert virtual disks from thick to thin formats, and can convert RDMs to VMDKs (as long as virtual machines have not been configured to use VMDirectPath I/O).

During Storage VMotion operations, non-virtual disk files are copied to the new virtual machine home using network file copier (NFC). A standard VMotion operation is then employed to start up a new virtual machine on the same host, instead of on a different host. This new virtual machine uses the configuration file in the new virtual machine home directory. A VMotion migration that occurs on the same host is known as a “self-VMotion” migration.

A self-VMotion migration uses the same process as a normal VMotion migration. This is done to get the virtual machine using a swap file in the new home location and to reopen other files (especially the `.nvram` configuration file, and so forth) that have been moved to the new home location. Self-VMotion is the quickest and easiest way to get the virtual machine to transition over to using the new files, especially the new swap file.

Storage VMotion In Action

Slide 7-96



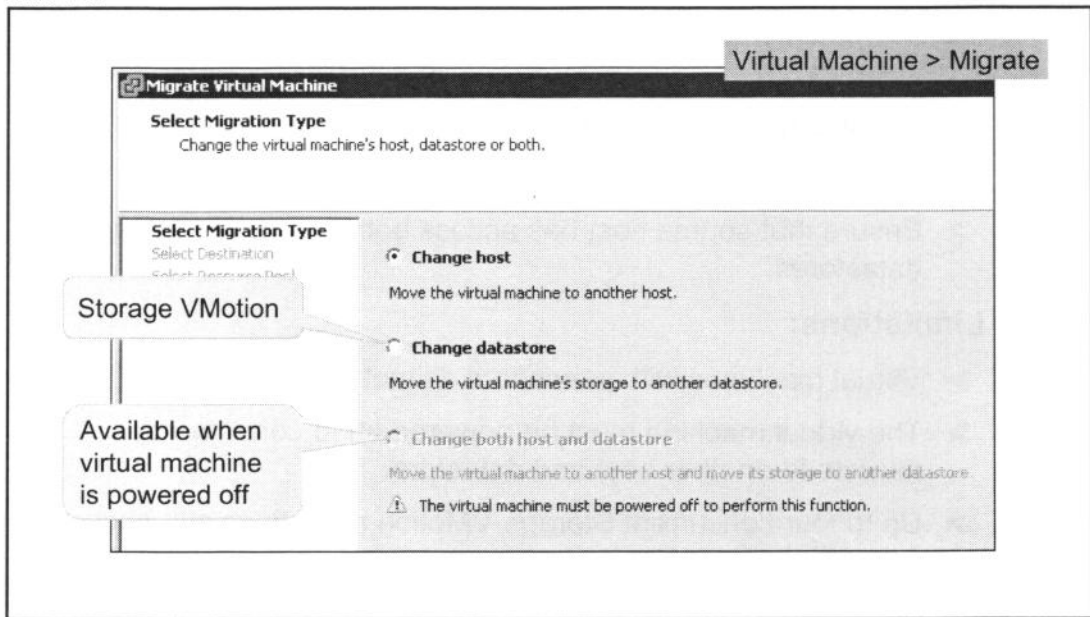
This diagram shows what happens when you migrate a virtual machine using Storage VMotion.

1. Upon initiating a migration, vSphere copies all virtual machine files except the disks from the old virtual machine directory to a new directory on the destination datastore.
2. vSphere enables changed block tracking on the virtual machine's disk. Changed block tracking tracks changes to the disk so that vSphere knows which regions of the disk include data. vSphere does this by creating a bitmap for each block of data in the VMDK files. If any blocks are modified, the corresponding bit in the bitmap is updated to reflect the modification. In this way, vSphere can determine which blocks of data are static and which blocks have updated data.
3. vSphere "precopies" the virtual machine's disk and swap file from the disk on the source to the disk on the destination. During this time, the virtual machine is running and may be writing to its disk. Therefore, some regions of the disk change and must be resent. This is where changed block tracking comes in. vSphere first copies the contents of the entire disk to the destination. This is the first precopy iteration. It then queries the changed block tracking module to determine which regions of the disk were written to during the first iteration. vSphere performs a second iteration of precopy, only copying those regions that were changed during the first iteration. Typically, the number of changed regions is significantly smaller than the total size of the disk, so the second iteration takes much less time. vSphere continues precopying until the amount of modified data is small enough to be copied very quickly.

4. ESX/ESXi invokes fast suspend/resume on the virtual machine. Fast suspend/resume does exactly what its name implies: the virtual machine is quickly suspended and resumed. The new virtual machine process uses the destination virtual machine home and disks. Before ESX/ESXi allows the new virtual machine to start running again, the final changed regions of the source disk are moved to the destination so that the destination disk image is identical to the source.
5. Once the virtual machine is running on the destination datastore, ESX/ESXi removes the component files of the virtual machine from the source host.

Migrating Using Storage VMotion

Slide 7-97



To migrate a virtual machine using Storage VMotion, right-click a virtual machine that is powered on, then choose **Migrate**. The Migrate Virtual Machine wizard appears. Select **Change datastore**. You select the destination datastore as well as the disk format of the virtual disk. By default, the disk format used will be the same format as the source's.

Storage VMotion Guidelines and Limitations

Slide 7-98

Guidelines:

- > Spend time planning and coordinating with administrators.
- > Perform during off-peak hours.
- > Ensure that source host has access both to source and target datastores.

Limitations:

- > Virtual machines with snapshots cannot be migrated.
- > The virtual machine must be powered off to concurrently migrate to another host and datastore.
- > Up to four concurrent Storage VMotion migrations can occur.

A virtual machine and its host must meet certain resource and configuration requirements for the virtual machine disks to be migrated with Storage VMotion.

One of the requirements of Storage VMotion is that the host on which the virtual machine is running must have access both to the source and the target datastores.

Storage VMotion is subject to the following limitations:

- Virtual machines with snapshots cannot be migrated using Storage VMotion.
- You cannot migrate virtual machines to a different host and a different datastore simultaneously, unless you power off the virtual machine.
- vSphere supports a maximum of four simultaneous VMotion or Storage VMotion accesses to a single datastore. A migration with VMotion involves two simultaneous accesses to the datastore: by the source and destination hosts. A migration with Storage VMotion involves one access to the source datastore and one access to the destination datastore. Therefore, if no other migrations are occurring, up to four concurrent Storage VMotion migrations involving the datastore can occur simultaneously.

Lab 13

Slide 7-99

In this lab, you will perform several virtual machine management tasks.

1. Remove a virtual machine from the vCenter Server inventory.
2. Re-add the virtual machine and verify that it appears in the inventory.
3. Delete a virtual machine from disk and verify that it can no longer be accessed.
4. Take snapshots of a virtual machine.
5. Revert to a snapshot.
6. Migrate a virtual machine using Storage VMotion.

Lesson Summary

Slide 7-100

- > The Snapshot Manager allows you to revert back to a snapshot and delete one or more of a virtual machine's snapshots.
- > A virtual machine that is removed from the vCenter Server inventory can be returned to the inventory because its files are not deleted from disk.
- > Storage VMotion allows you to migrate a virtual machine from one datastore to another while the virtual machine is powered on.

Key Points

Slide 7-101

- > There are various methods to create a virtual machine. Choose the method that best fits your needs.
- > Deploying virtual machines from a template allows you to easily create many virtual machines.
- > vCenter Server provides useful features for provisioning virtual machines, such as vCenter Converter and Guided Consolidation.

NOTES