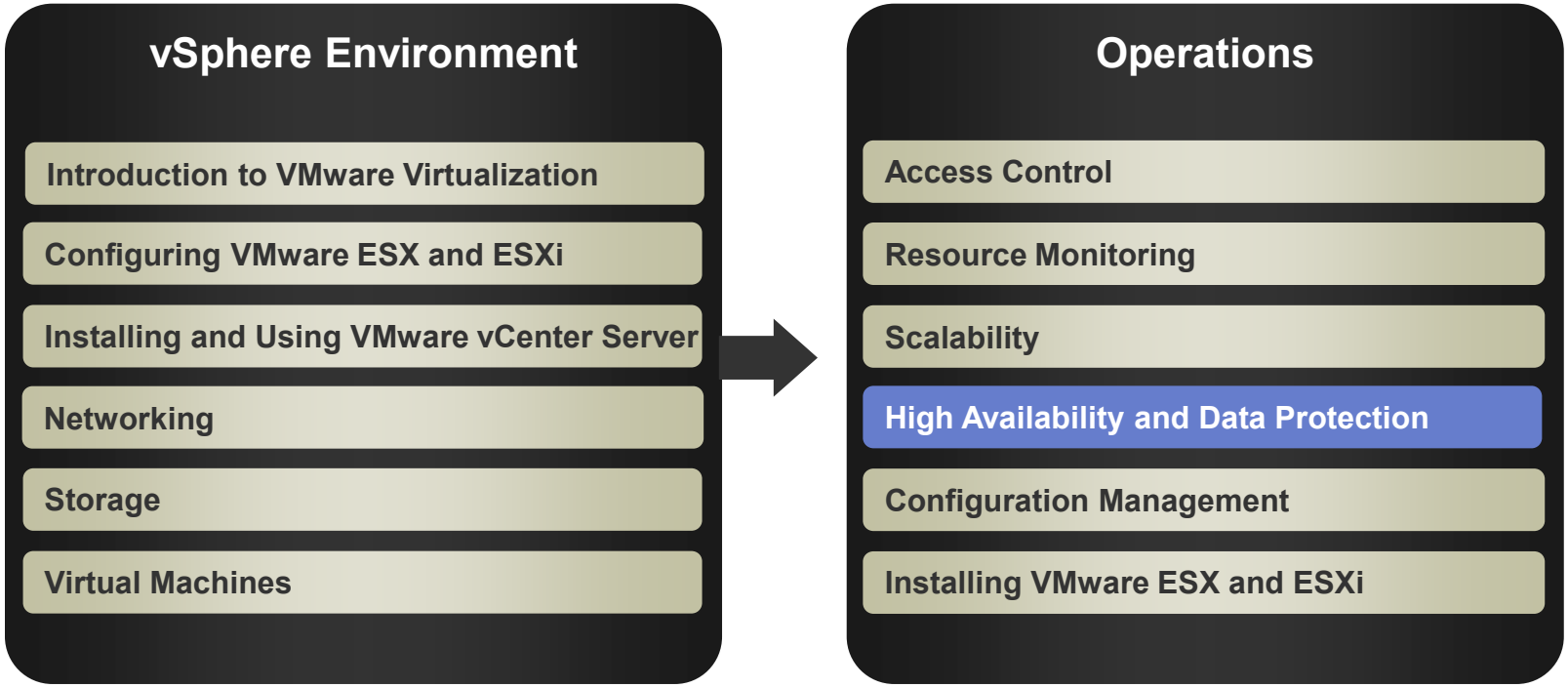
High Availability and Data Protection

Module 11

You Are Here



Importance

- Most organizations today rely on computer-based services like e-mail, databases, and Web-based applications. The failure of any of these services can mean lost productivity and revenue. Configuring highly available computer-based services is extremely important for an organization to remain competitive in today's business environment.

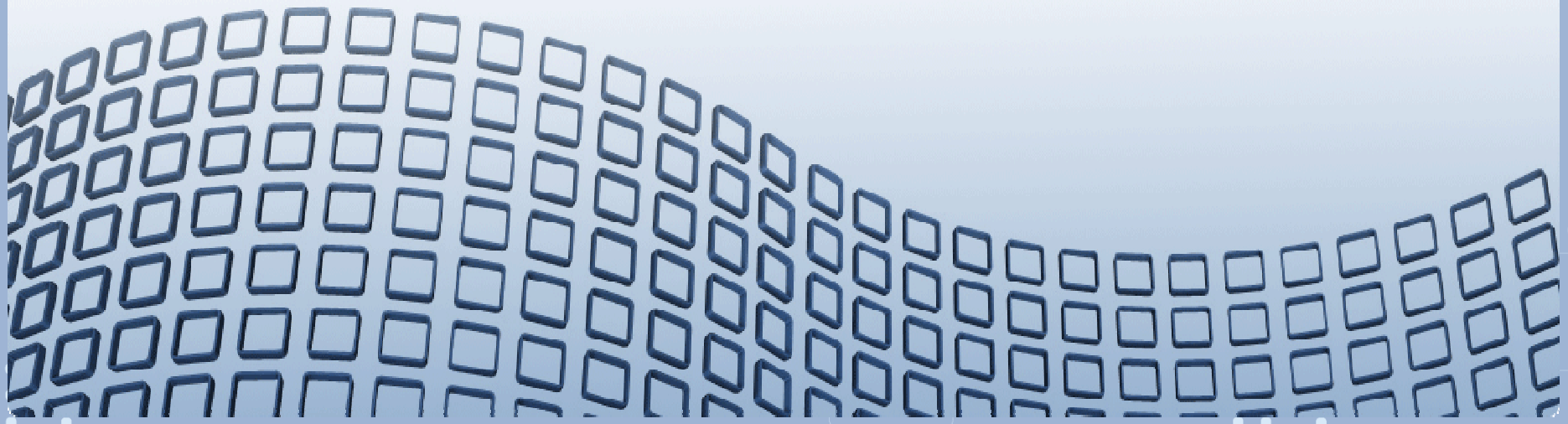
Module Lessons

Lesson 1: High Availability and Data Protection Overview

Lesson 2: VMware High Availability

Lesson 3: Data Protection

Lesson 1: High Availability and Data Protection Overview



Lesson Objectives

- Describe VMware® solutions for:
  - High availability
  - Fault tolerance
  - Data protection

High Availability and Fault Tolerance

A highly available system is one that is continuously operational for a desirably long length of time.

A fault-tolerant system is designed so that, in the event of an unplanned outage, a backup component can immediately take over with no loss of service.

What level of availability is important to you?

- It varies. The system must match the highest level of requirement (the most 9s) for any virtual machine.

99% available – 87 hours or 3.5 days of downtime per year
99.9% available – 8.76 hours of downtime per year
99.99% available – 52 minutes of downtime per year
99.999% available – 5 minutes of downtime per year

VMware Availability and Fault Tolerance Solutions

Availability features in VMware ESX™/ESXi:

- Storage availability using multipathing
- Network availability using NIC teaming
- VMware VMotion™ and Storage VMotion

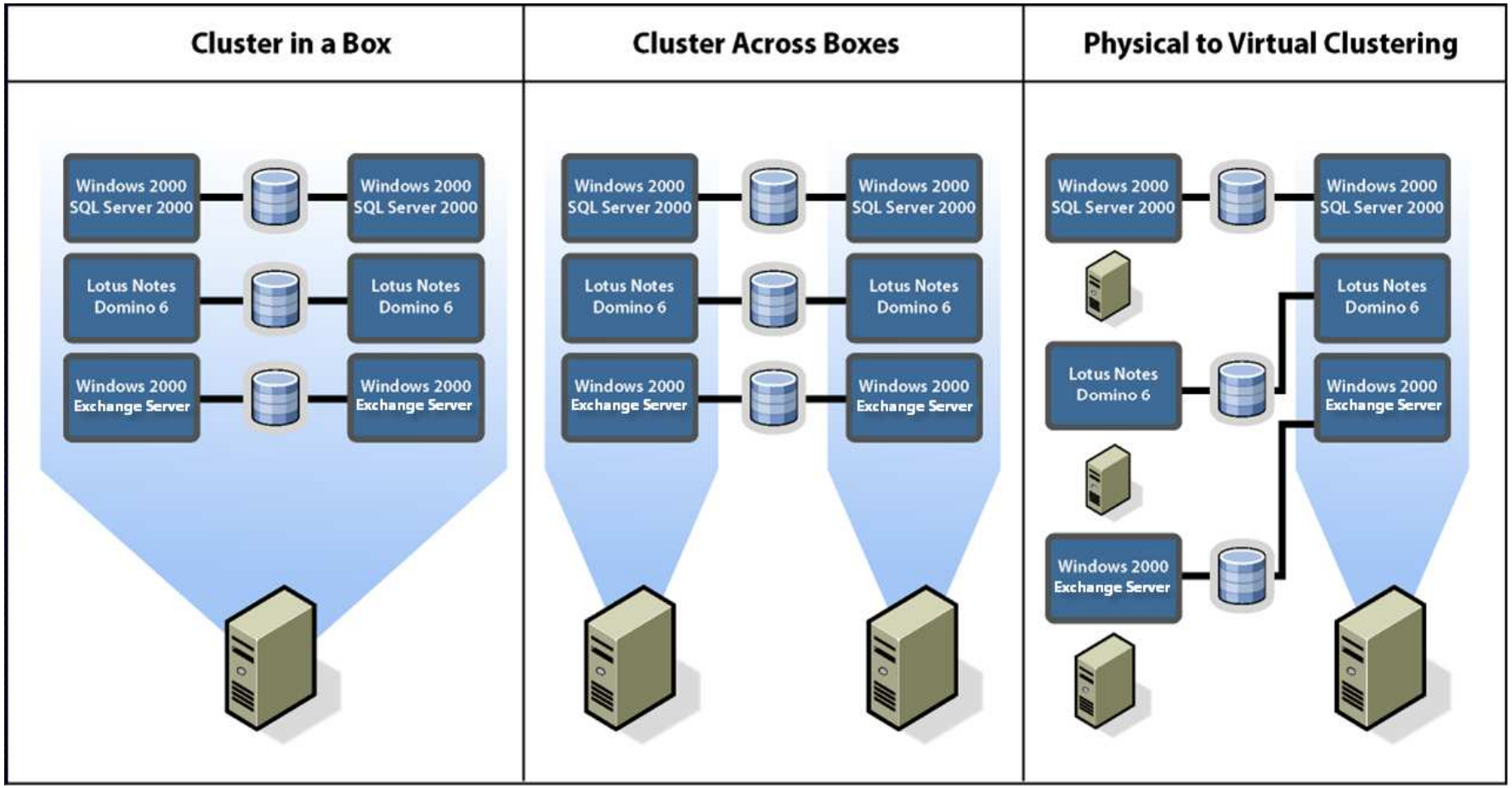
VMware availability product:

- VMware Site Recovery Manager – Decreases planned and unplanned downtime. SRM protects all of your important systems and applications with disaster recovery.

VMware HA, FT, and MSCS Clustering

	VMware HA	*FT*	*MSCS Clustering*
Level of availability	**High availability**	**Fault tolerance**	**Fault tolerance**
Amount of downtime	**Minimal**	**Zero**	**Zero**
Guest operating systems supported	**Works with all supported guest operating systems**	**Works with all supported guest operating systems**	**Works with Windows operating systems**
ESX hardware supported	**Works with all supported ESX hardware**	**Limited to the newest ESX hardware**	**Limited to hardware supported by Microsoft**
Uses	**Use to provide high availability for all your virtual machines.**	**Use to provide fault tolerance to your critical virtual machines.**	**Use if you already have in-house expertise with MSCS.**

MSCS Clustering



vCenter Server Availability

Make VMware vCenter™ Server, as well as the components it relies on, highly available.

vCenter Server relies on:

- vCenter Server database
  - Cluster the database; refer to the specific database documentation.
- Active Directory structure
  - Set up using multiple redundant servers.

Methods for making vCenter Server available:

- Cluster vCenter Server using MSCS.
- Create a standby host (physical machine or virtual machine).
- Use VMware vCenter Server Heartbeat.

Data-Protection Solutions

VMware data-protection products:

- VMware Consolidated Backup
  - A centralized backup facility for virtual machines that works in conjunction with many third-party backup tools
- VMware Data Recovery
  - An agentless, disk-based backup-and-recovery solution for virtual machines, based on a virtual appliance
  - Based on the VMware vStorage APIs for Data Protection

Lesson Summary

- VMware HA, SRM, and vCenter Server Heartbeat provide VMware vSphere™ availability solutions.
- VMware Fault Tolerance and support for MSCS clustering provide vSphere fault-tolerant solutions.
- VMware Data Recovery and VMware Consolidated Backup provide data-protection solutions.

Lesson 2:
VMware High Availability

Lesson Objectives

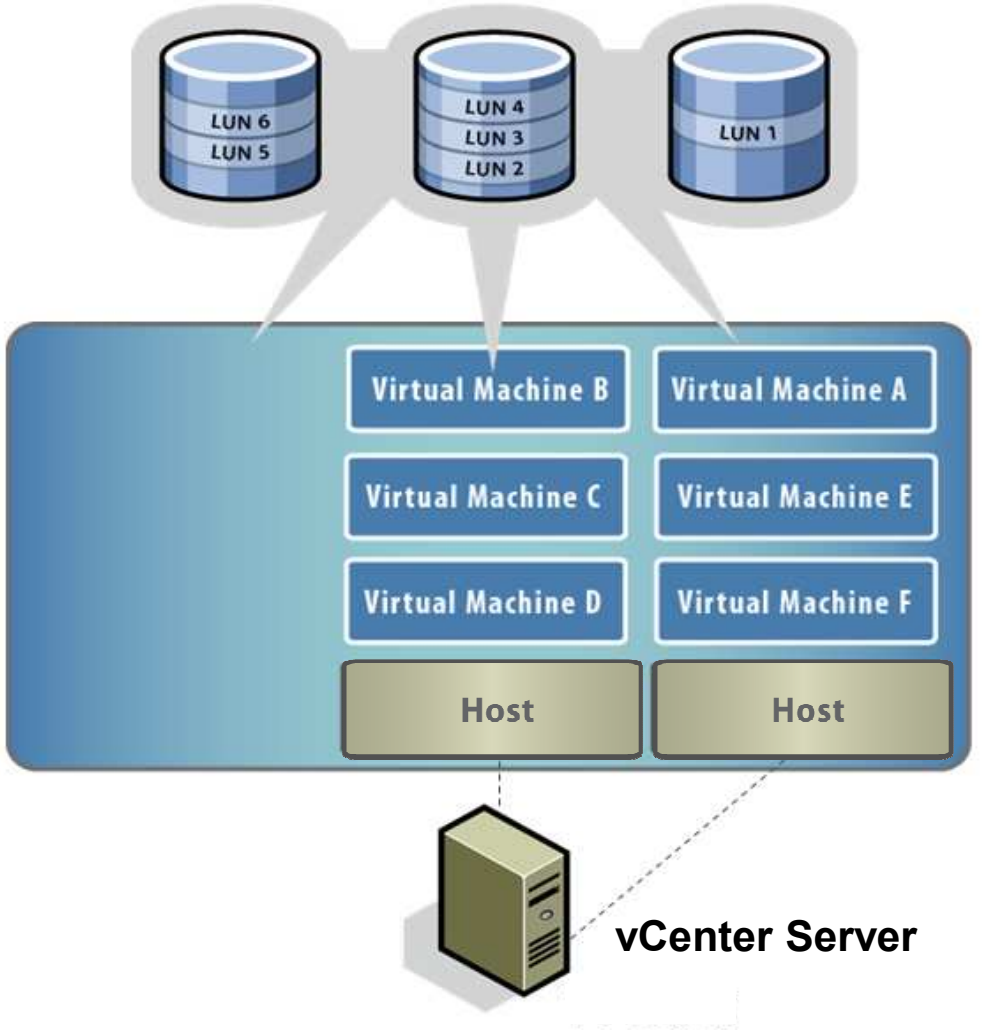
- Describe VMware HA functionality
- Enable VMware HA in a DRS cluster
- Configure VMware HA settings
- Describe VMware Fault Tolerance

VMware High Availability

VMware HA:

- Provides automatic restart of virtual machines in case of physical host failures
- Provides high availability while reducing the need for passive standby hardware and dedicated administrators
- Provides support for virtual machine failures with virtual machine monitoring and VMware Fault Tolerance
- Is configured, managed, and monitored using vCenter Server

VMware HA in Action



Using VMware HA and DRS Together

The first priority of VMware HA is the immediate availability of all virtual machines.

Using VMware HA and DRS together combines automatic failover with load balancing.

- Results in fast rebalancing of virtual machines after VMware HA has moved virtual machines to different hosts

Detecting a Host Failure

Detecting a host failure is done by monitoring the heartbeats sent between the primary and secondary hosts.

A heartbeat is sent every second (by default) over the "heartbeat" network.

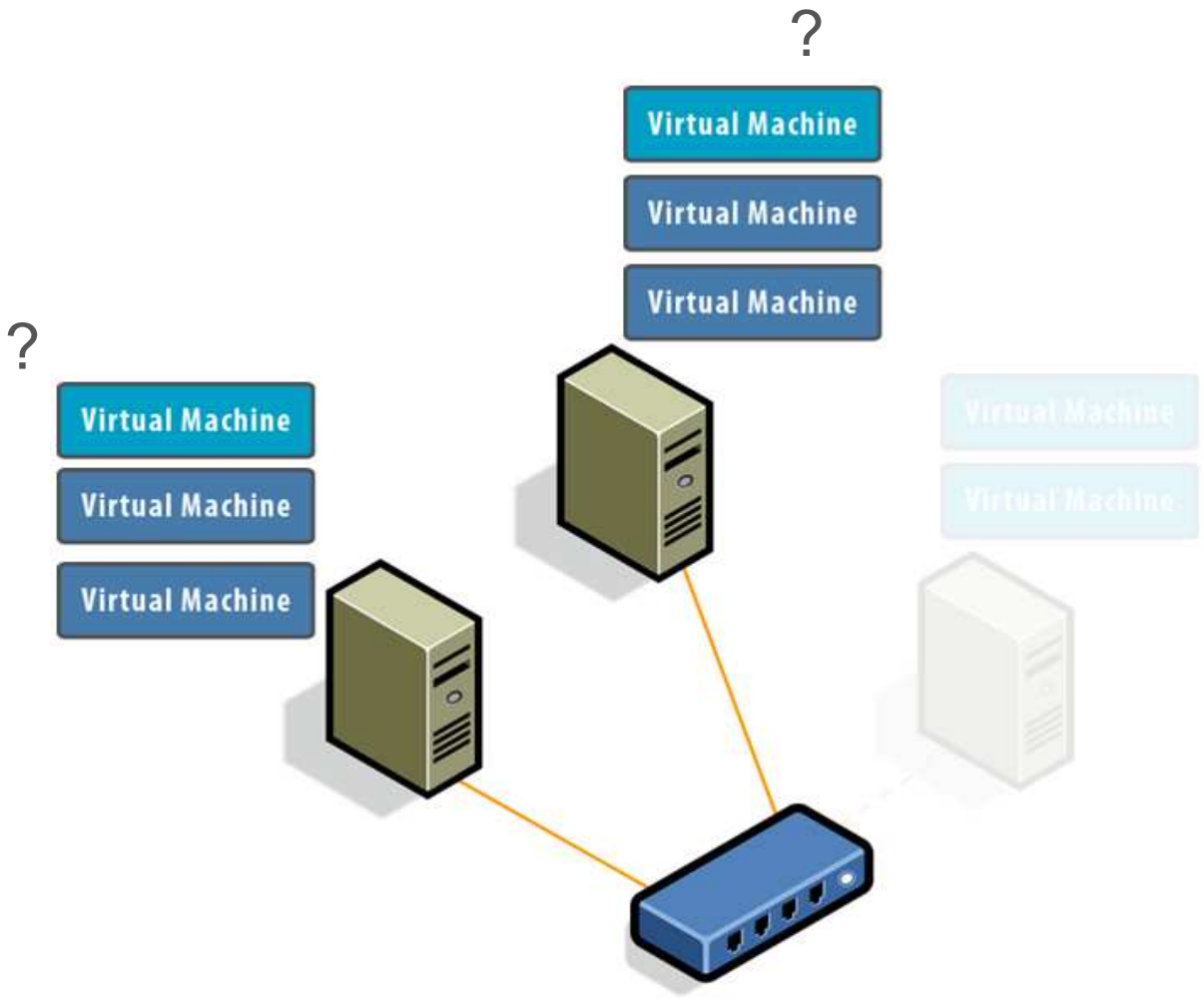
- On ESX hosts, the service console network is used.
- On ESXi hosts, a VMkernel network is used.

If a host in the cluster loses its connection to the heartbeat network, but the host continues running, the host is isolated from the cluster.

Host Isolation

A network failure might cause a "split-brain" condition.

VMware HA waits 12 seconds before deciding that a host is isolated.



VMware HA Prerequisites

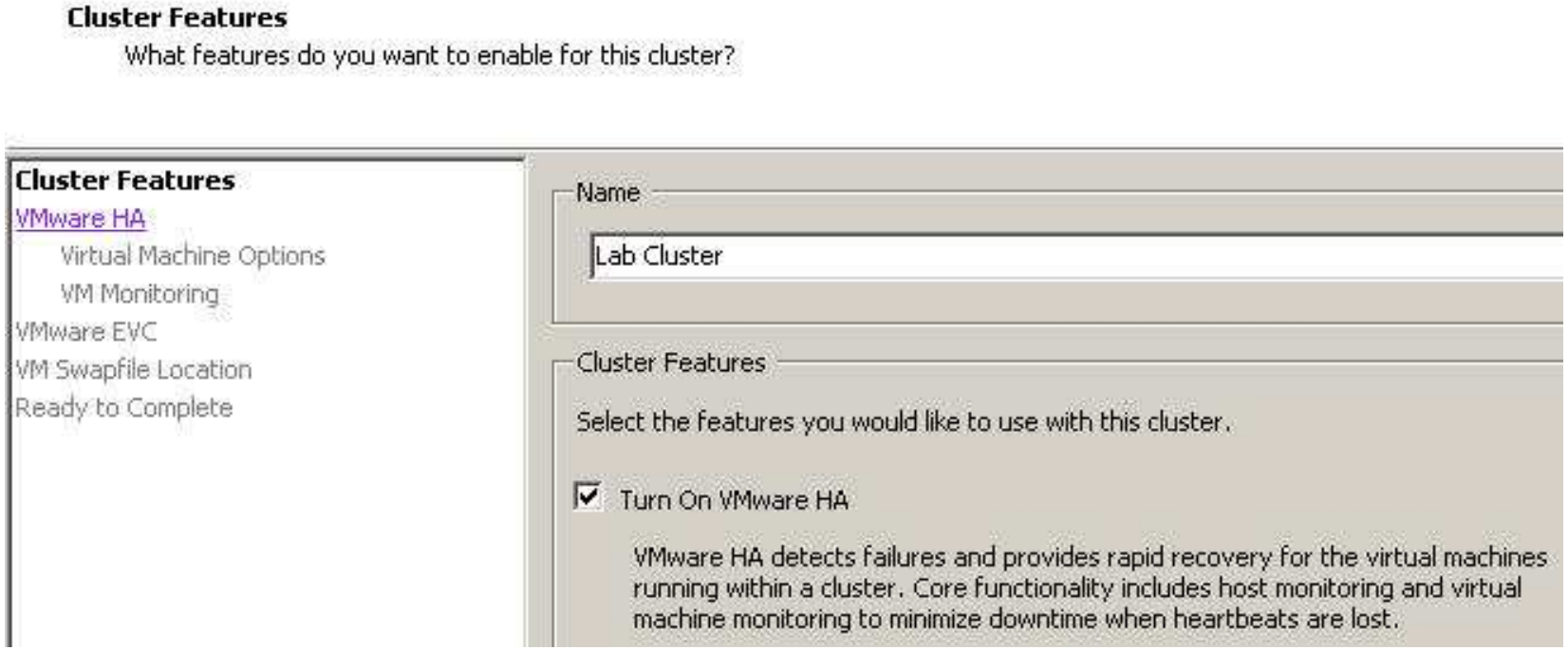
You should be able to power on a virtual machine from all hosts within the cluster.

- All hosts must have access to common resources (shared storage, virtual machine network).

Configure a redundant heartbeat network.

Enabling VMware HA

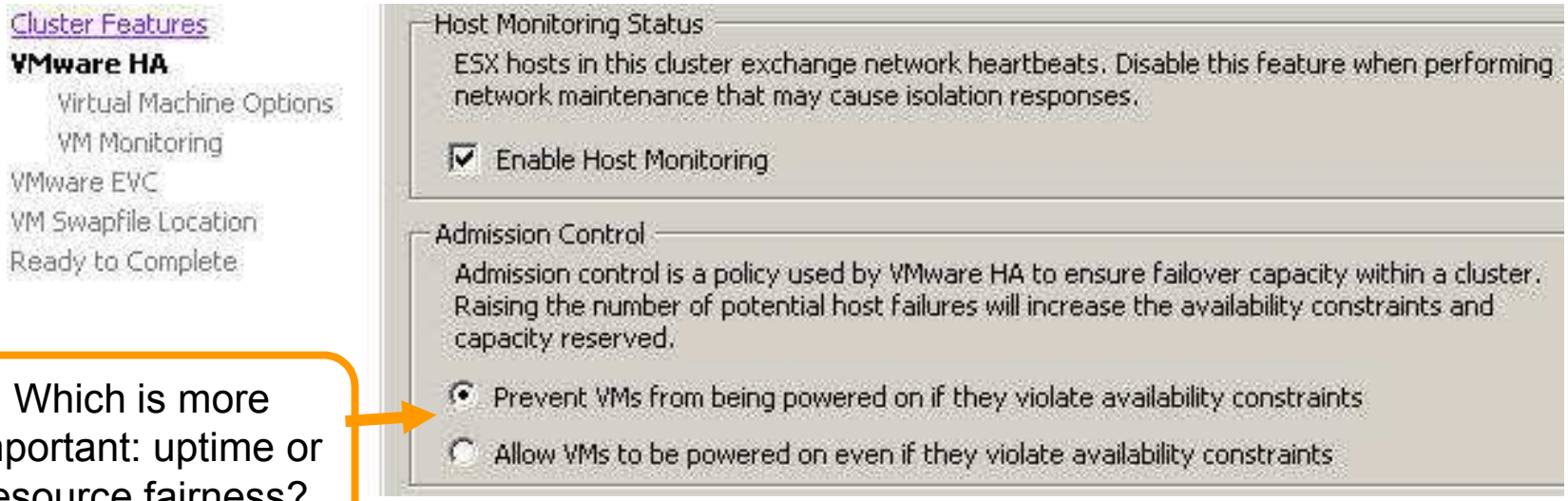
Enable VMware HA by creating a new cluster or modifying an existing DRS cluster.



Configuring VMware HA Settings

Disable host monitoring when performing maintenance activities on the host.

Admission control helps ensure that there are sufficient resources to provide high availability.



Which is more important: uptime or resource fairness?

Keeping Strict Admission Control Enabled

For maximum failover protection, keep strict admission control enabled.

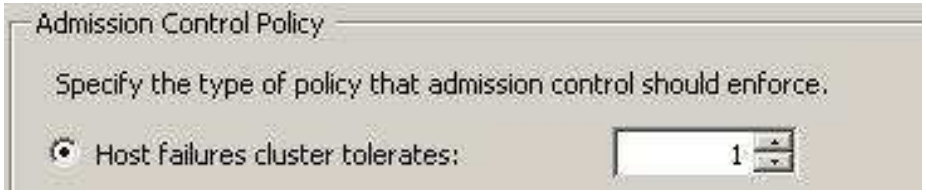
- DRS and VMware Distributed Power Management (DPM) protect the availability of failover capacity at all times.
- DRS does not evacuate virtual machines from a host if doing so violates failover requirements.
- DPM does not place hosts in standby mode if doing so would violate failover requirements.

Disable strict admission control if:

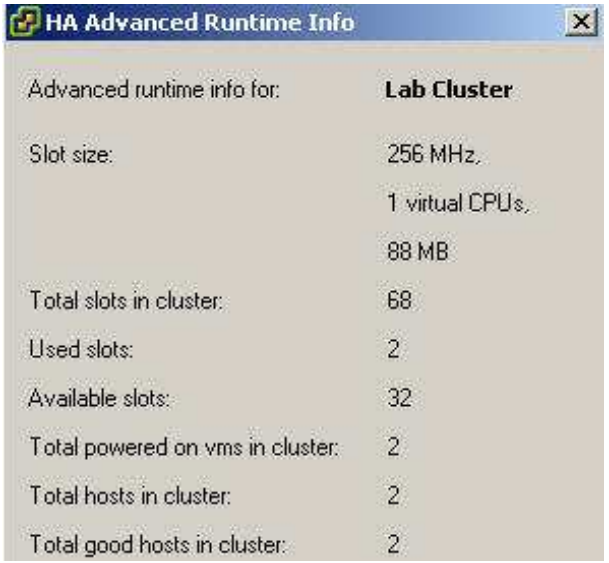
- You need to perform a nontrivial task and there are currently not enough resources in the cluster

Admission Control Policy: Host Failures Tolerated

VMware HA reserves enough resources to tolerate a specified number of host failures.



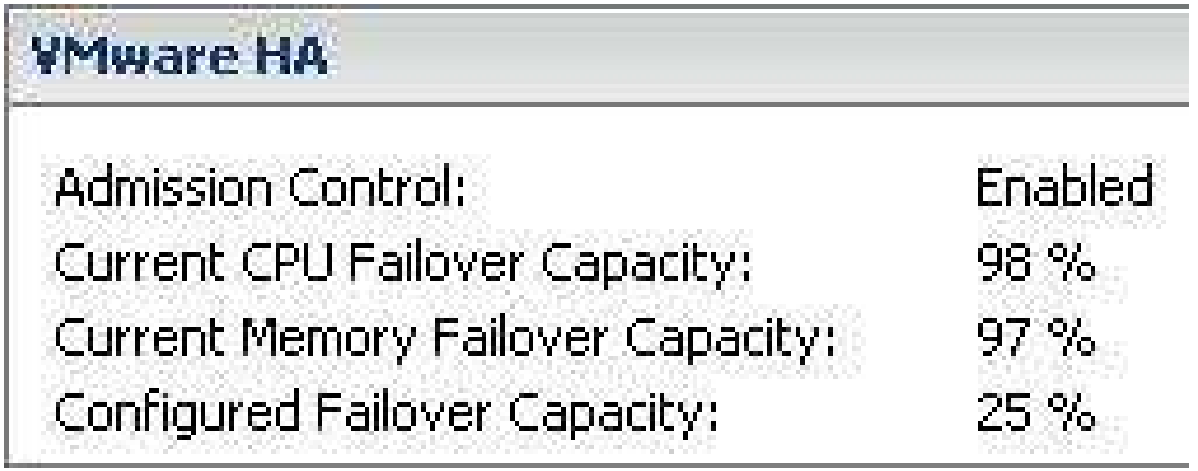
The HA Cluster Summary **tab shows information about this policy.**



Admission Control Policy: Cluster Resource %

VMware HA reserves specified percentage of total cluster capacity.

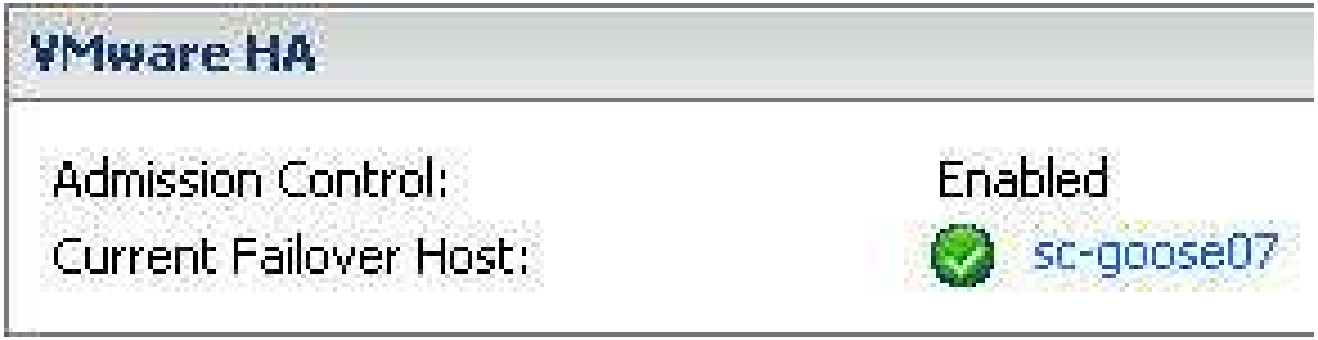
The HA Cluster Summary **tab shows information about this policy.**



Admission Control Policy: Specify Failover Host

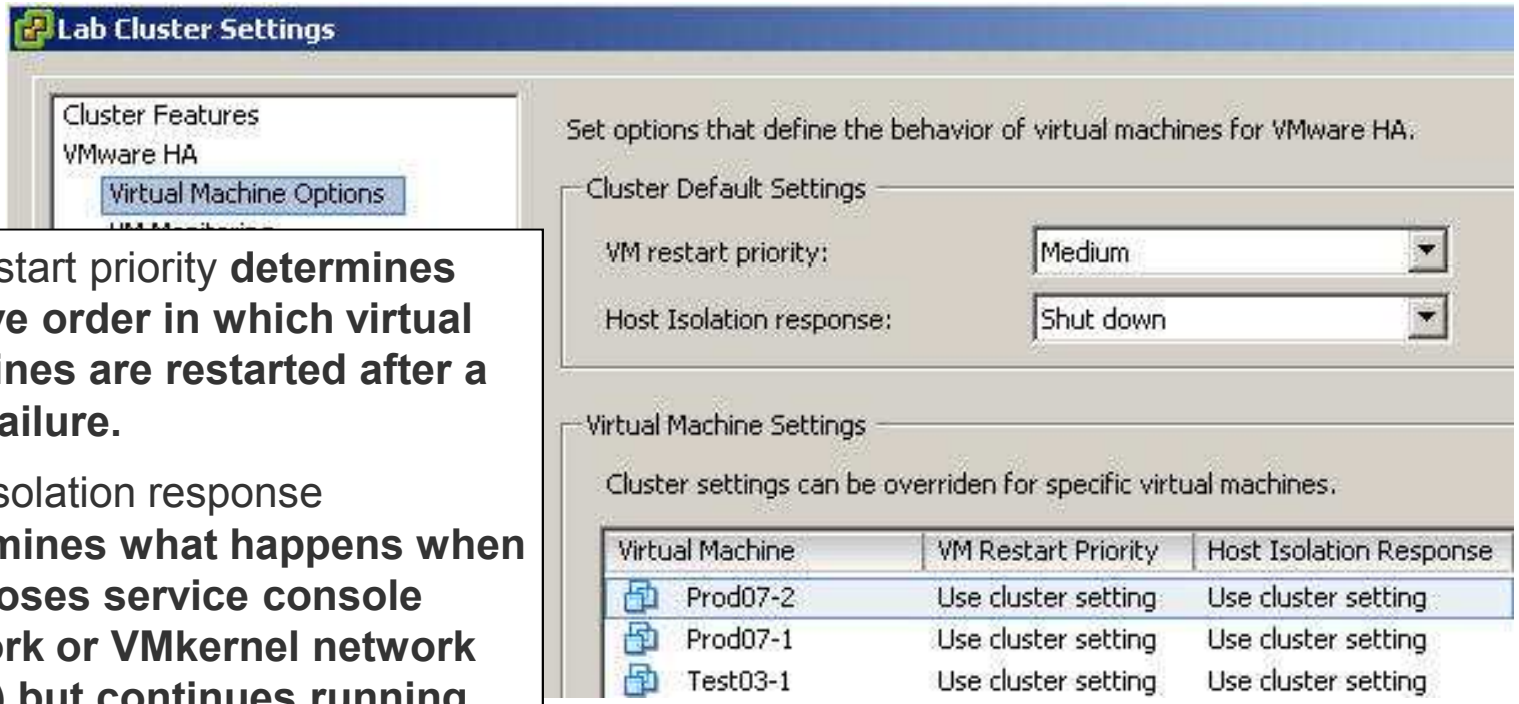
VMware HA dedicates a host exclusively for failover service.

The HA Cluster Summary **tab shows information about this policy.**



Configuring Virtual Machine Options

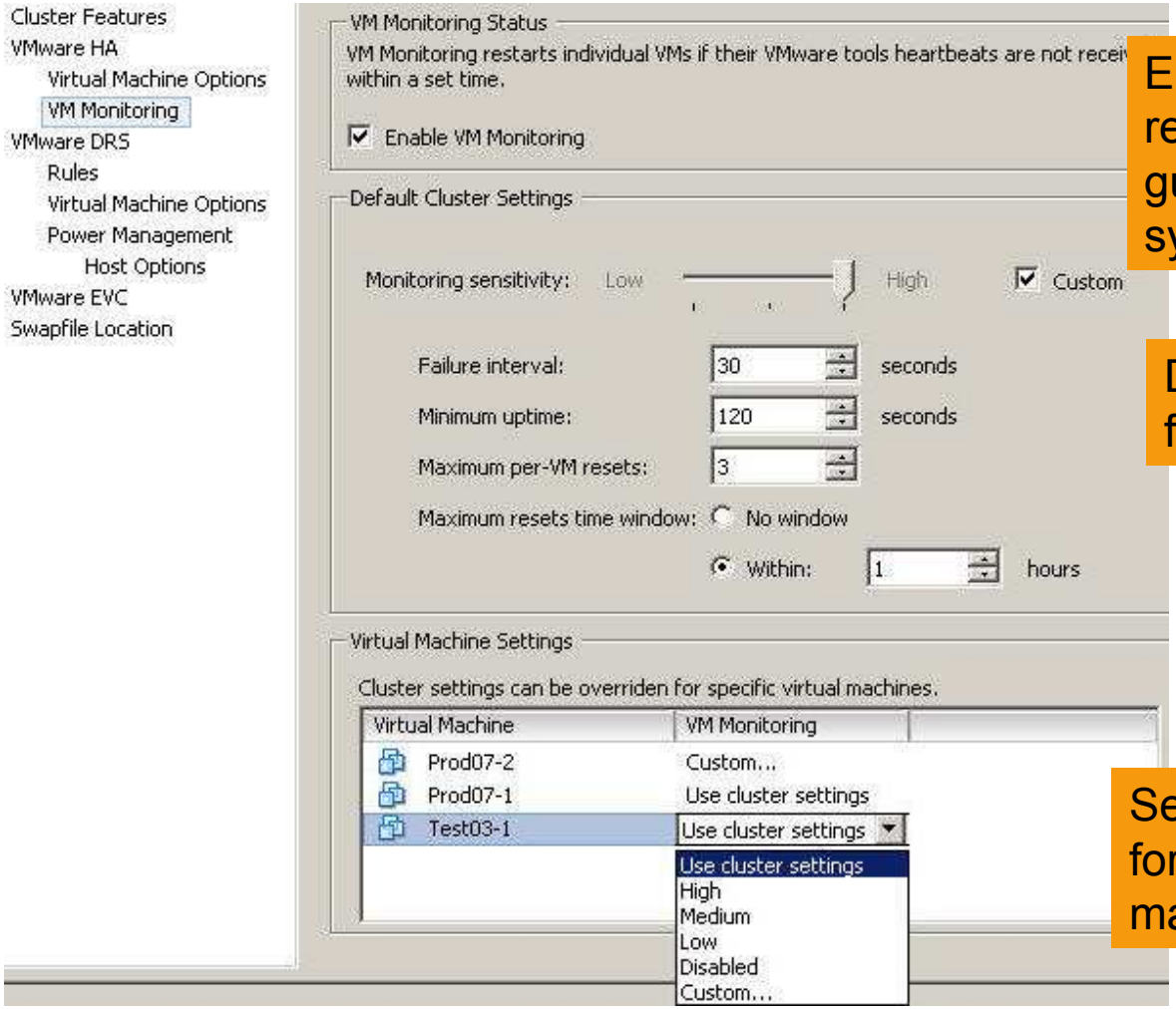
Configure options at the cluster level or per virtual machine.



VM restart priority **determines relative order in which virtual machines are restarted after a host failure.**

Host isolation response **determines what happens when host loses service console network or VMkernel network (ESXi) but continues running.**

Configuring Virtual Machine Monitoring

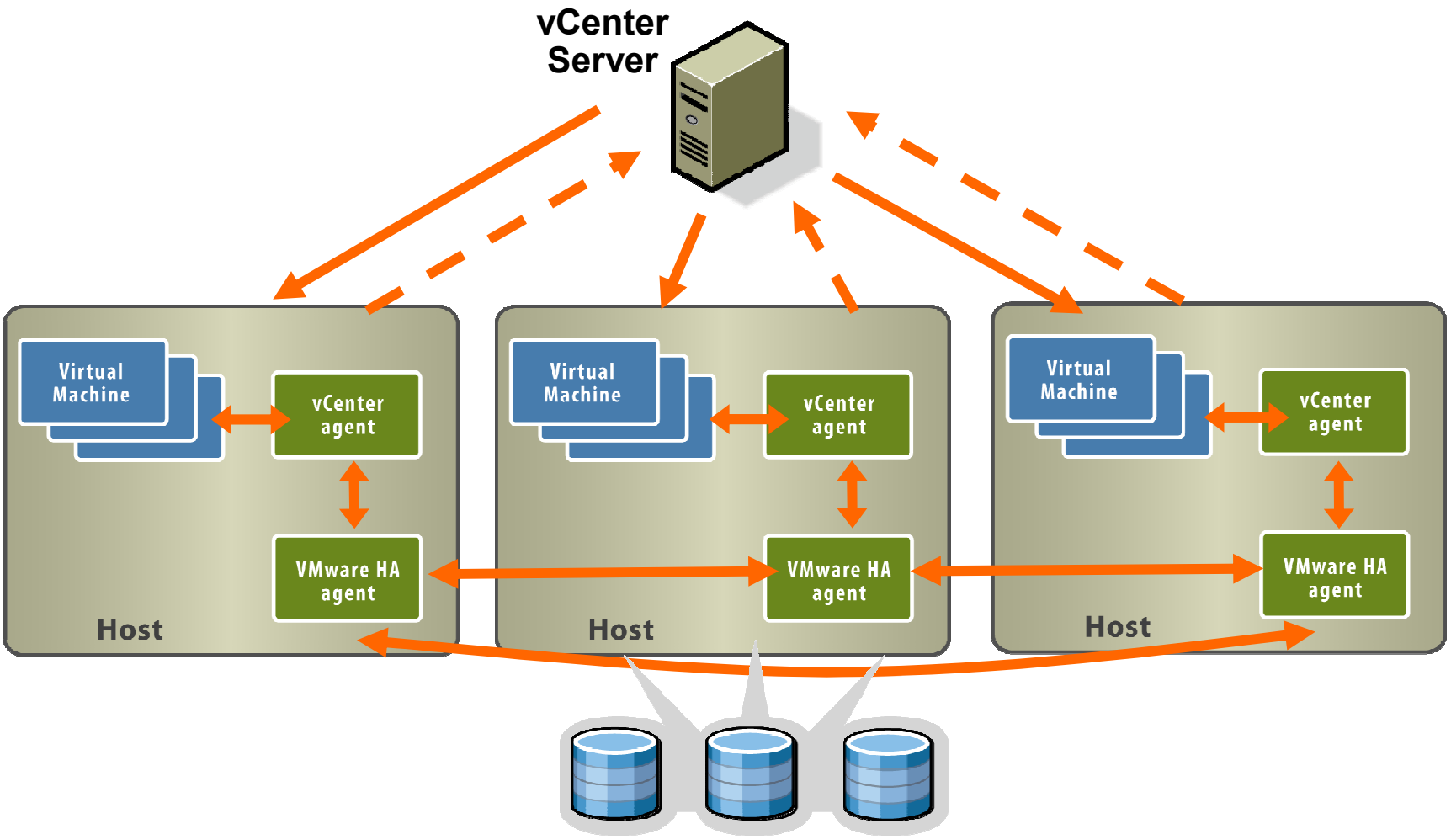


Enable automatic restart due to failure of guest operating system.

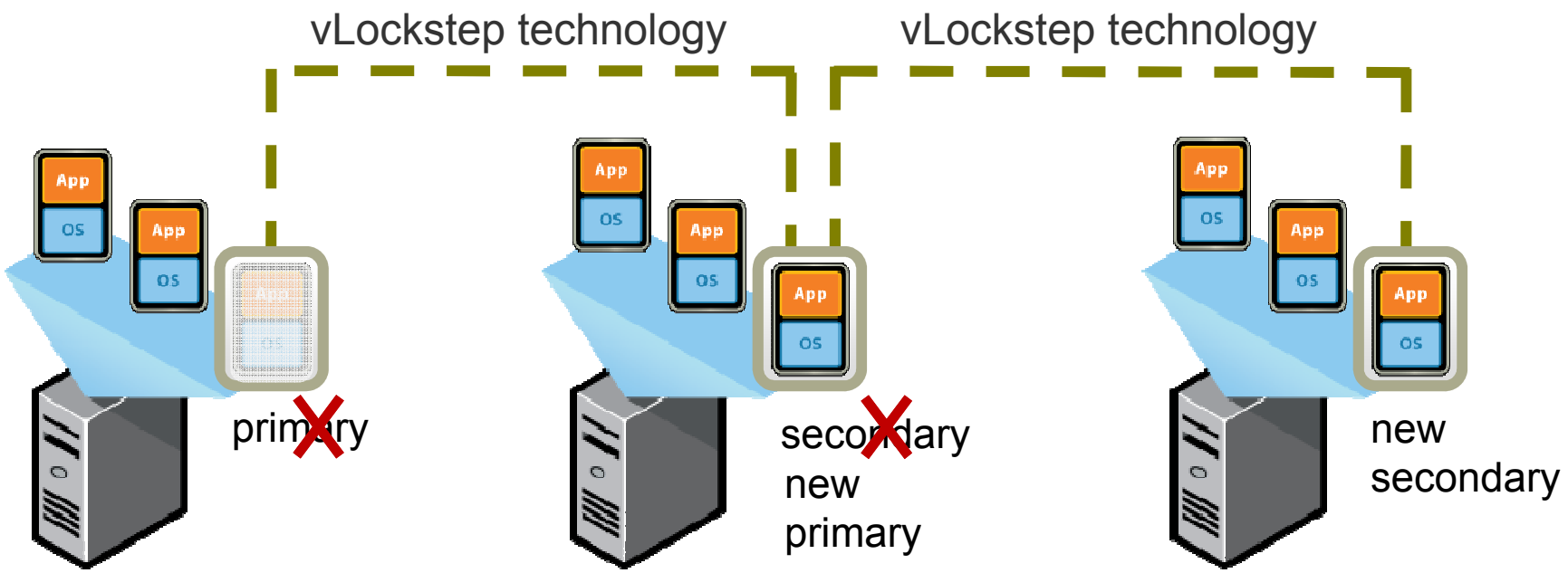
Determine how quickly failures are detected.

Set monitoring sensitivity for individual virtual machines.

Architecture of a VMware HA Cluster

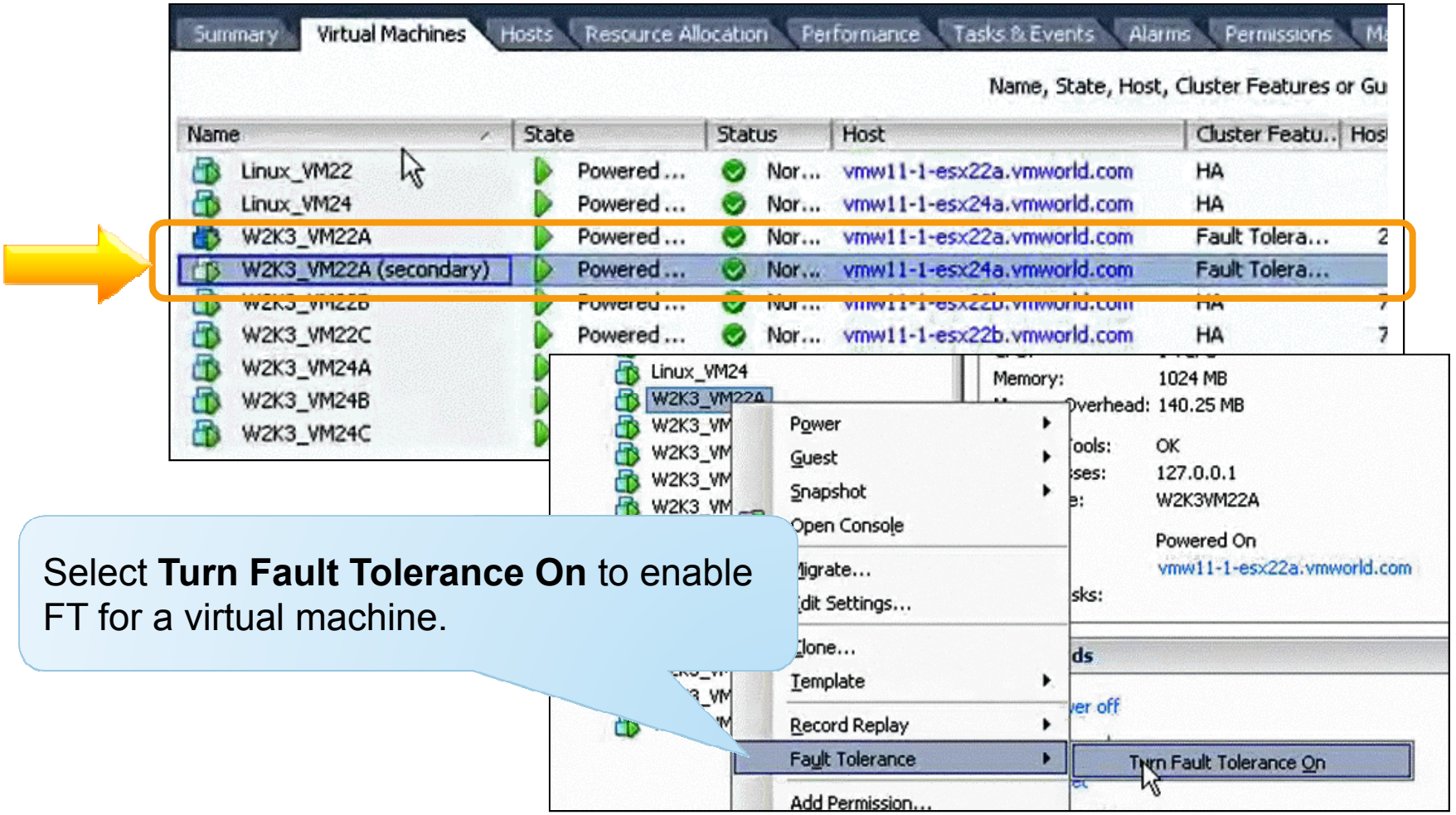


VMware Fault Tolerance



FT provides zero-downtime, zero-data-loss protection to virtual machines in a VMware HA cluster.

Enabling VMware Fault Tolerance



Select **Turn Fault Tolerance On** to enable FT for a virtual machine.

Lab 20

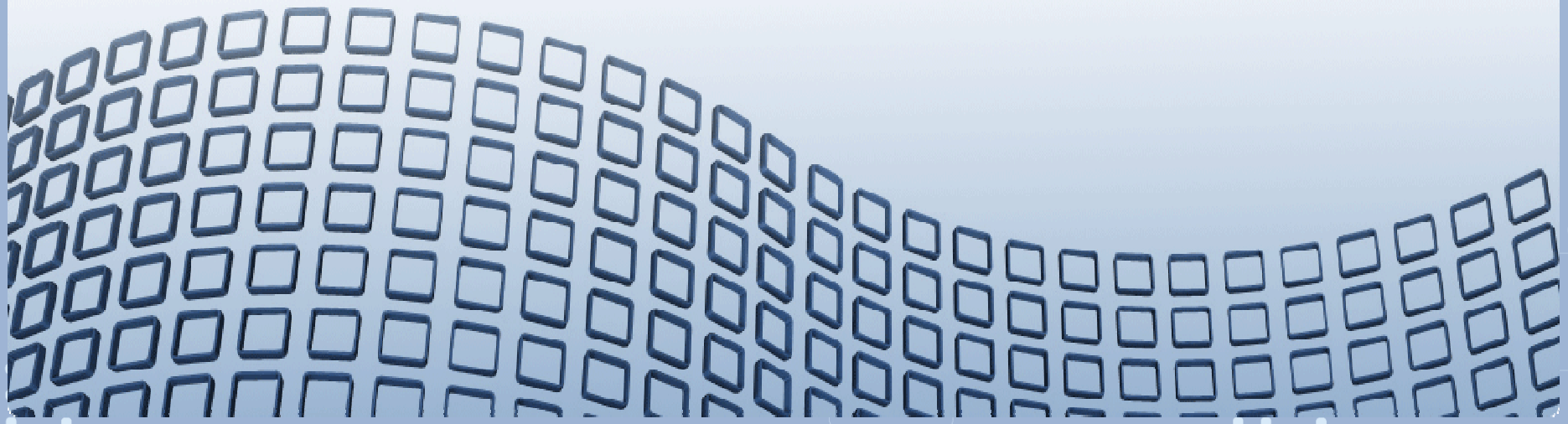
In this lab, you will demonstrate VMware HA functionality.

1. Modify the cluster to add VMware HA functionality.
2. Verify VMware HA functionality.

Lesson Summary

- It is a good practice to enable both DRS and VMware HA in a cluster.
- For maximum protection, keep strict admission control enabled because this helps to ensure that sufficient resources remain, even after some number of concurrent host failures.
- FT provides zero-downtime and zero-data-loss protection to designated virtual machines in a VMware HA cluster.

Lesson 3:
Data Protection



Lesson Objectives

- Describe the strategy for backing up ESX/ESXi hosts
- Describe the strategy for backing up virtual machines
- Describe VMware data-protection solutions:
  - Consolidated Backup
  - Data Recovery
- Back up a virtual machine using Data Recovery

What to Back Up

These are the vSphere components to back up:

- ESX service console
- ESXi configuration
- Virtual machine data

Backing Up the ESX Service Console

Service console backups do not need to be made as frequently as virtual machine backups.

VMware supports a number of different backup agents for the service console.

Backing Up ESXi Configuration Data

Always back up your ESXi host configuration after changing the configuration or upgrading the ESXi image.

To back up an ESXi Installable or ESXi Embedded configuration, use the vicfg-cfgbackup command.

- Use command to back up or restore the host's configuration.
- Run from the vSphere Command-Line Interface.

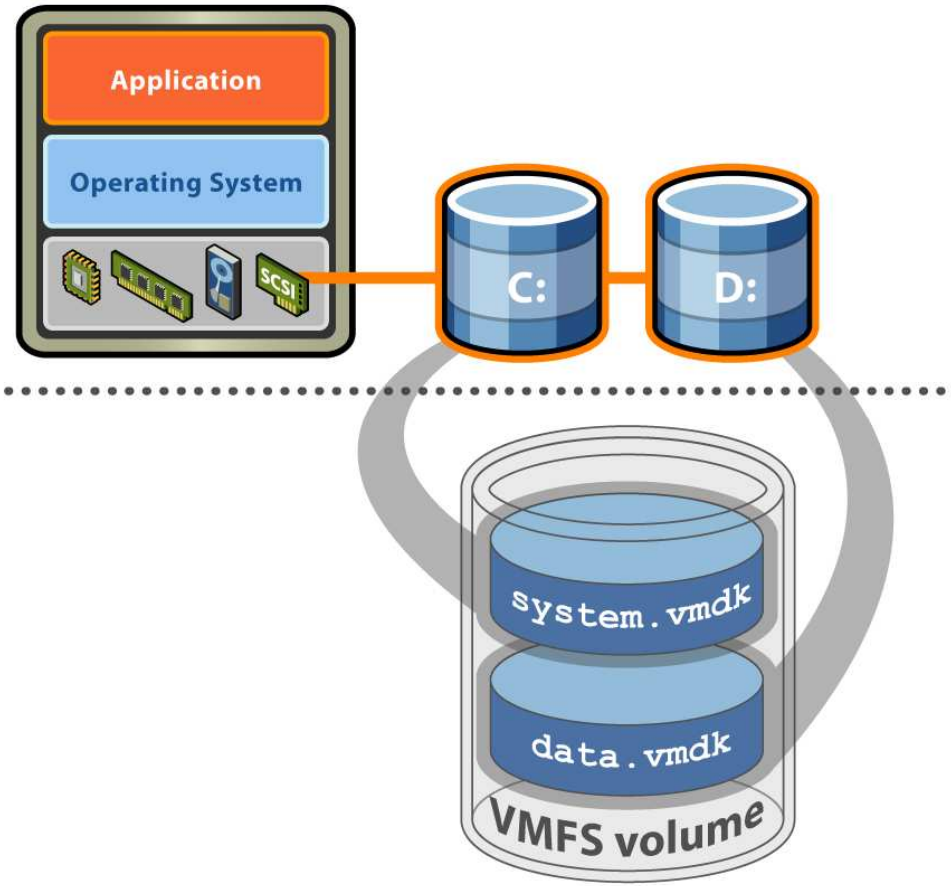
Backing Up Virtual Machines

Store application data in separate virtual disks from system images.

Use full virtual machine backups for system images.

- The alternative is to redeploy from template.

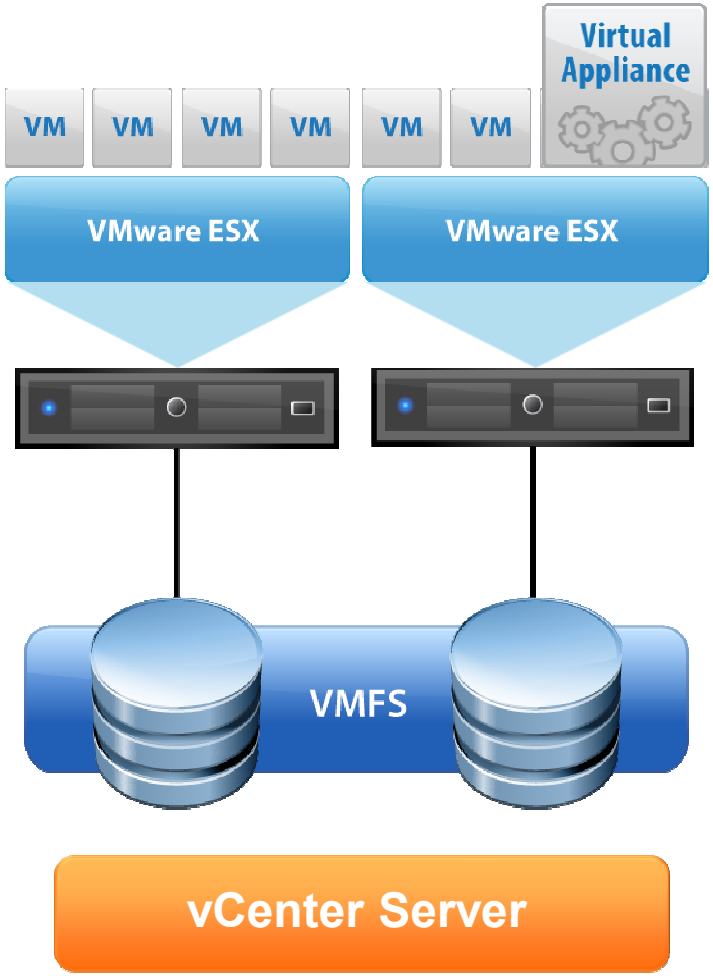
Use Consolidated Backup or Data Recovery.



Consolidated Backup

- Works along with third-party backup agents to perform backups
- Centralizes backup on a Consolidated Backup proxy server, which can be a physical or virtual machine
- Eliminates the need for having a backup agent installed in each virtual machine
- Can read virtual disk data to back up directly from storage (Fibre Channel or iSCSI)
- Supports file-level full and incremental backups for Windows virtual machines and image-level backups of any supported guest operating system

Data Recovery



Backup-and-recovery appliance

- Agentless, disk-based backup and recovery tool for virtual machines
- Linux appliance

vCenter Server integration

- vSphere Client plug-in
- Wizard-driven backup and restore job creation

For the vSphere administrator who

- Wants a simple user interface with minimal options
- Wants to leverage disk as destination storage

Setting Up Data Recovery

1. Add the appliance to the vCenter Server inventory by deploying an OVF template.
   a. Configure the appliance networking.
   b. Configure the appliance time zone.
2. Add the destination storage device to the appliance.
3. Install the Data Recovery plug-in into the vSphere Client.
4. Access the management user interface in the vSphere Client at **Home** > **Solutions and Applications**.

   The host for the appliance and the host for the virtual machine being backed up must be licensed for Data Recovery.

Backup Job

Create a backup job using the management UI.

Each appliance supports backing up 100 virtual machines.

Each appliance supports a maximum of 100 backup jobs.

A backup job consists of:

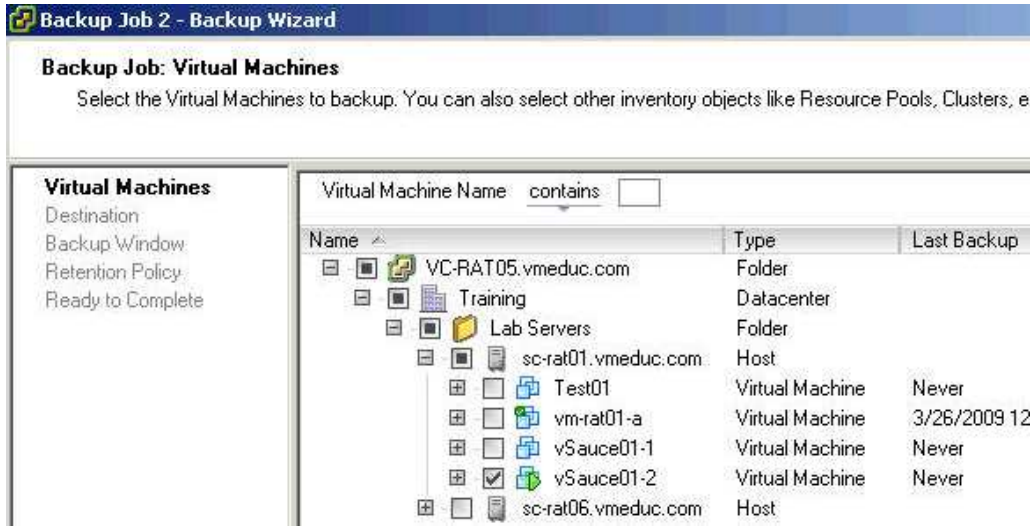
- Source (virtual machines to back up)
- Destination
- Backup window
- Retention policy

Backup Job: Source

The backup source can be at any level in the inventory – datacenter, folder, host, virtual machine, virtual machine's disk.

The user is warned if:

- Virtual machine is not on a licensed host
- More than 100 virtual machines are selected for backup



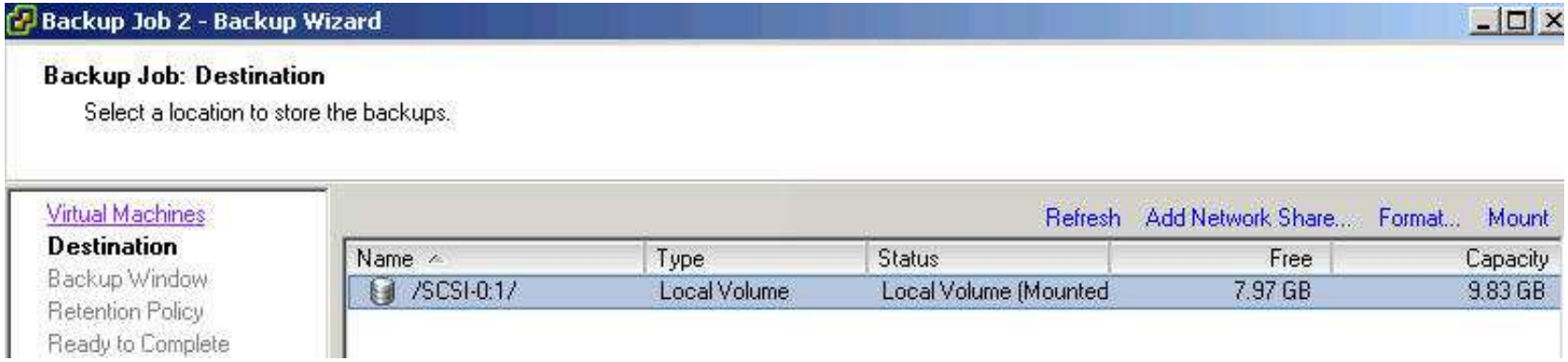
Backup Job: Destination

The destination storage can be a VMware vStorage VMFS datastore (local, iSCSI, or Fibre Channel), an NFS datastore, or a CIFS share.

- Destination is formatted as deduplication storage.

Manually add the destination, a virtual disk, to the appliance.

Each backup job can use at most two different destinations.

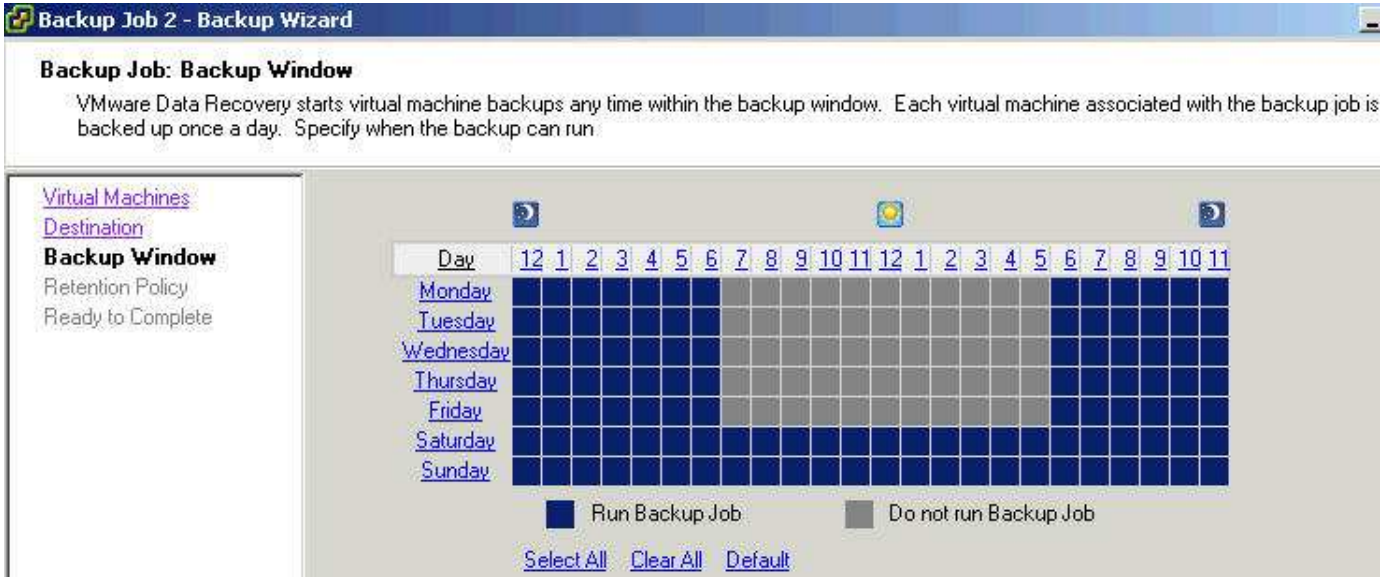


Backup Job: Backup Window

Specify the time during the week when the backup can run.

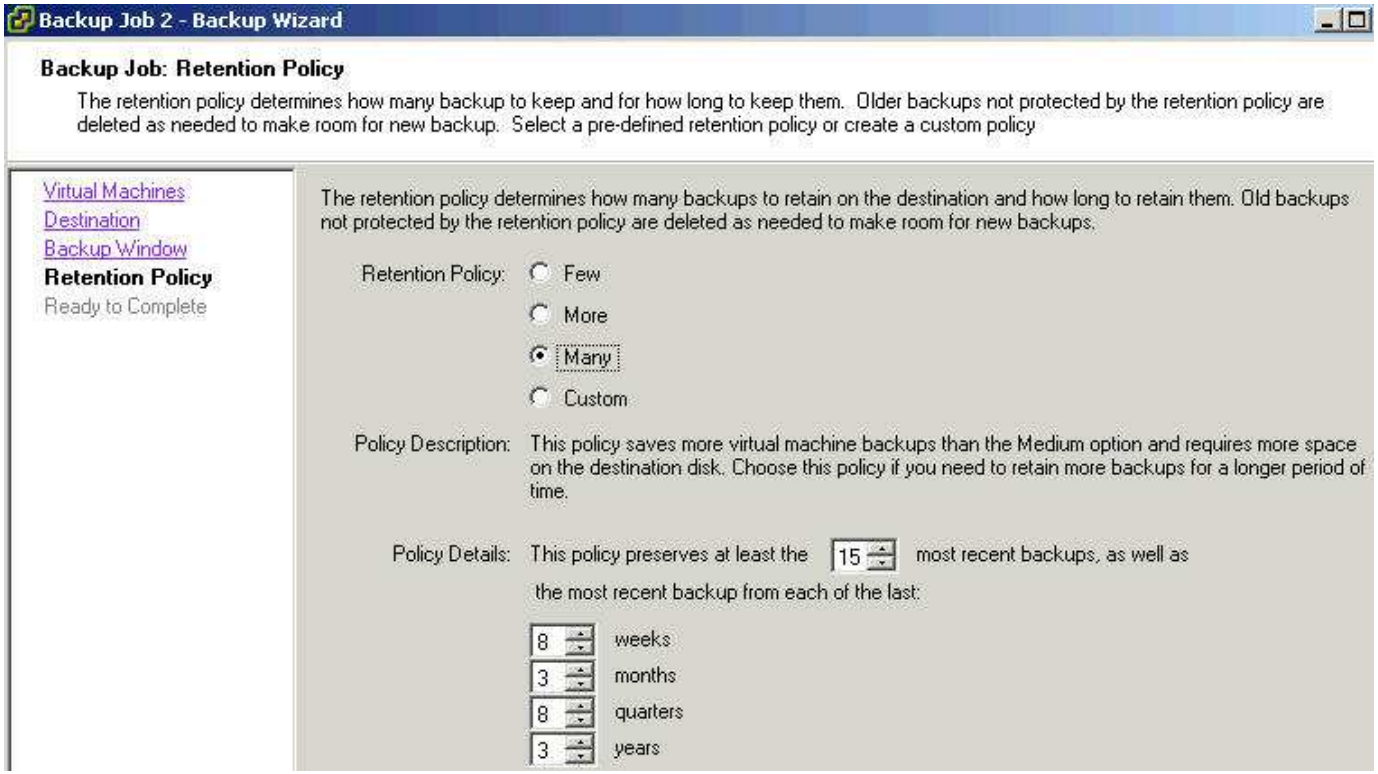
Virtual machines are sorted in ascending order based on the last backup time.

- Virtual machines not backed up for the longest time have highest priority.



Backup Job: Retention Policy

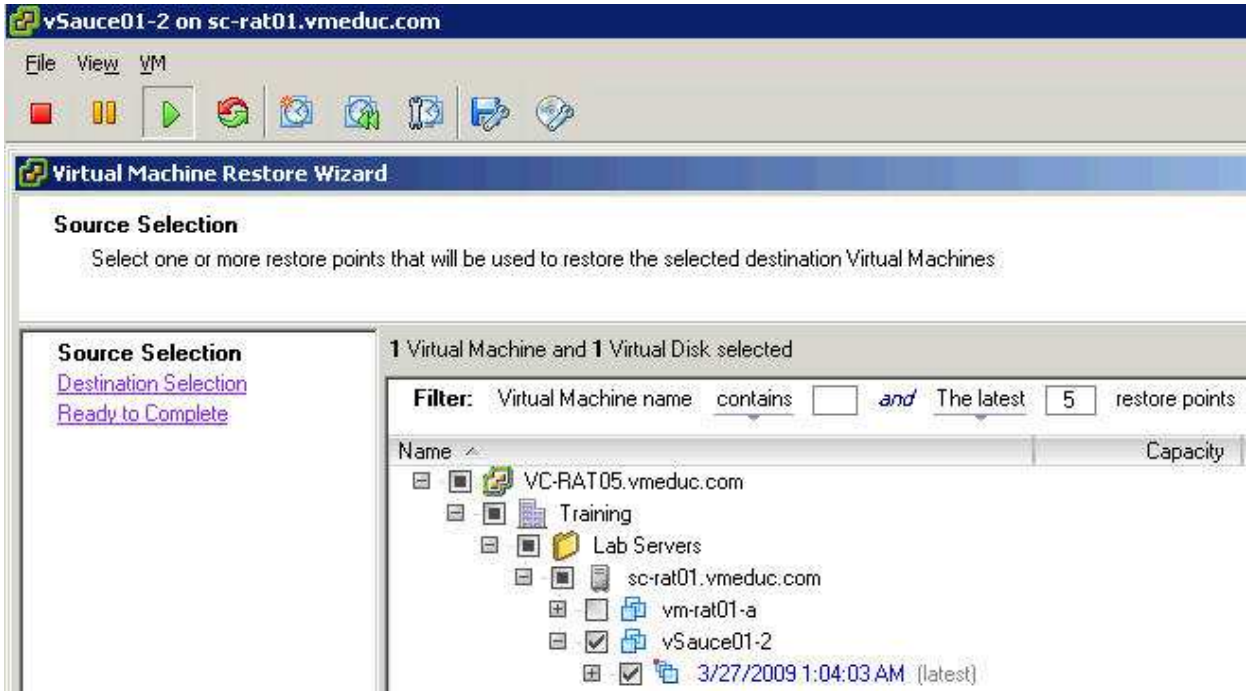
Specify a predefined or custom retention policy.



Restore Job: Selecting Object to Restore

To create a restore job, select the object to restore:

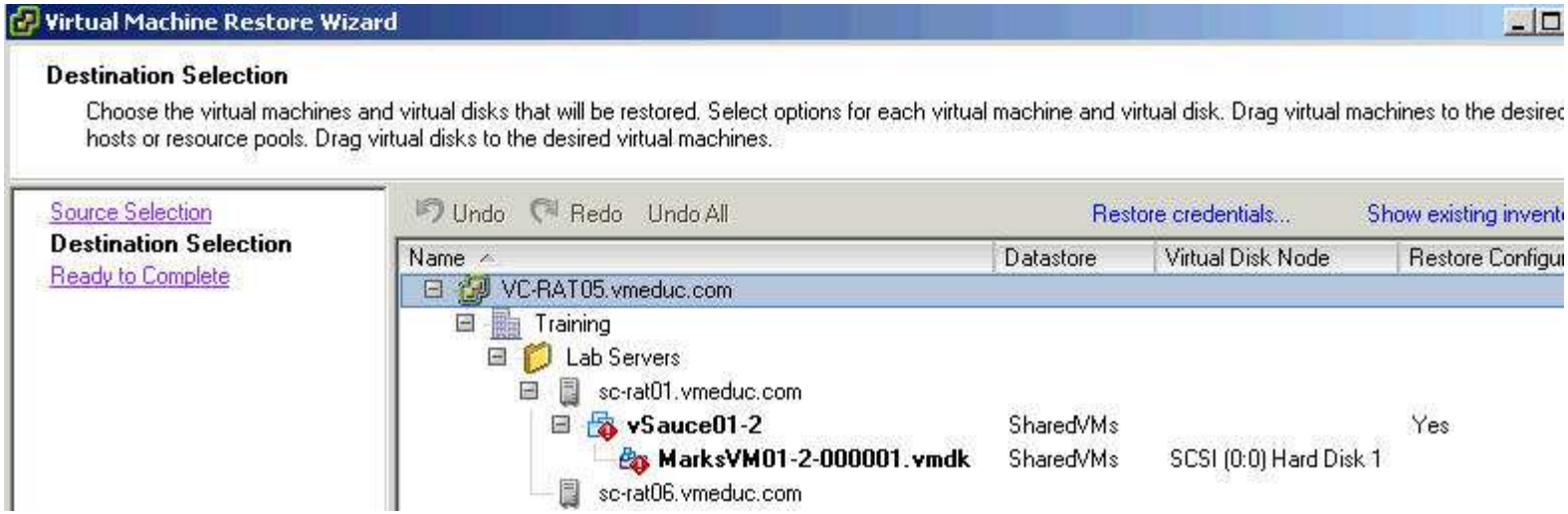
- For example, multiple virtual machines or a certain disk of a virtual machine



Restore Job: Selecting the Destination

Select the destination:

- Original location of virtual machine
- Different host, resource pool, or datastore



Lab 21

In this lab, you will back up and recover a virtual machine using VMware Data Recovery.

1. Install the Data Recovery plug-in.
2. Modify the Data Recovery virtual machine.
3. Perform initial setup of the Data Recovery appliance.
4. Create a backup job.
5. Create a restore job.

Lesson Summary

- Back up the ESX service console using a supported third-party backup agent or by making a copy of important configuration files.
- Back up the ESXi configuration data using the `vicfg-cfgbackup` command.
- Back up virtual machines using the Data Recovery disk-based backup utility.

Key Points

- VMware HA provides high availability to virtual machines.
- FT and MSCS clustering provides fault tolerance to virtual machines.
- Data Recovery and Consolidated Backup provide data protection for virtual machines.