Migrating Virtual Machines

Migrating Virtual Machines

Migration means moving a virtual machine from one host, datastore, or vCenter Server system to another host, datastore, or vCenter Server system.

Types of migrations:

- Cold: Migrate a powered-off virtual machine to a new host or datastore.
- Suspended: Migrate a suspended virtual machine to a new host or datastore.
- vSphere vMotion: Migrate a powered-on virtual machine to a new host.
- vSphere Storage vMotion: Migrate a powered-on virtual machine's files to a new datastore.
- Shared-nothing vSphere vMotion: Migrate a powered-on virtual machine to a new host and a new datastore simultaneously.

vSphere vMotion Migration

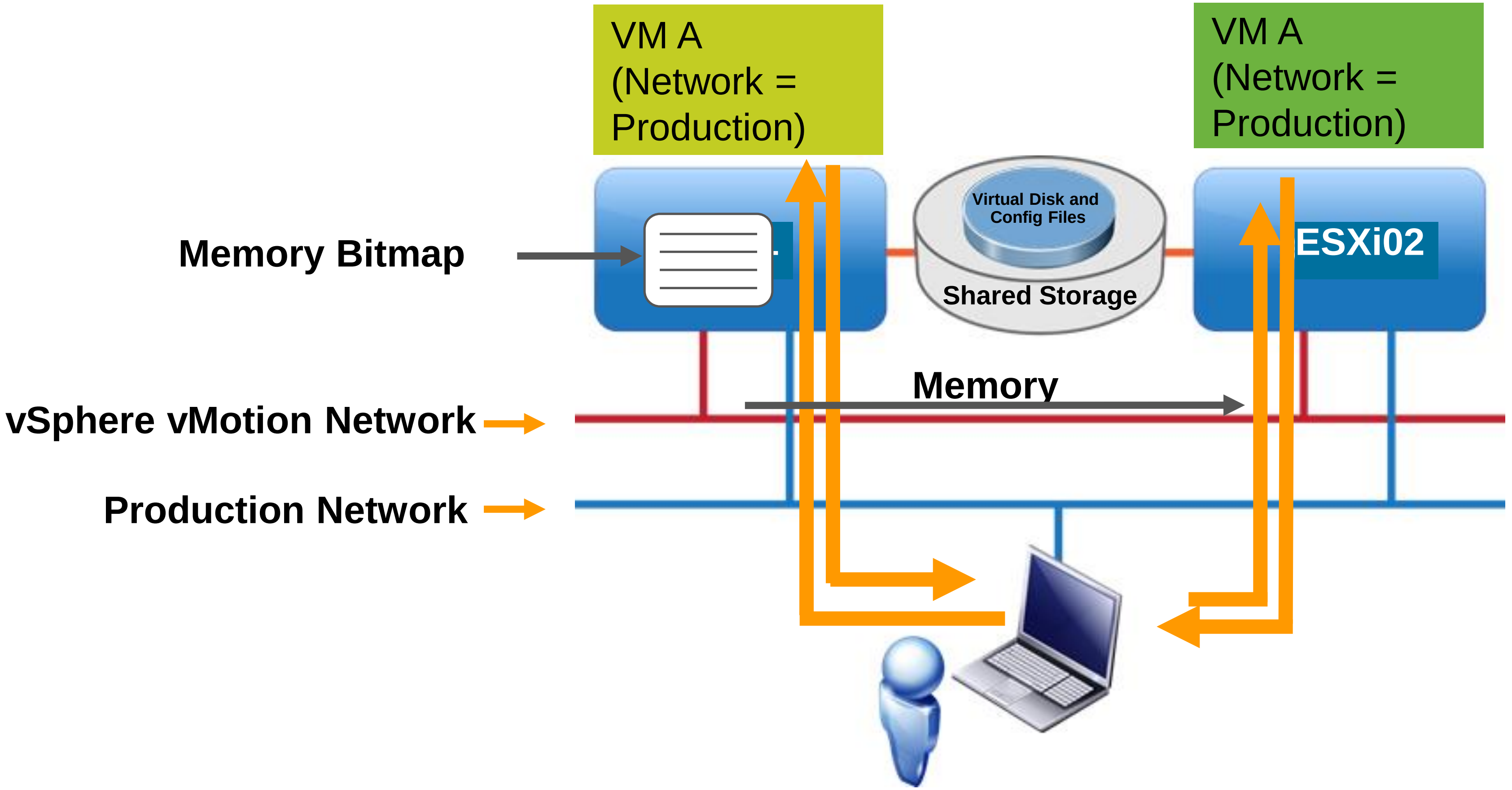
A vSphere vMotion migration moves a powered-on virtual machine from one host to another.

vSphere vMotion provides the following capabilities:

- Improves overall hardware use
- Enables continuous virtual machine operation while accommodating scheduled hardware downtime
- Allows vSphere DRS to balance virtual machines across hosts

vSphere vMotion Migration Workflow

The source host (ESXi01) and the destination host (ESXi02) have access to the shared datastore that holds the virtual machine’s files.



vSphere vMotion Migration Requirements

A virtual machine must meet the following requirements:

- It should not have an active connection to an internal virtual switch, because migrating such a virtual machine produces an error.
- It must not have CPU affinity configured.
- It must not have a connection to a virtual device, such as a CD/DVD or floppy drive, with a local image mounted.
- If its swap file is not accessible to the destination host, vSphere vMotion must be able to create a swap file that is accessible to the destination host before migration can begin.
- If it uses an RDM disk, the RDM file and the LUN to which it maps must be accessible by the destination host.

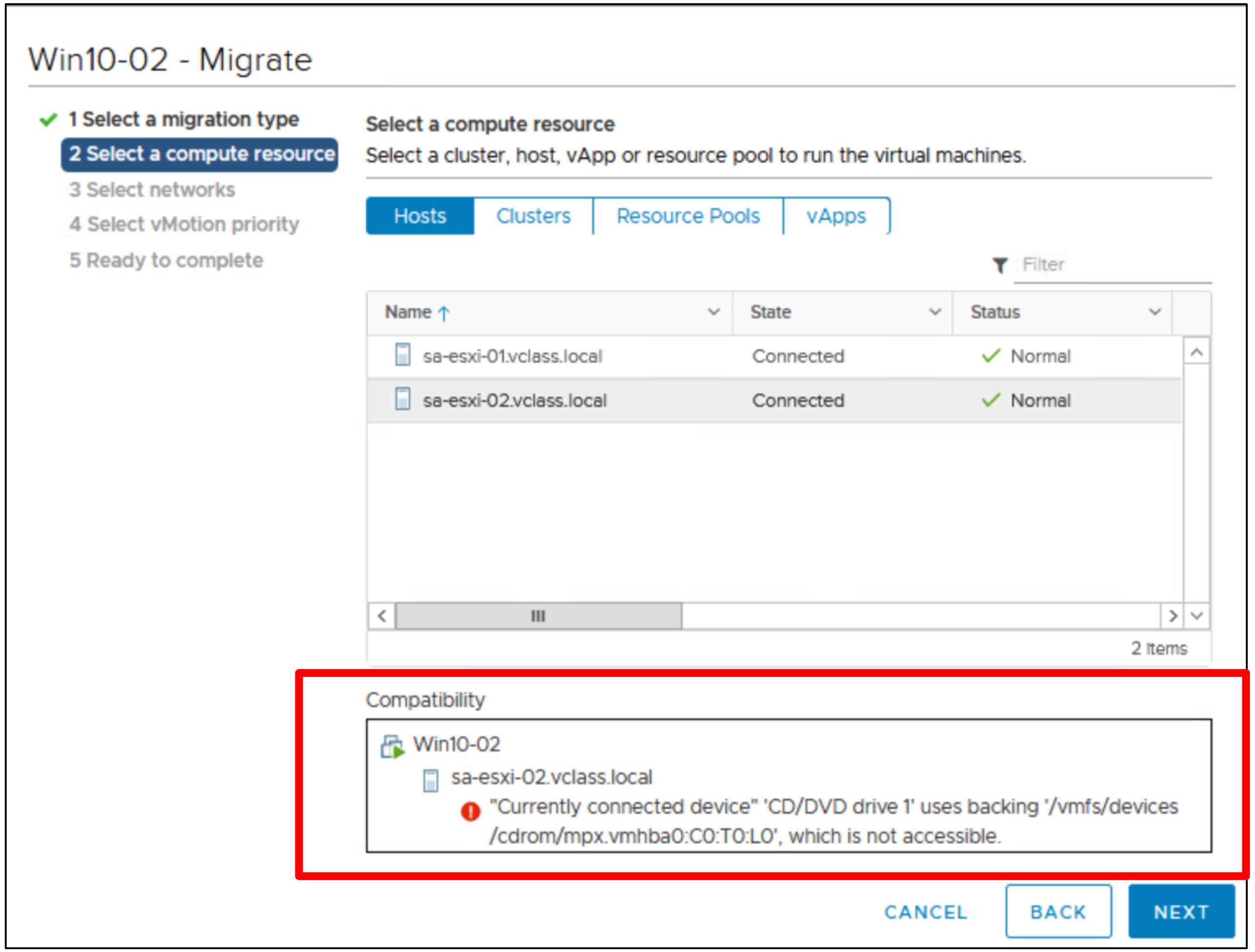
Host Requirements for vSphere vMotion Migration

Source and destination hosts must have the following characteristics:

- Accessibility to all of the virtual machine’s storage (Fibre Channel, iSCSI, or NAS):
  - 128 concurrent vSphere vMotion migrations are possible per VMFS or NFS datastore.
- At least a 1 Gigabit Ethernet (1GigE) network:
  - Each active vSphere vMotion process requires a minimum throughput of 250Mbit/sec on the vSphere vMotion network.
  - Concurrent vSphere vMotion migrations are limited to four on a 1 Gbps network.
  - Concurrent vSphere vMotion migrations are limited to eight on a 10 Gbps (or faster) network.
  - For better performance, dedicate at least two port groups to the vSphere vMotion traffic.
- Compatible CPUs:
  - The CPU feature sets of both the source host and the destination host must be compatible.
  - Some features can be hidden by using EVC or compatibility masks.

Checking vSphere vMotion Errors

When you select the host and cluster, a validation check is performed to verify that most vSphere vMotion requirements were met.



Win10-02 - Migrate

- ✓ 1 Select a migration type
- 2 Select a compute resource
- 3 Select networks
- 4 Select vMotion priority
- 5 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

Name ↑	State	Status
sa-esxi-01.vclass.local	Connected	✓ Normal
sa-esxi-02.vclass.local	Connected	✓ Normal

2 items

Compatibility

Win10-02

sa-esxi-02.vclass.local

"Currently connected device" 'CD/DVD drive 1' uses backing '/vmfs/devices/cdrom/mpx.vmhba0:C0:T0:L0', which is not accessible.

Migration with vSphere Storage vMotion

With vSphere Storage vMotion, you can migrate a virtual machine and its disk files from one datastore to another while the virtual machine is running.

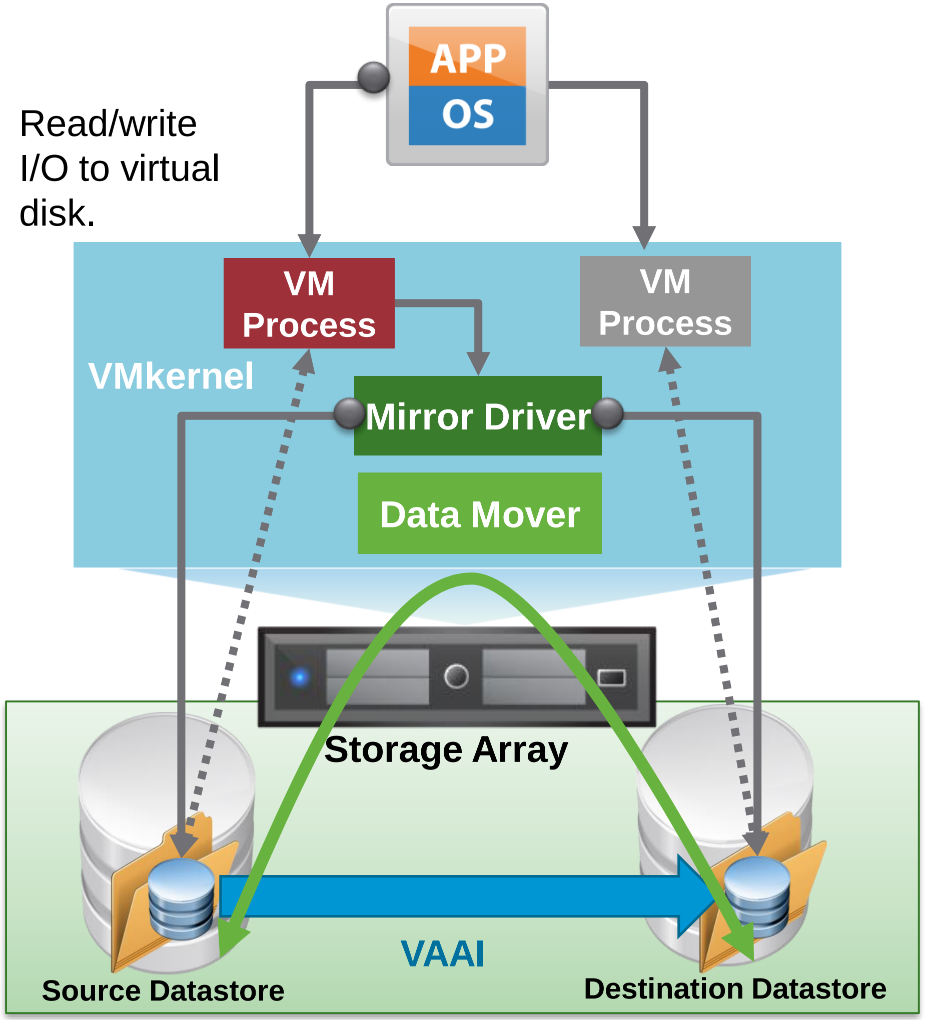
Using vSphere Storage vMotion you can perform the following tasks:

- Move virtual machines off arrays for maintenance or to upgrade.
- Change the disk provisioning type.
- Change virtual machine files on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and `.nvram` files.
- Move virtual machines off a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.
- Redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

vSphere Storage vMotion in Action

vSphere Storage vMotion uses an I/O mirroring architecture to copy disk blocks between source and destination:

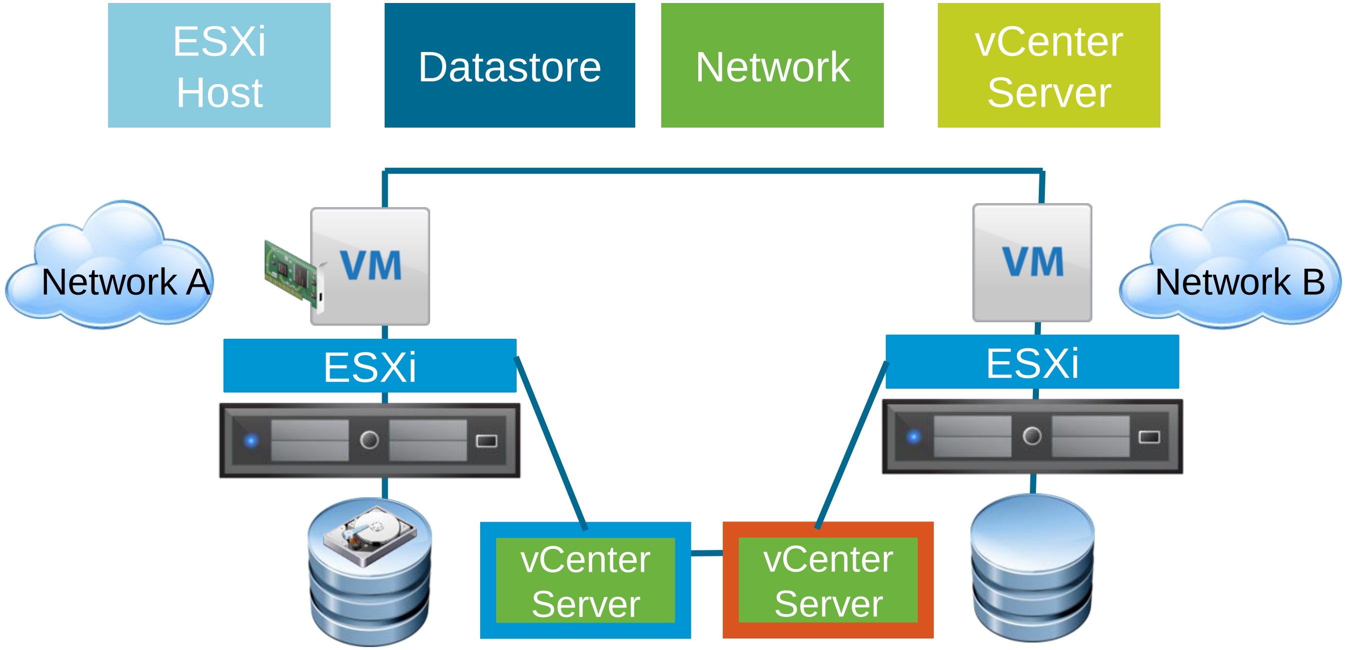
1. Initiate storage migration.
2. Use the VMkernel data mover or vSphere Storage APIs - Array Integration to copy data.
3. Start a new virtual machine process.
4. Mirror I/O calls to file blocks that are already copied to virtual disk on the destination datastore.
5. Cut over to the destination virtual machine process to begin accessing the virtual disk copy.



Shared-Nothing vSphere vMotion Migration

Shared-nothing vSphere vMotion migration enables a virtual machine to change its host, datastores, networks, and vCenter Server instances simultaneously, even if the two hosts do not have a shared storage.

This technique combines vSphere vMotion and vSphere Storage vMotion into a single operation.



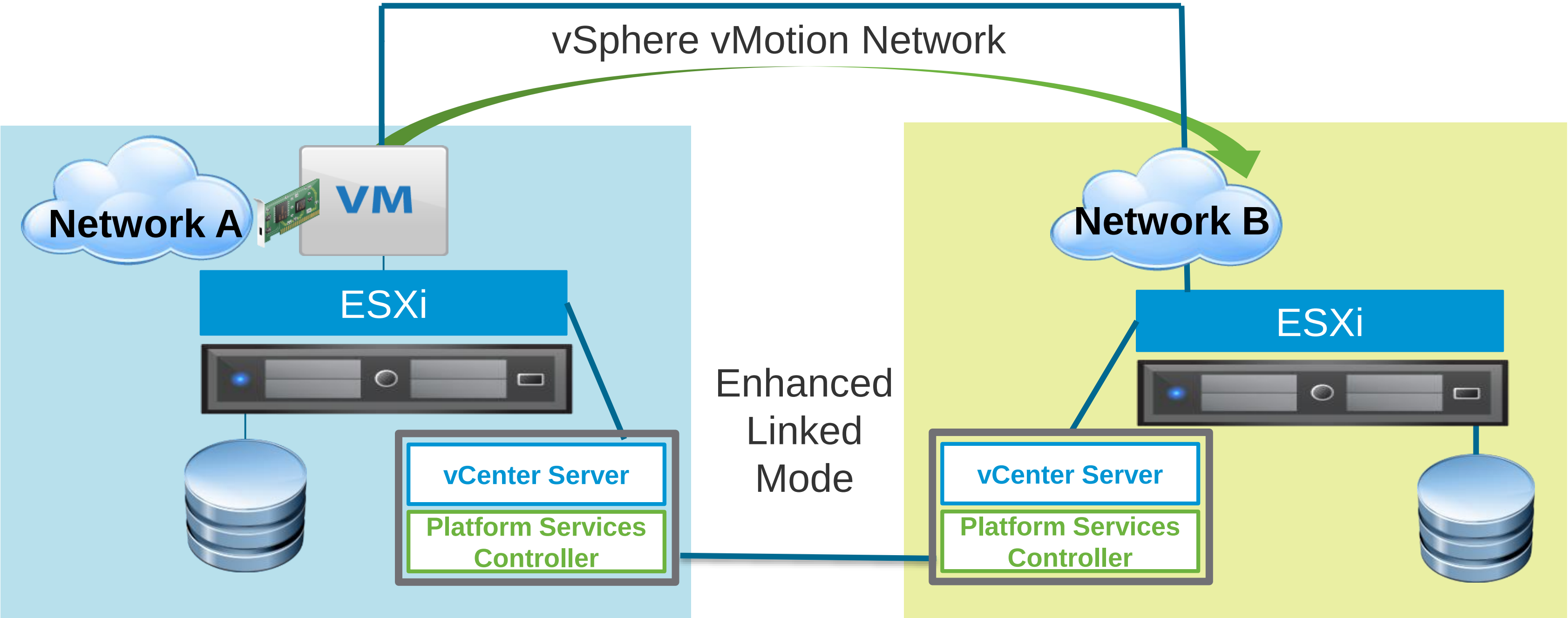
You can migrate virtual machines beyond storage accessibility boundaries and between hosts, within and across clusters, data centers, and vCenter Server instances.

Cross-vCenter migrations

vSphere vMotion can migrate virtual machines between linked vCenter Server systems.

Requirements:

- ESXi hosts and vCenter Server systems must be upgraded to vSphere 6.x.
- vCenter Server instances must be in Enhanced Linked Mode.
- Hosts must be time-synchronized.
- Both of the vCenter Server systems should be the same vCenter Server version.



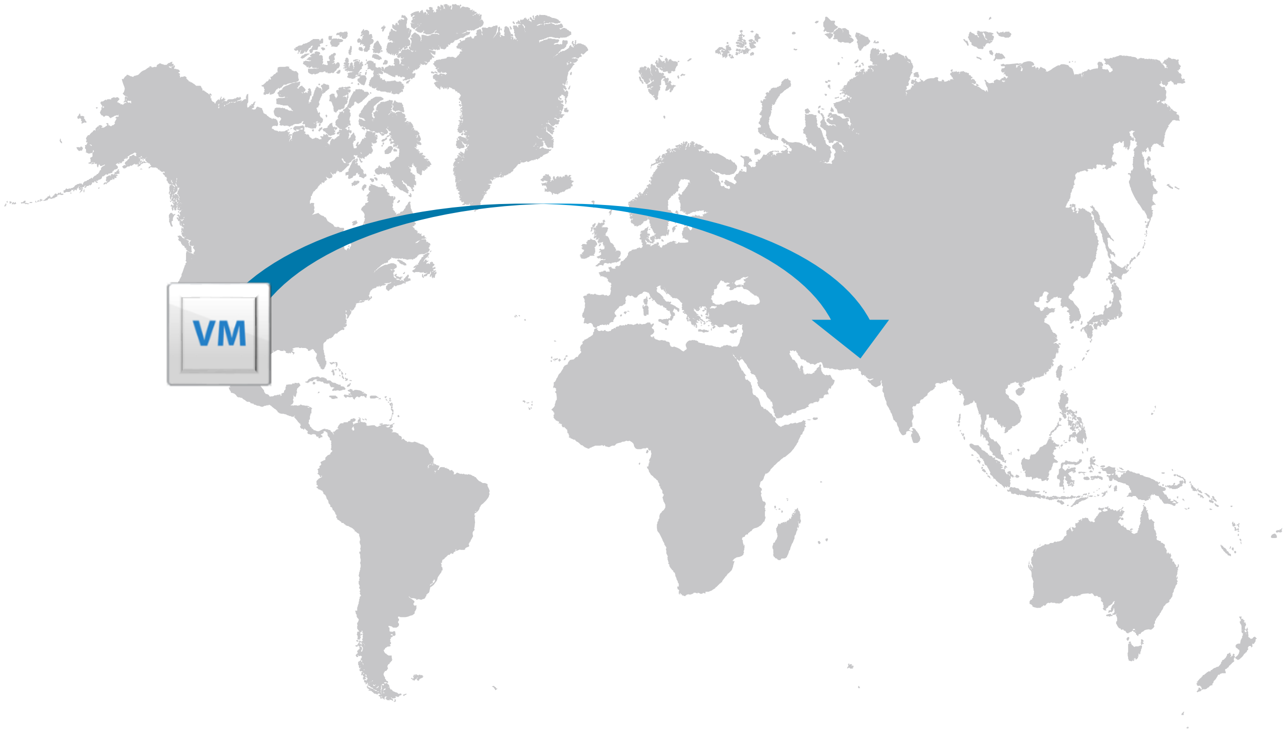
Long-Distance vSphere vMotion Migration

Long-distance vSphere vMotion migration is an extension of vSphere vMotion migration across vCenter Server instances.

This migration is targeted at environments where vCenter Server systems are spread across large geographic distances and where the latency across sites is high.

Use cases for long-distance vSphere vMotion migration:

- Permanent migrations
- Disaster avoidance
- VMware Site Recovery Manager™ and disaster avoidance testing
- Multisite load balancing
- Follow-the-Sun scenario support



Networking Prerequisite for Long-Distance vSphere vMotion Migration

vSphere vMotion migrations between vCenter Server instances must connect over layer 3 connections:

- Virtual machine network:
  - L2 connection.
  - Same virtual machine IP address available at destination.
- vSphere vMotion network:
  - L3 connection.
  - Secure (recommended if not using vSphere 6.5 or later encrypted vSphere vMotion).
  - 250 Mbps per vSphere vMotion operation.
  - Round-trip time between hosts can take up to 150 milliseconds.

Network Checks for Migrations Between vCenter Server Instances

vCenter Server performs several network compatibility checks to prevent the following configuration problems:

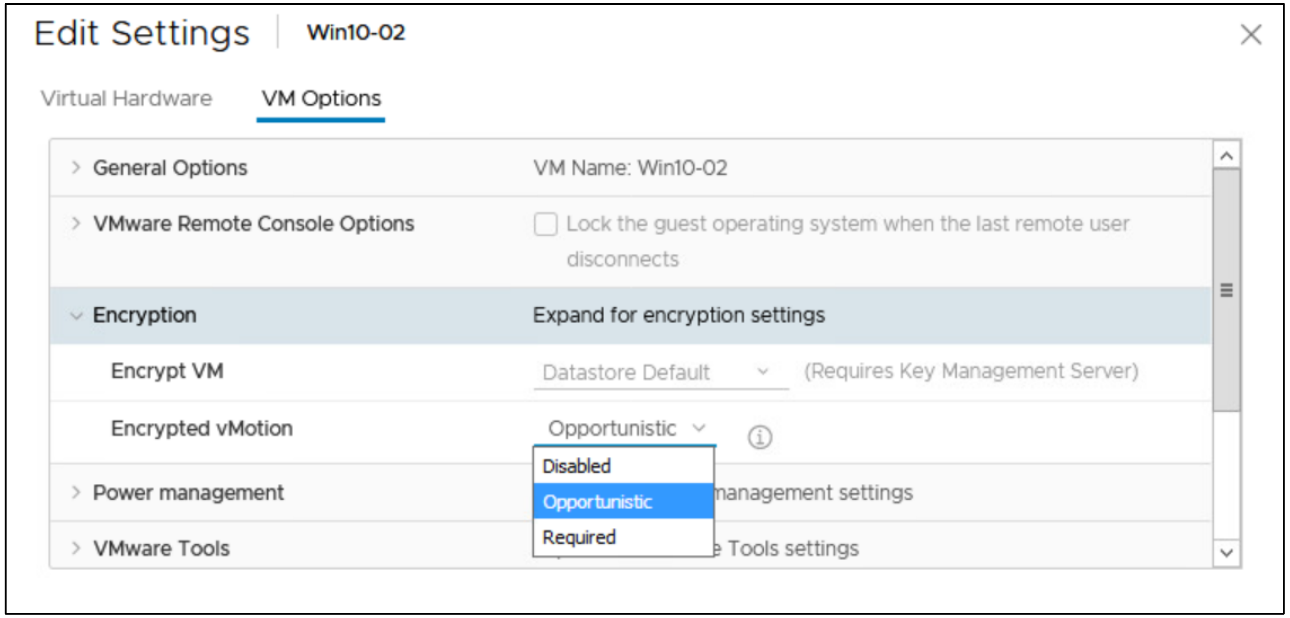
- MAC address incompatibility on the destination host
- vSphere vMotion migration from a distributed switch to a standard switch
- vSphere vMotion migration between distributed switches of different versions
- vSphere vMotion migration to an internal network, for example, a network without a physical NIC

Encrypted vSphere vMotion

vSphere vMotion always uses encryption when migrating encrypted virtual machines.

For virtual machines that are not encrypted, select one of the following encrypted vSphere vMotion options:

- **Disabled**.
- **Opportunistic:** Encrypted vSphere vMotion is used if the source and destination hosts support it.
- **Required:** If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion fails.



Edit Settings | Win10-02

General Options: VM Name: Win10-02

VMware Remote Console Options: □ Lock the guest operating system when the last remote user disconnects

Encryption: Expand for encryption settings

Encrypt VM: Datastore Default (Requires Key Management Server)

Encrypted vMotion: Opportunistic

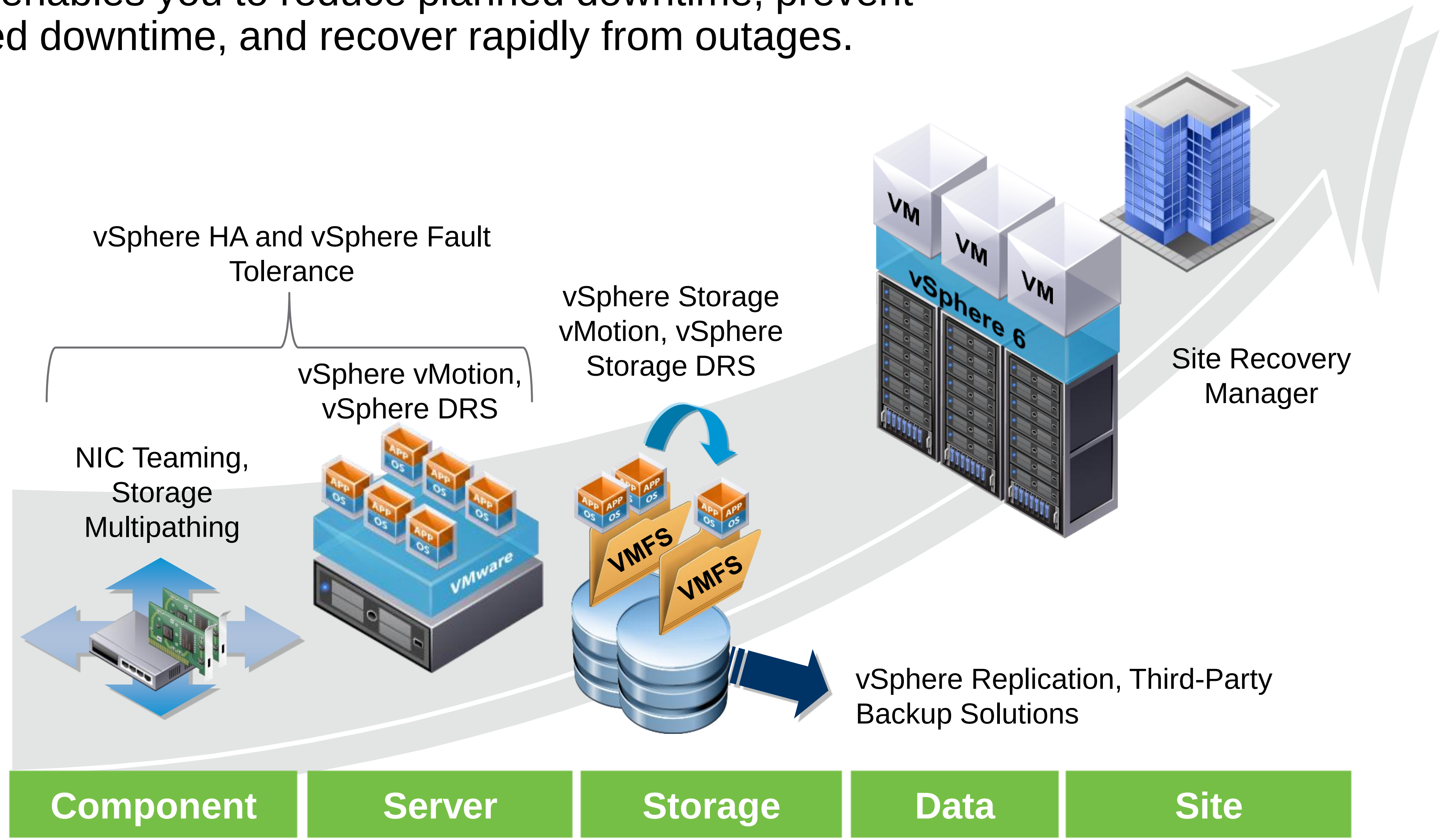
Power management: management settings

VMware Tools: Tools settings

vSphere HA, vSphere Fault Tolerance, and Protecting Data

Protection at Every Level

vSphere enables you to reduce planned downtime, prevent unplanned downtime, and recover rapidly from outages.



vSphere HA and vSphere Fault Tolerance

vSphere vMotion, vSphere DRS

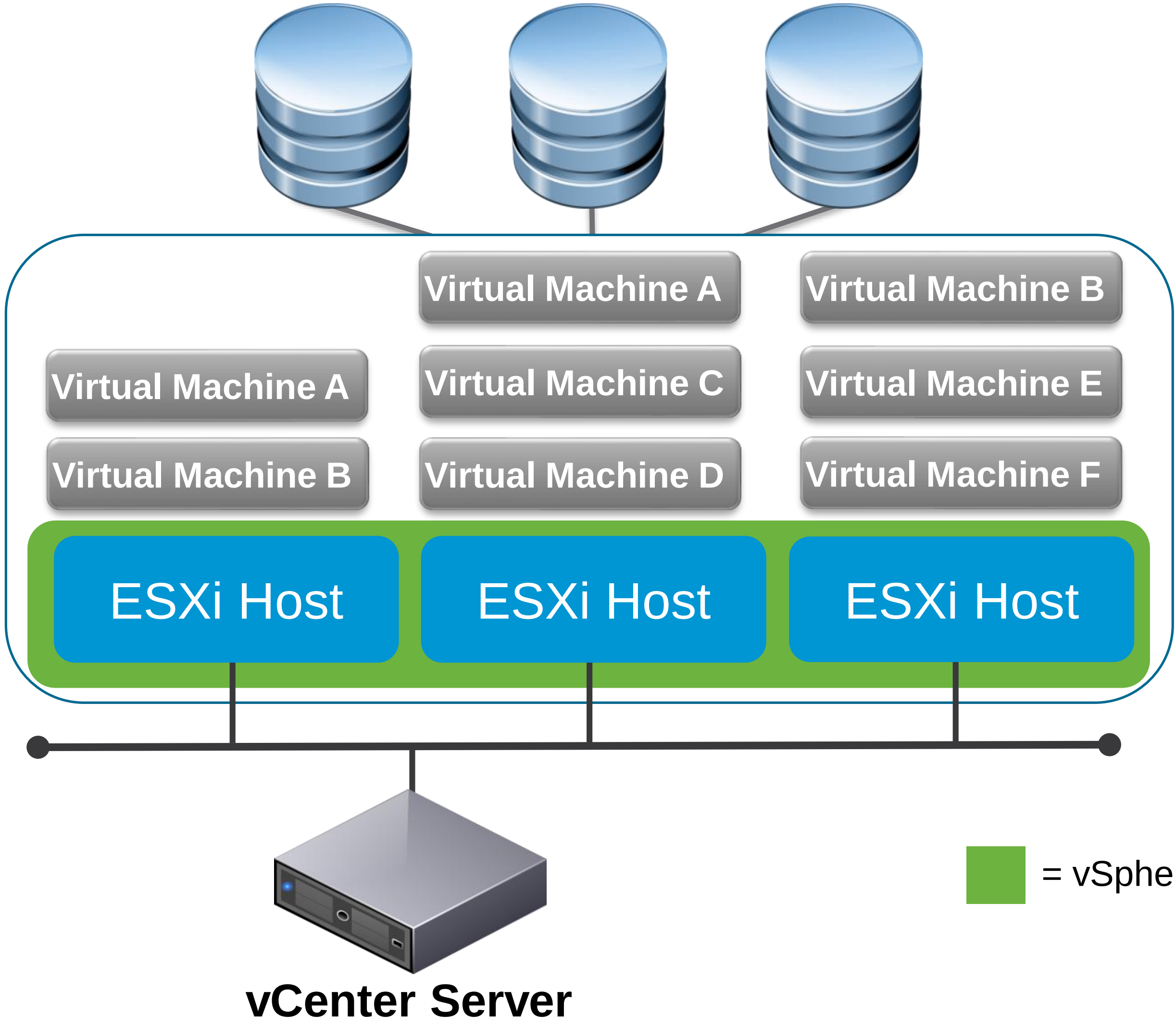
vSphere Storage vMotion, vSphere Storage DRS

NIC Teaming, Storage Multipathing

Site Recovery Manager

vSphere Replication, Third-Party Backup Solutions

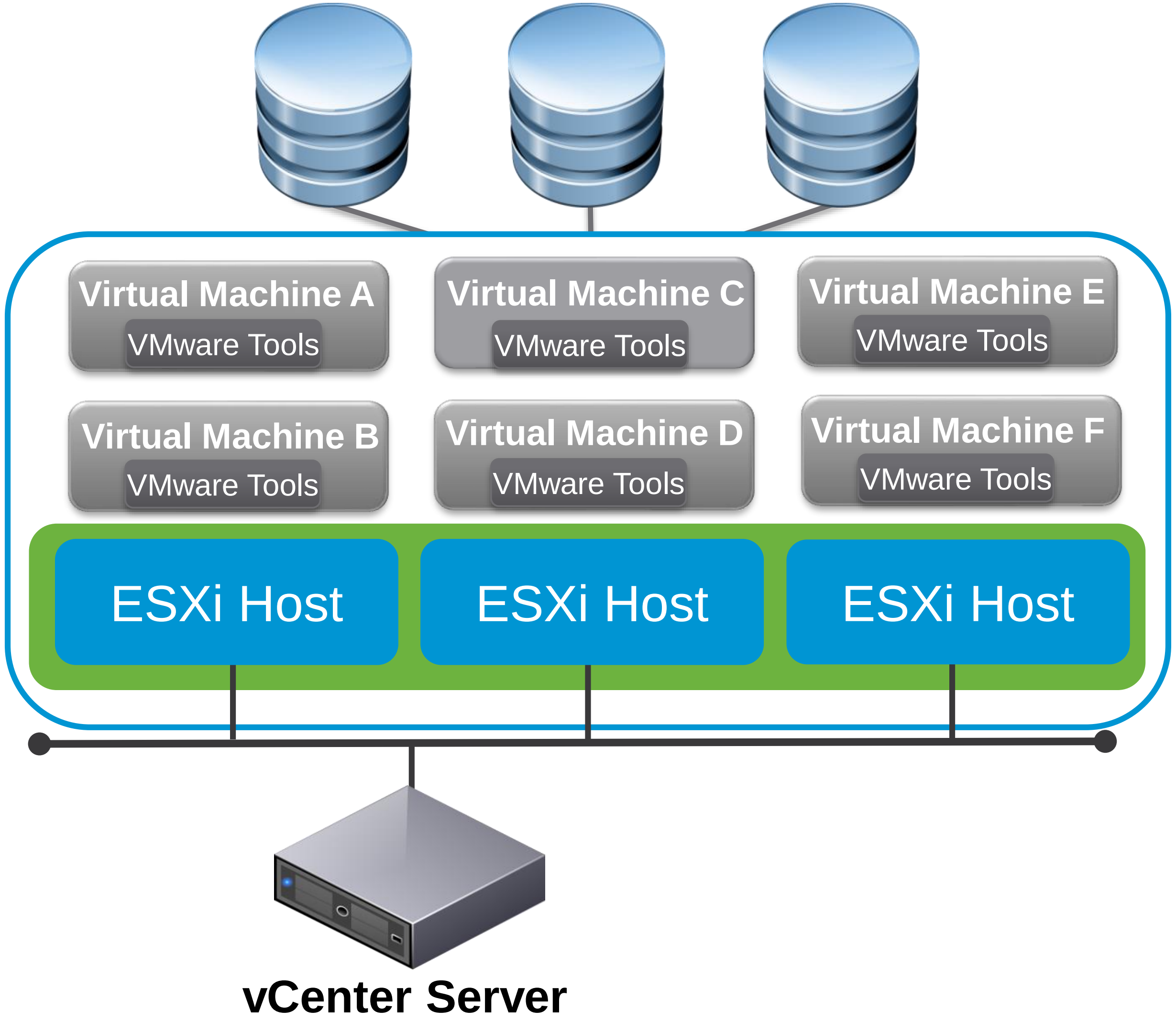
vSphere HA Scenario: ESXi Host Failure



When a host fails, vSphere HA restarts the impacted virtual machines on other hosts.

🟩 = vSphere HA Cluster

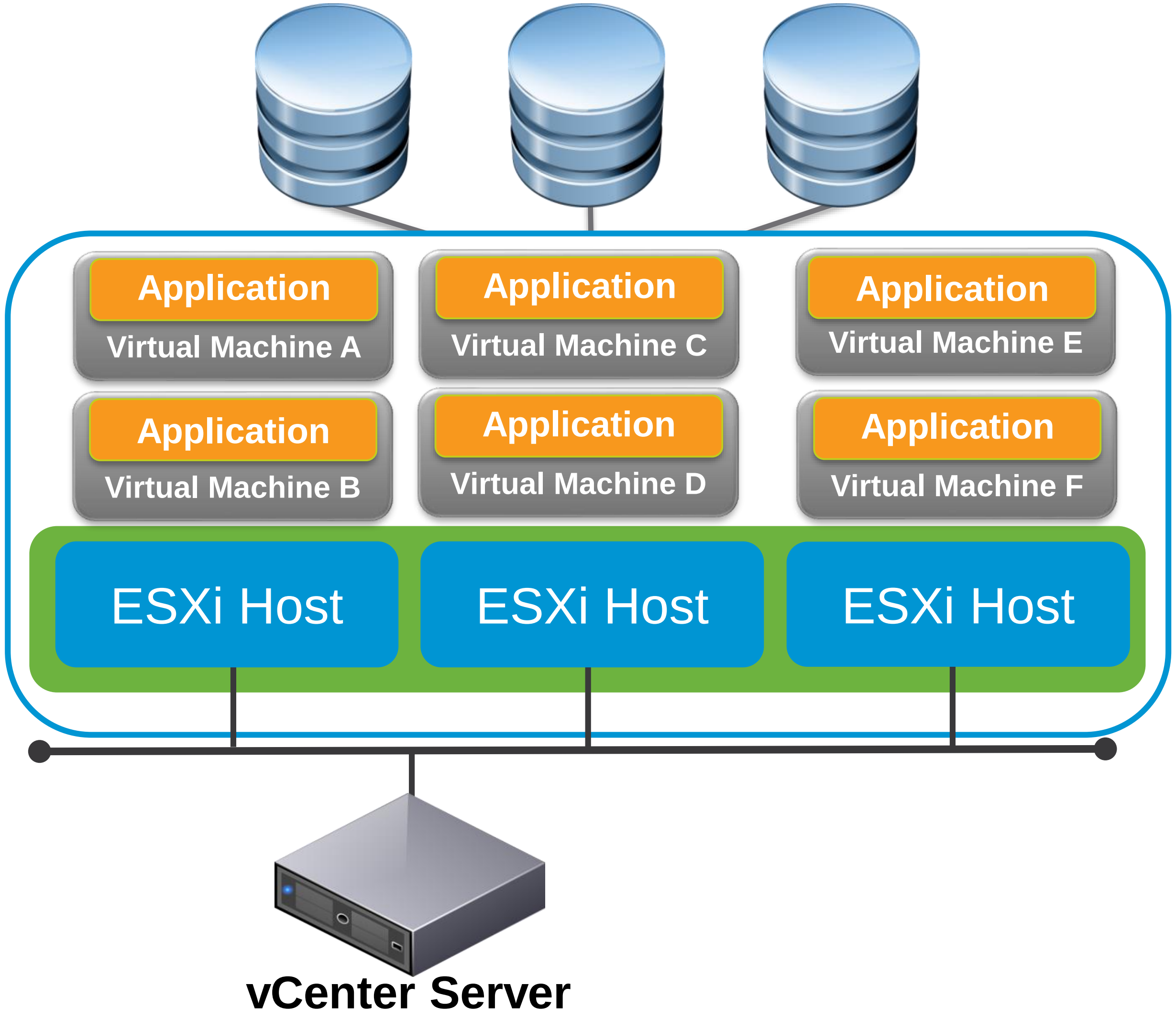
vSphere HA Scenario: Guest Operating System Failure



When a virtual machine stops sending heartbeats or the virtual machine process crashes (vmx), vSphere HA resets the virtual machine.

🟩 = vSphere HA Cluster

vSphere HA Scenario: Application Failure



When an application fails, vSphere HA restarts the impacted virtual machine on the same host.

VM Component Protection (VMCP) requires installation of VMware Tools.

🟩 **= vSphere HA Cluster**

Importance of Redundant Heartbeat Networks

In a vSphere HA cluster, heartbeats have the following characteristics:

- They are sent between the master host and the slave hosts.
- They are used to determine whether a master host or a slave host has failed.
- They are sent over a heartbeat network.

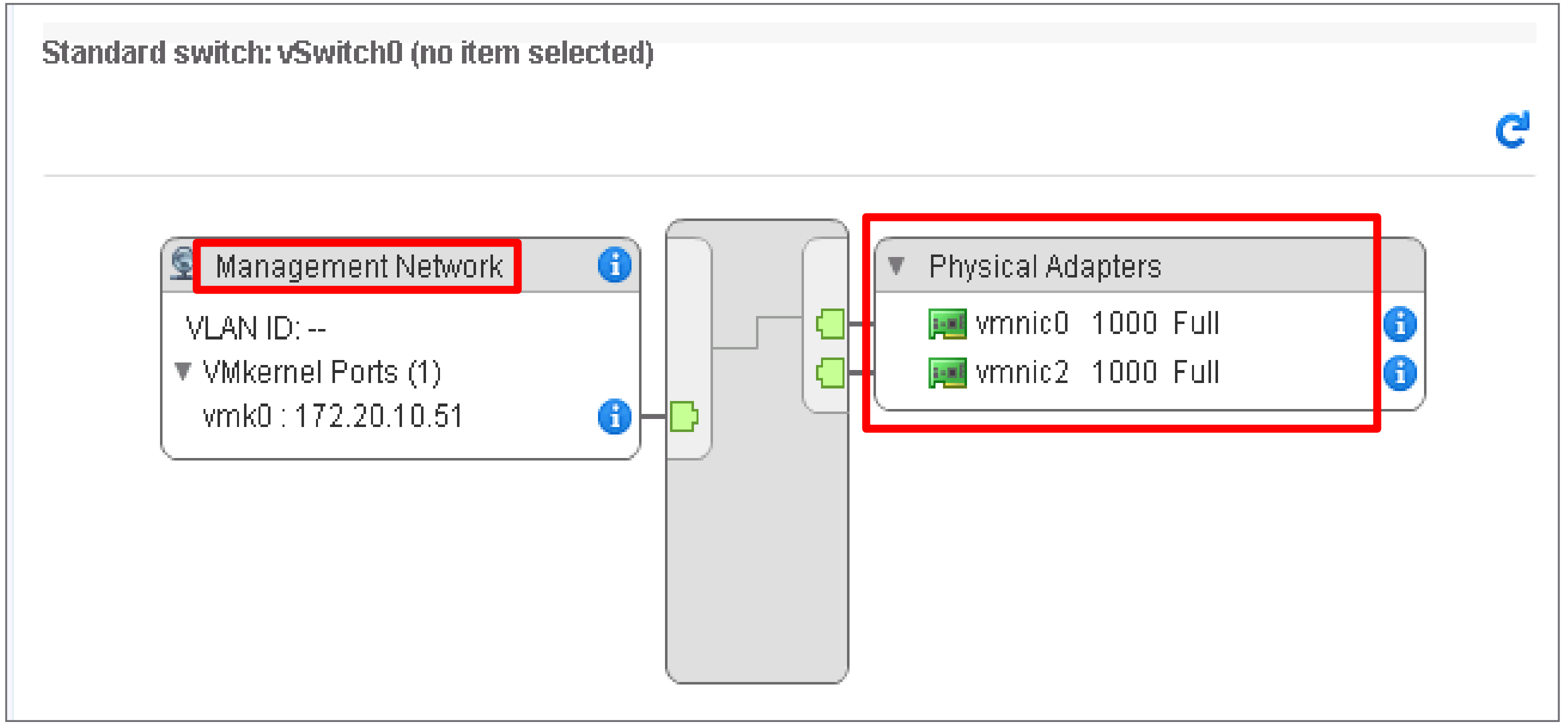
Redundant heartbeat networks ensure reliable failure detection and minimize the chance of host-isolation scenarios.

Heartbeat network implementation:

- Implemented by using a VMkernel port that is marked for management.
- Implemented by using a VMkernel port that is marked for vSAN traffic when vSAN is in use.

Redundancy Using NIC Teaming

You can use NIC teaming to create a redundant heartbeat network on ESXi hosts.



Standard switch: vSwitch0 (no item selected)

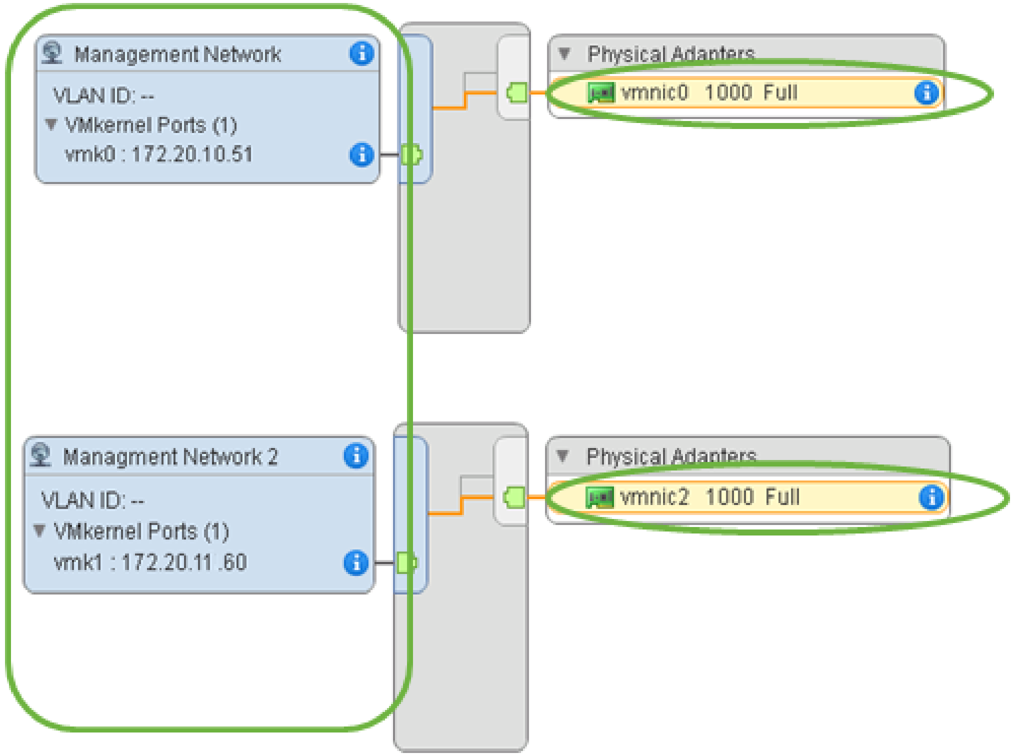
NIC Teaming on an ESXi Host

Redundancy Using Additional Networks

You can create redundancy by configuring more heartbeat networks.

On each ESXi host, create a second VMkernel port on a separate virtual switch with its own physical adapter.

Redundant management networking enables the reliable detection of failures and prevents isolation or partition conditions from occurring, because heartbeats can be sent over multiple networks.



Management Network
VLAN ID: --
▼ VMkernel Ports (1)
vmk0 : 172.20.10.51

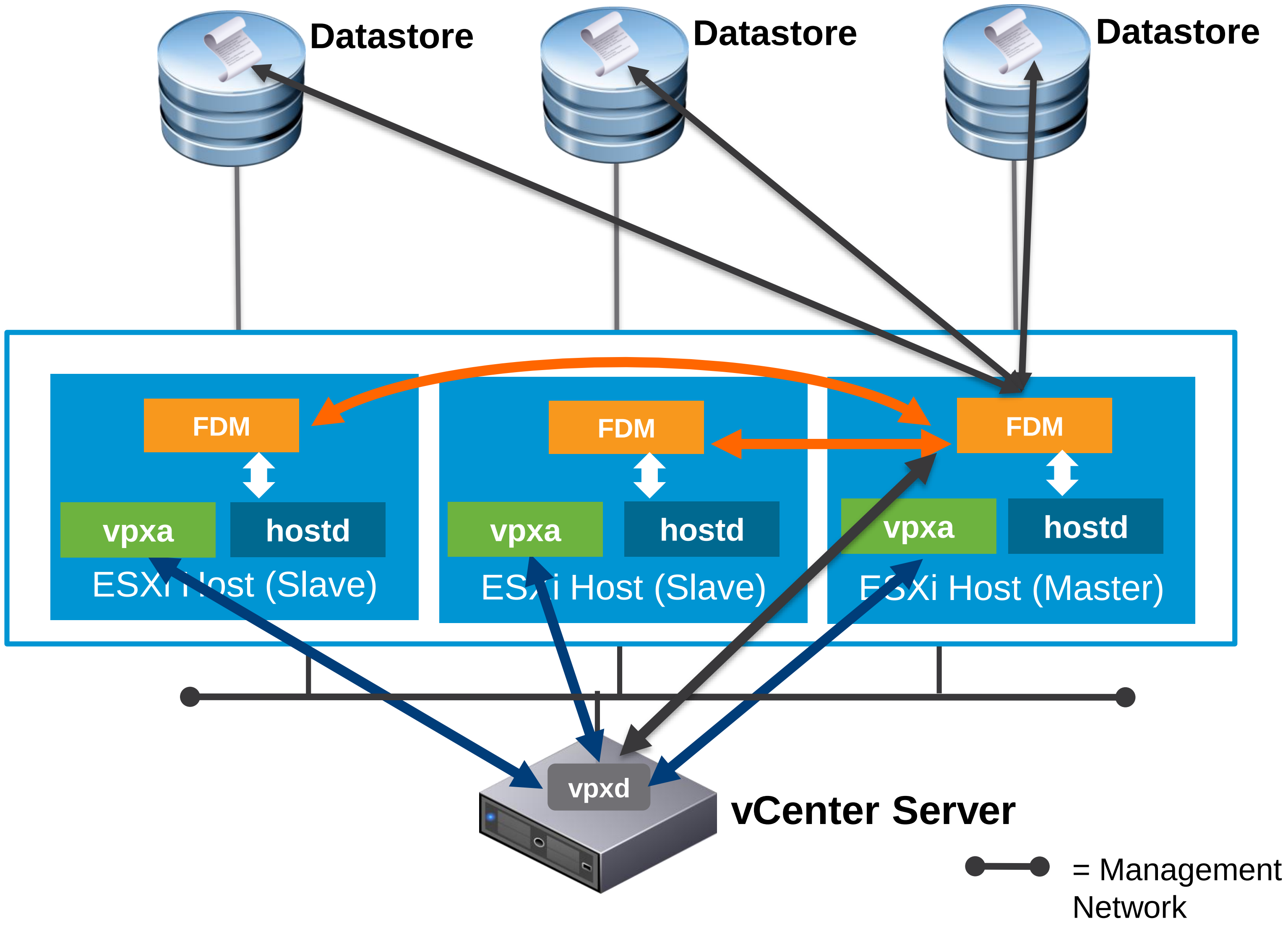
▼ Physical Adapters
vmnic0 1000 Full

Managment Network 2
VLAN ID: --
▼ VMkernel Ports (1)
vmk1 : 172.20.11 .60

▼ Physical Adapters
vmnic2 1000 Full

vSphere HA Architecture: Agent Communication

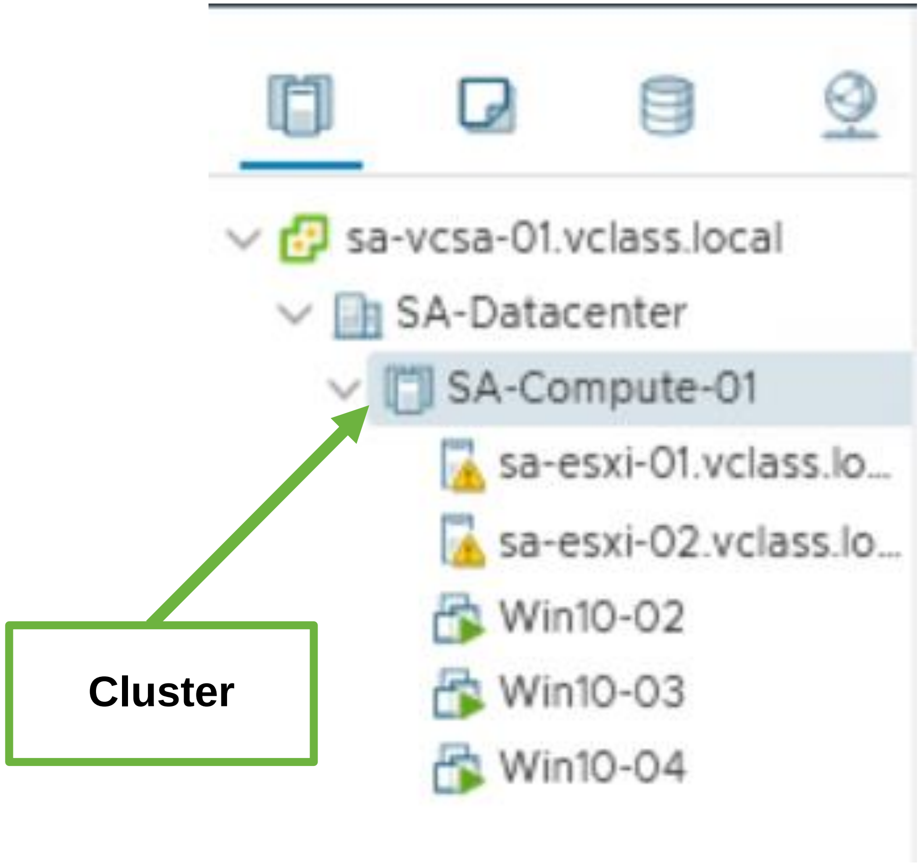
To configure high availability, ESXi hosts are grouped into an object called a cluster.



About Clusters

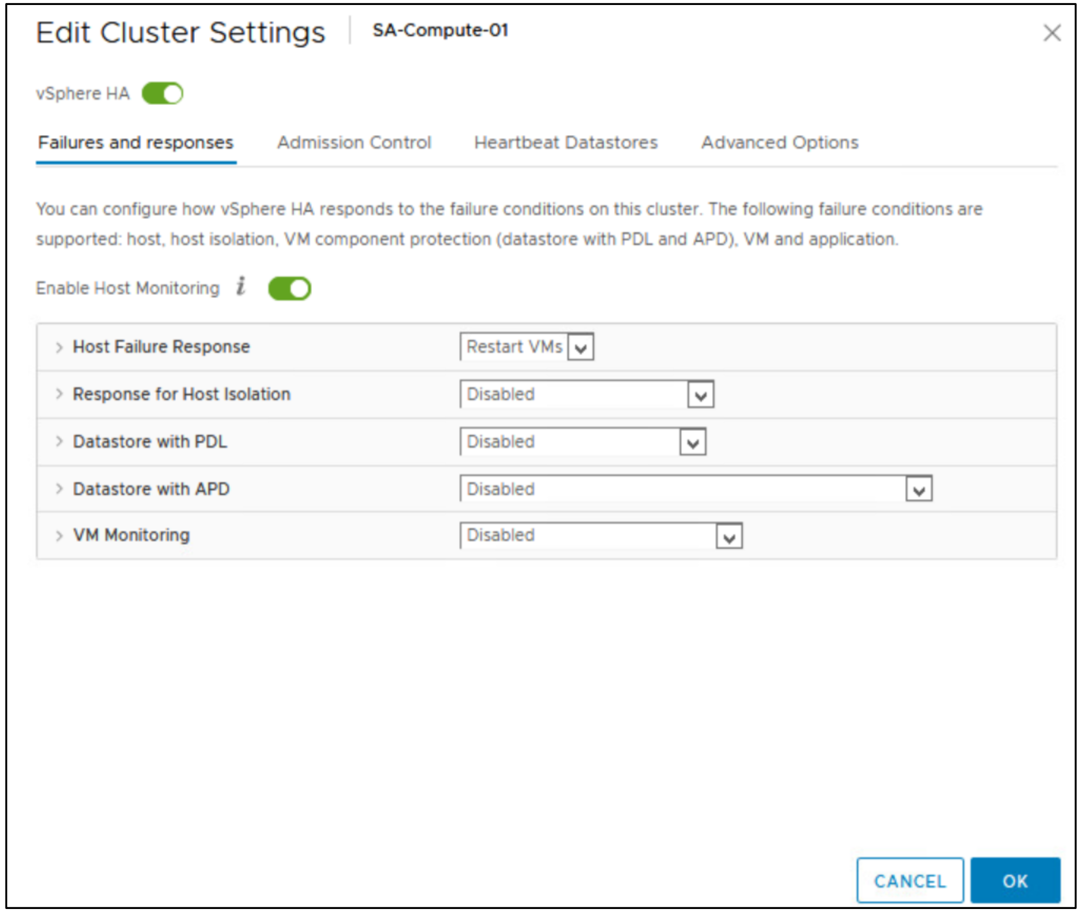
A cluster is used in vSphere to share physical resources between a group of ESXi hosts. vCenter Server manages cluster resources as a single pool of resources.

Features such as vSphere HA, vSphere DRS, and vSAN can be enabled in a cluster.



Configuring vSphere HA Settings

When you create or configure a vSphere HA cluster, you must configure settings that determine how the feature works.



vSphere HA: On

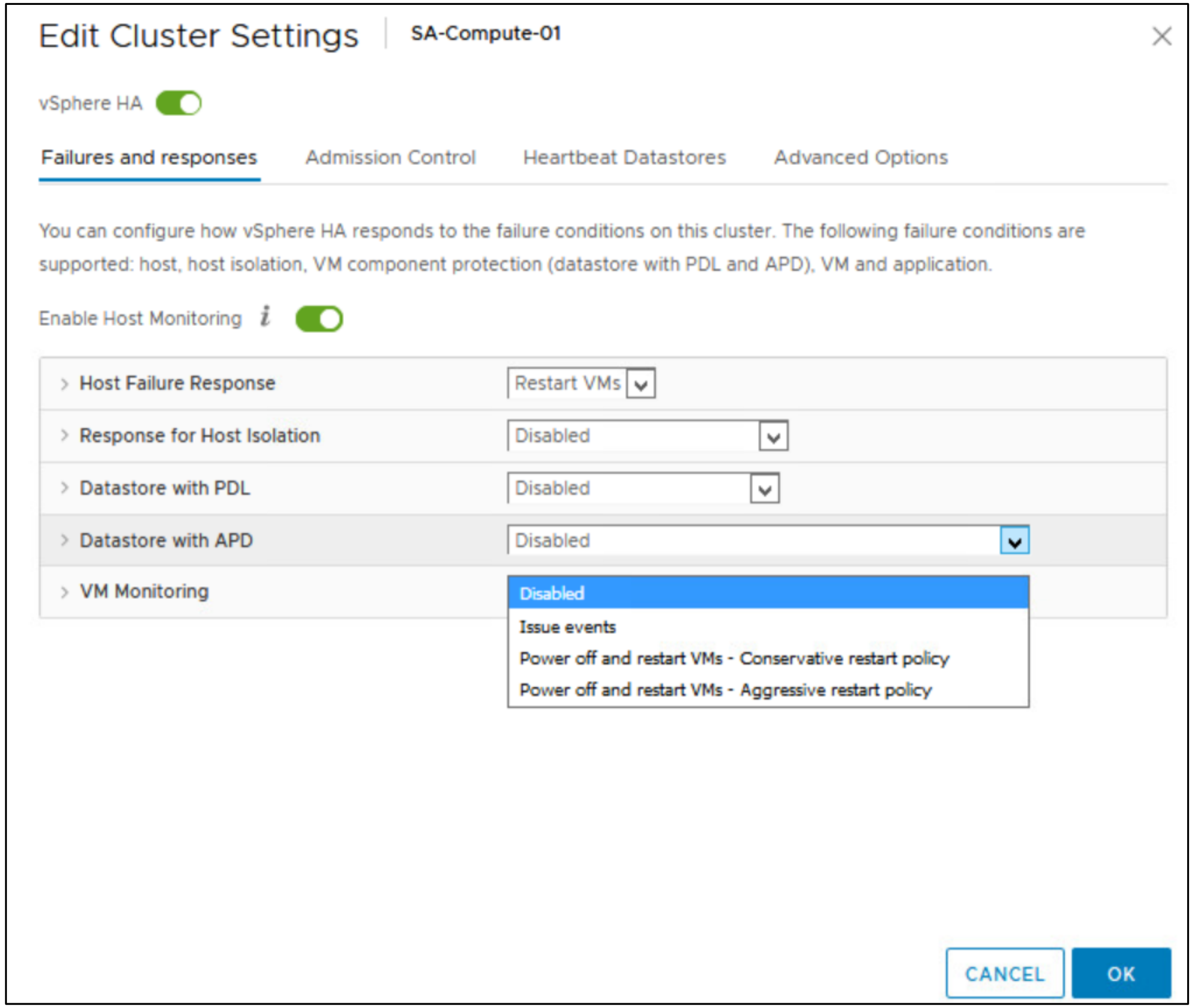
You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring: On

› Host Failure Response	Restart VMs
› Response for Host Isolation	Disabled
› Datastore with PDL	Disabled
› Datastore with APD	Disabled
› VM Monitoring	Disabled

vSphere HA Settings: Failure and Responses

You use the Failures and responses pane to configure a cluster's response if a failure occurs.



Edit Cluster Settings | SA-Compute-01

vSphere HA

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

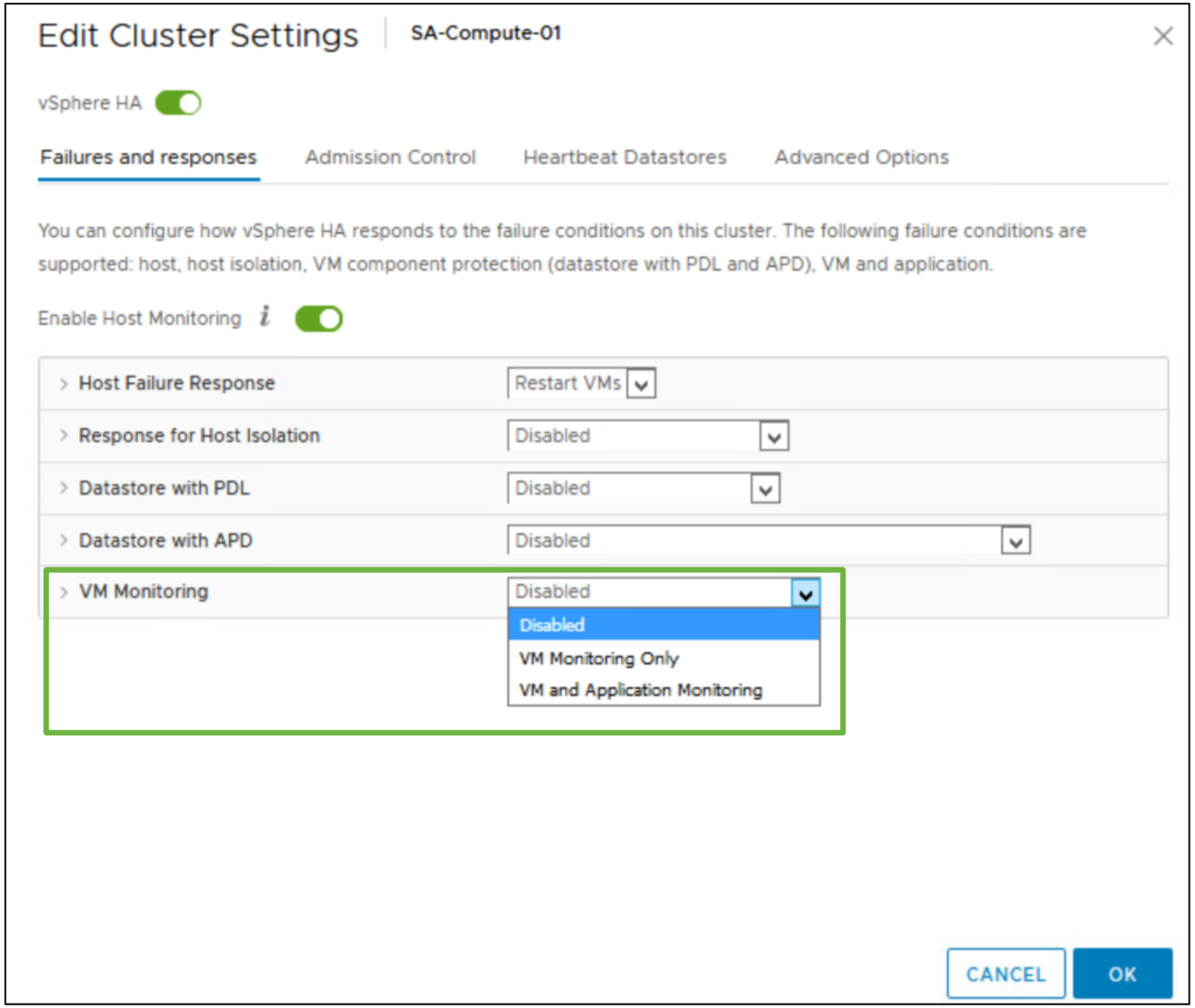
Enable Host Monitoring

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	

Disabled
Issue events
Power off and restart VMs - Conservative restart policy
Power off and restart VMs - Aggressive restart policy
CANCEL
OK

vSphere HA Settings: Virtual Machine Monitoring

You use VM Monitoring settings to control the monitoring of virtual machines.



Edit Cluster Settings | SA-Compute-01

vSphere HA: on

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

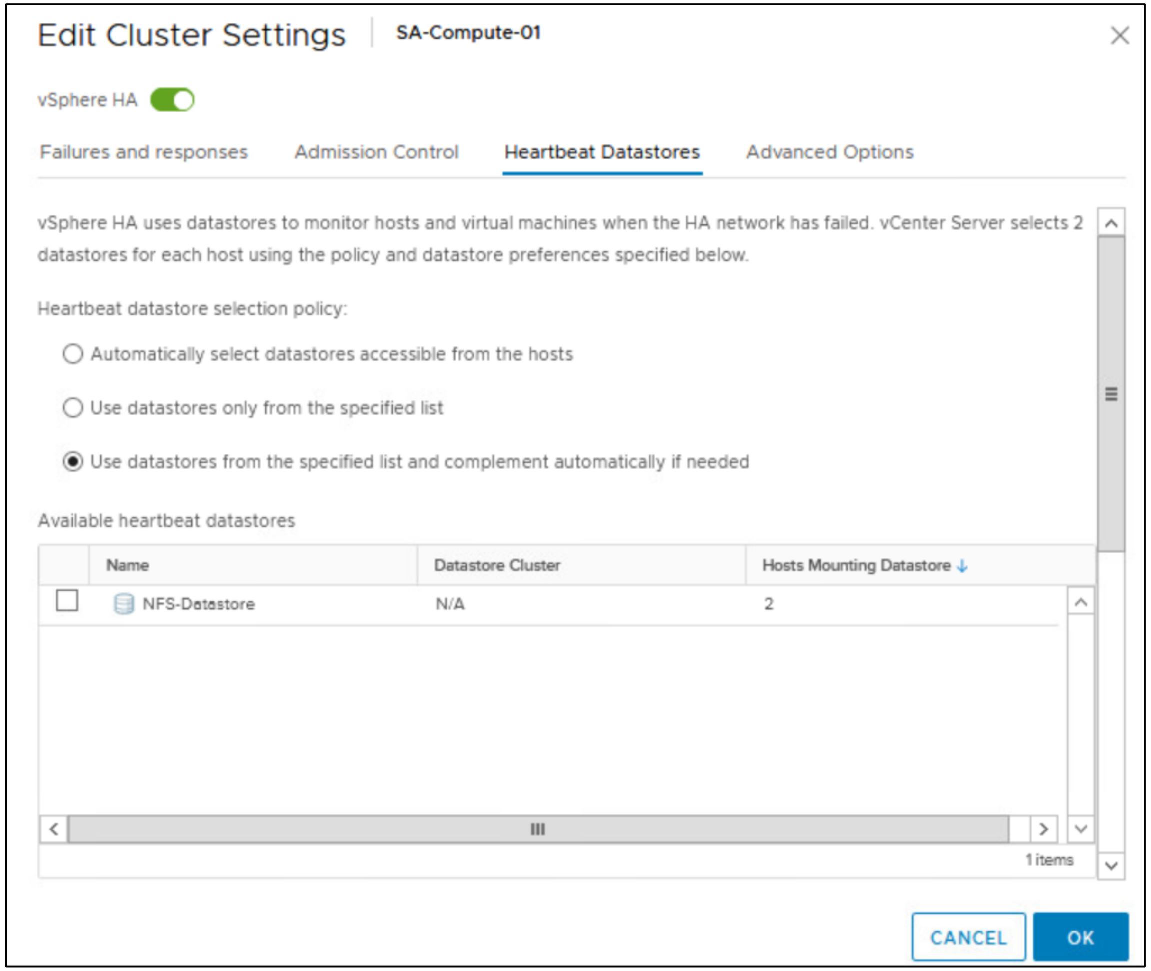
You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring: on

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	Disabled

vSphere HA Settings: Heartbeat Datastores

A heartbeat file is created on the selected datastores and is used if the management network fails.



Edit Cluster Settings | SA-Compute-01

vSphere HA ●

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 2 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

○ Automatically select datastores accessible from the hosts

○ Use datastores only from the specified list

● Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

	Name	Datastore Cluster	Hosts Mounting Datastore ↓
□	NFS-Datastore	N/A	2

1 items