
Section 4
Installing, Configuring, and Setup

Objective 4.1
Identify Virtual Switch configuration options.

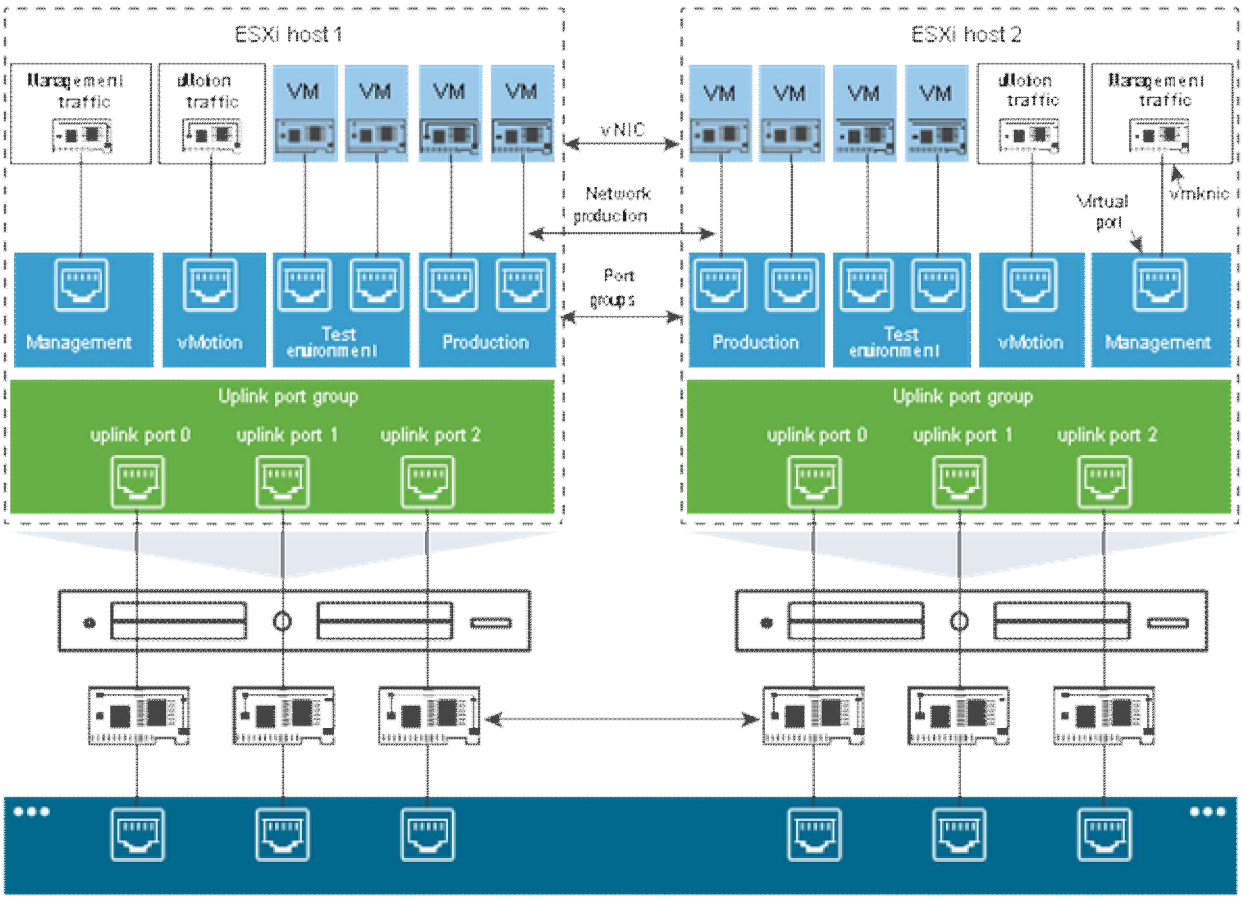
vSphere Standard Switches

You can create abstracted network devices called vSphere Standard Switches. You use standard switches to provide network connectivity to hosts and virtual machines. A standard switch can bridge traffic internally between virtual machines in the same VLAN and link to external networks.

Standard Switch Overview

To provide network connectivity to hosts and virtual machines, you connect the physical NICs of the hosts to uplink ports on the standard switch. Virtual machines have network adapters (vNICs) that you connect to port groups on the standard switch. Every port group can use one or more physical NICs to handle their network traffic. If a port group does not have a physical NIC connected to it, virtual machines on the same port group can only communicate with each other but not with the external network.

Figure 2-1. vSphere Standard Switch architecture



A vSphere Standard Switch is very similar to a physical Ethernet switch. Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port. Each logical port on the standard switch is a member of a single port

group. For information about maximum allowed ports and port groups, see the *Configuration Maximums* documentation.

Standard Port Groups

Each port group on a standard switch is identified by a network label, which must be unique to the current host. You can use network labels to make the networking configuration of virtual machines portable across hosts. You should give the same label to the port groups in a data center that use physical NICs connected to one broadcast domain on the physical network. Conversely, if two port groups are connected to physical NICs on different broadcast domains, the port groups should have distinct labels.

For example, you can create *Production* and *Test environment* port groups as virtual machine networks on the hosts that share the same broadcast domain on the physical network.

A VLAN ID, which restricts port group traffic to a logical Ethernet segment within the physical network, is optional. For port groups to receive the traffic that the same host sees, but from more than one VLAN, the VLAN ID must be set to VGT (VLAN 4095).

Number of Standard Ports

To ensure efficient use of host resources on ESXi hosts, the number of ports of standard switches are dynamically scaled up and down. A standard switch on such a host can expand up to the maximum number of ports supported on the host.

vSphere Networking Update 1 - VMware vSphere 7.0, page 17

vSphere Standard Switch Properties

vSphere Standard Switch settings control switch-wide defaults for ports, which can be overridden by port group settings for each standard switch. You can edit standard switch properties, such as the uplink configuration and the number of available ports.

Number of Ports on ESXi Hosts

To ensure efficient use of host resources on ESXi hosts, the ports of virtual switches are dynamically scaled up and down. A switch on such a host can expand up to the maximum number of ports supported on the host. The port limit is determined based on the maximum number of virtual machines that the host can handle.

Change the Size of the MTU on a vSphere Standard Switch

Change the size of the maximum transmission unit (MTU) on a vSphere Standard Switch to improve the networking efficiency by increasing the amount of payload data transmitted with a single packet, that is, enabling jumbo frames.

Procedure

1 In the vSphere Client, navigate to the host.

2 On the Configure tab, expand Networking and select Virtual Switches.

3 Select a standard switch from the table and click Edit settings.

4 Change the MTU (Bytes) value for the standard switch.

   You can enable jumbo frames by setting an MTU value greater than 1500. You cannot set an MTU size greater than 9000 bytes.

5 Click OK.

Change the Speed of a Physical Adapter

A physical adapter can become a bottleneck for network traffic if the adapter speed does not match application requirements. You can change the connection speed and duplex of a physical adapter to transfer data in compliance with the traffic rate.

If the physical adapter supports SR-IOV, you can enable it and configure the number of virtual functions to use for virtual machine networking.

Procedure

1 In the vSphere Client, navigate to a host.

2 On the Configure tab, expand Networking and select Physical adapters.

   The physical network adapters of the host appear in a table that contains details for each physical network adapter.

3 Select the physical network adapter from the list and click the Edit adapter settings icon.

4 Select speed and duplex mode of the physical network adapter from the drop-down menu.

5 Click OK.

Add and Team Physical Adapters in a vSphere Standard Switch

Assign a physical adapter to a standard switch to provide connectivity to virtual machines and VMkernel adapters on the host. You can form a team of NICs to distribute traffic load and to configure failover.

NIC teaming combines multiple network connections to increase throughput and provide redundancy should a link fail. To create a team, you associate multiple physical adapters to a single vSphere Standard Switch.

Procedure

1 In the vSphere Client, navigate to the host.

2 On the Configure tab, expand Networking and select Virtual Switches.

3 Select the standard switch you want to add a physical adapter to.

4 Click Manage Physical Adapters.

5 Add one or more available physical network adapters to the switch.

   a Click Add adapters, select one or more network adapters from the list and click OK.

      The selected adapters appear in the failover group list under the Assigned Adapters list.

   b (Optional) Use the up and down arrows to change the position of an adapter in the failover groups.

      The failover group determines the role of the adapter for exchanging data with the external network, that is, active, standby or unused. By default, the adapters are added as active to the standard switch.

6 Click OK to apply the physical adapter configuration.

View the Topology Diagram of a vSphere Standard Switch

You can examine the structure and components of a vSphere Standard Switch by using its topology diagram.

The topology diagram of a standard switch provides a visual representation of the adapters and port groups connected to the switch.
From the diagram you can edit the settings of a selected port group and of a selected adapter.

Procedure

1 In the vSphere Client, navigate to the host.

2 On the Configure tab, expand Networking and select Virtual Switches.

3 Select the standard switch from the list.

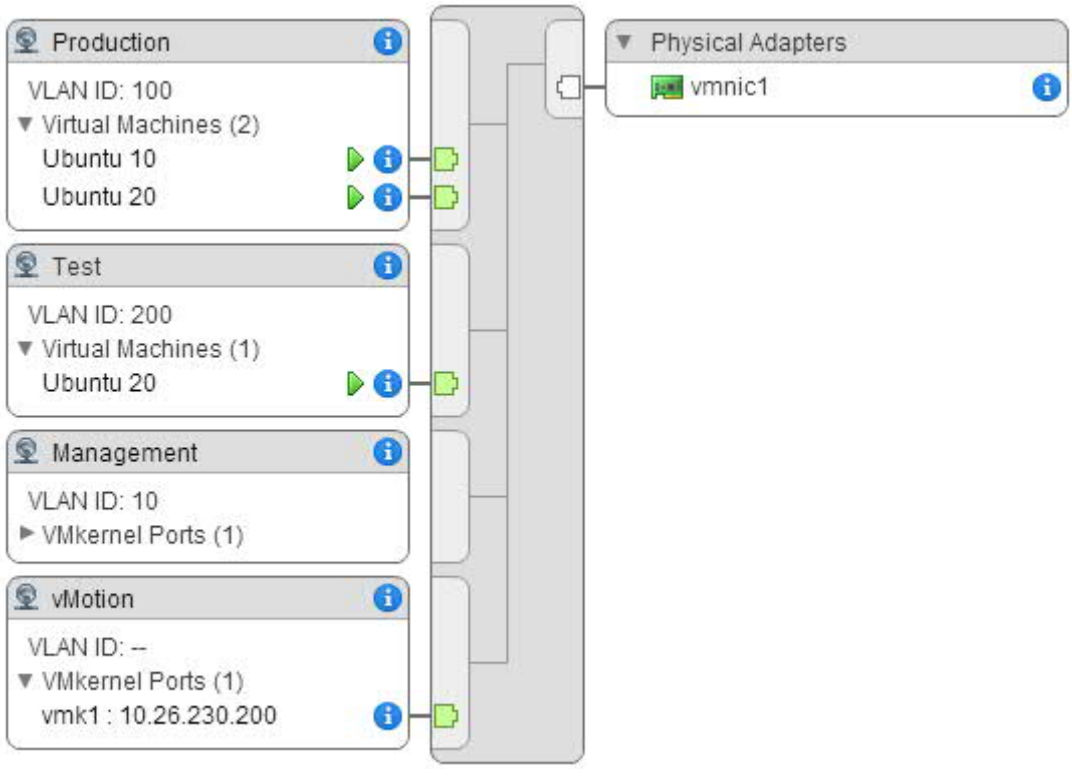
Results

The diagram appears under the list of virtual switches on the host.

Example: Diagram of a Standard Switch That Connects the VMkernel and Virtual Machines to the Network

In your virtual environment, a vSphere Standard Switch handles VMkernel adapters for vSphere vMotion and for the management network, and virtual machines grouped. You can use the central topology diagram to examine whether a virtual machine or VMkernel adapter is connected to the external network and to identify the physical adapter that carries the data.

Figure 2-2. Topology Diagram of a Standard Switch That Connects the VMkernel and Virtual Machines to the Network

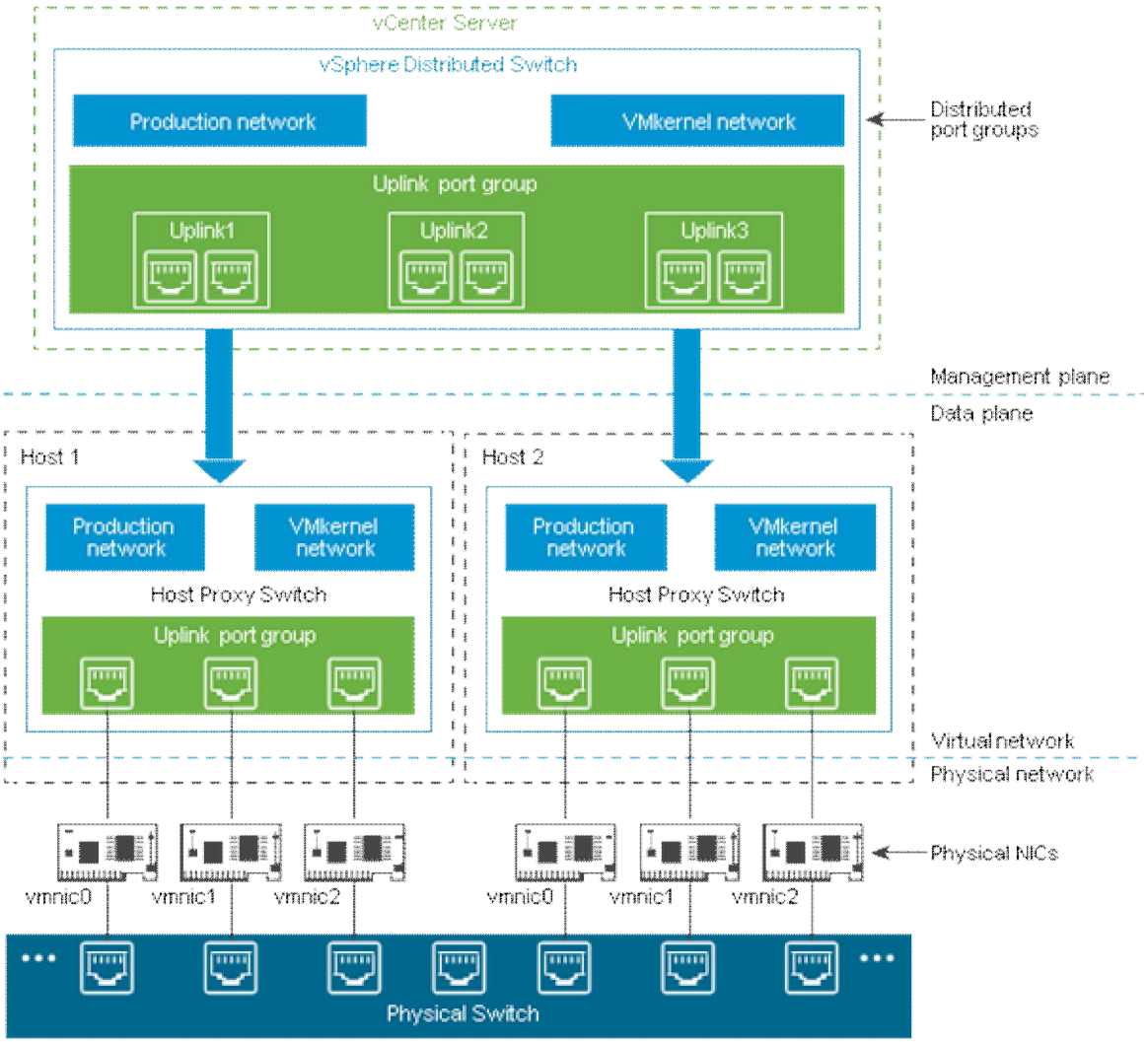


vSphere Networking Update 1 - VMware vSphere 7.0, page 23

vSphere Distributed Switch Architecture

A vSphere Distributed Switch provides centralized management and monitoring of the networking configuration of all hosts that are associated with the switch. You set up a distributed switch on a vCenter Server system, and its settings are propagated to all hosts that are associated with the switch.

Figure 3-1. vSphere Distributed Switch Architecture



A network switch in vSphere consists of two logical sections that are the data plane and the management plane. The data plane implements the packet switching, filtering, tagging, and so on. The management plane is the control structure that you use to configure the data plane functionality. A vSphere Standard Switch contains both data and management planes, and you configure and maintain each standard switch individually.

A vSphere Distributed Switch separates the data plane and the management plane. The management functionality of the distributed switch resides on the vCenter Server system that lets you administer the networking configuration of your environment on a data center level. The data plane remains locally on every host that is associated with the distributed switch. The data plane section of the distributed switch is called a host proxy switch. The networking configuration that you create on vCenter Server (the management plane) is automatically pushed down to all host proxy switches (the data plane).

The vSphere Distributed Switch introduces two abstractions that you use to create consistent networking configuration for physical NICs, virtual machines, and VMkernel services.

Uplink port group

An uplink port group or dvuplink port group is defined during the creation of the distributed switch and can have one or more uplinks. An uplink is a template that you use to configure physical connections of hosts as well as failover and load balancing policies. You map physical NICs of hosts to uplinks on the distributed switch. At the host level, each physical NIC is connected to an uplink port with a particular ID. You set failover and load balancing policies over uplinks and the policies are automatically propagated to the host proxy switches, or the data plane. In this way you can apply consistent failover and load balancing configuration for the physical NICs of all hosts that are associated with the distributed switch.

Distributed port group

Distributed port groups provide network connectivity to virtual machines and accommodate VMkernel traffic. You identify each distributed port group by using a network label, which must be unique to the current data center. You configure NIC teaming, failover, load balancing, VLAN, security, traffic shaping , and other policies on distributed port groups. The virtual ports that are connected to a distributed port group share the same properties that are configured to the distributed port group. As with uplink port groups, the configuration that you set on distributed port groups on vCenter Server (the management plane) is automatically propagated to all hosts on the distributed switch through their host proxy switches (the data plane). In this way you can configure a group of virtual machines to share the same networking configuration by associating the virtual machines to the same distributed port group.

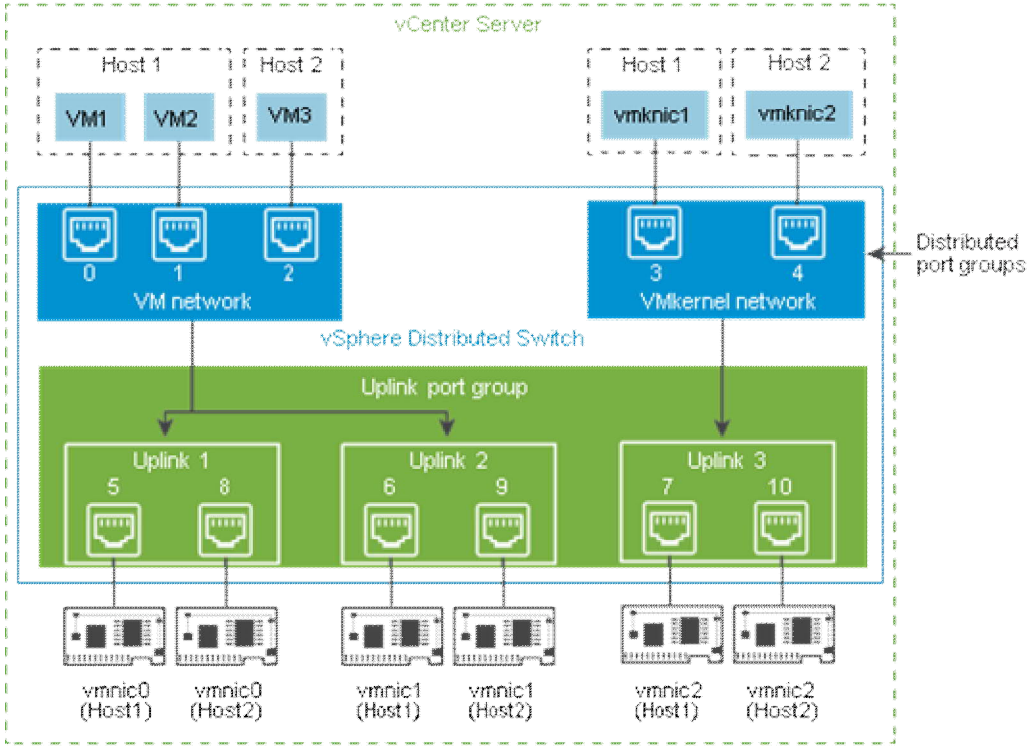
For example, suppose that you create a vSphere Distributed Switch on your data center and associate two hosts with it. You configure three uplinks to the uplink port group and connect a physical NIC from each host to an uplink. In this way, each uplink has two physical NICs from each host mapped to it, for example Uplink 1 is configured with vmnic0 from Host 1 and Host 2. Next you create the Production and the VMkernel network distributed port groups for virtual machine networking and VMkernel services. Respectively, a representation of the Production and the VMkernel network port groups is also created on Host 1 and Host 2. All policies that you set to the Production and the VMkernel network port groups are propagated to their representations on Host 1 and Host 2.

To ensure efficient use of host resources, the number of distributed ports of proxy switches is dynamically scaled up and down. A proxy switch on such a host can expand up to the maximum number of ports supported on the host. The port limit is determined based on the maximum number of virtual machines that the host can handle.

vSphere Distributed Switch Data Flow

The data flow from the virtual machines and VMkernel adapters down to the physical network depends on the NIC teaming and load balancing policies that are set to the distributed port groups. The data flow also depends on the port allocation on the distributed switch.

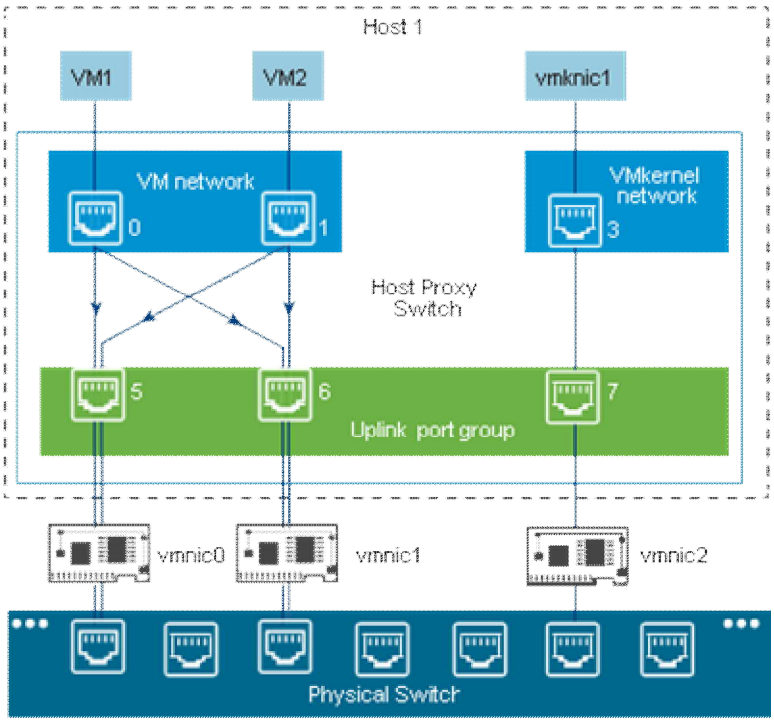
Figure 3-2. NIC Teaming and Port Allocation on a vSphere Distributed Switch



For example, suppose that you create the VM network and the VMkernel network distributed port groups, respectively with 3 and 2 distributed ports. The distributed switch allocates ports with IDs from 0 to 4 in the order that you create the distributed port groups. Next, you associate Host 1 and Host 2 with the distributed switch. The distributed switch allocates ports for every physical NIC on the hosts, as the numbering of the ports continues from 5 in the order that you add the hosts. To provide network connectivity on each host, you map vmnic0 to Uplink 1, vmnic1 to Uplink 2, and vmnic2 to Uplink 3.

To provide connectivity to virtual machines and to accommodate VMkernel traffic, you configure teaming and failover to the VM network and to the VMkernel network port groups. Uplink 1 and Uplink 2 handle the traffic for the VM network port group, and Uplink 3 handles the traffic for the VMkernel network port group.

Figure 3-3. Packet Flow on the Host Proxy Switch



On the host side, the packet flow from virtual machines and VMkernel services passes through particular ports to reach the physical network. For example, a packet sent from VM1 on Host 1 first reaches port 0 on the VM network distributed port group. Because Uplink 1 and Uplink 2 handle the traffic for the VM network port group, the packet can continue from uplink port 5 or uplink port 6 . If the packet goes through uplink port 5, it continues to vmnic0, and if the packet goes to uplink port 6, it continues to vmnic1.

vSphere Networking Update 1 - VMware vSphere 7.0, page 27

Edit General and Advanced vSphere Distributed Switch Settings

General settings for a vSphere Distributed Switch include the switch name and number of uplinks. Advanced settings for a distributed switch include Cisco Discovery Protocol and the maximum MTU for the switch.

Procedure

1 In the vSphere Client Home page, click Networking and select the distributed switch.

2 On the Configure tab, expand Settings and select Properties.

3 Click Edit.

4 Click General to edit the vSphere Distributed Switch settings.

Option	Description
Name	Enter the name for the distributed switch.
Number of uplinks	Select the number of uplink ports for the distributed switch. Click Edit uplink names to change the names of the uplinks.
Network I/O Control	Use the drop-down menu to enable or disable Network I/O control.

Description	Add or modify a description of the distributed switch settings.

5 Click Advanced to edit the vSphere Distributed Switch settings.

Option	Description
MTU (Bytes)	Maximum MTU size for the vSphere Distributed Switch. To enable jumbo frames, set a value greater than 1500 bytes.
Multicast filtering mode	• Basic. The distributed switch forwards traffic that is related to a multicast group based on a MAC address generated from the last 23 bits of the IPv4 address of the group. • IGMP/MLD snooping. The distributed switch forwards multicast traffic to virtual machines according to the IPv4 and IPv6 addresses of subscribed multicast groups by using membership messages defined by the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery protocol.
Discovery Protocol	a Select Cisco Discovery Protocol, Link Layer Discovery Protocol, or (disabled) from the Type drop-down menu. b Set Operation to Listen, Advertise, or Both. For information about Discovery Protocol, see Switch Discovery Protocol.
Administrator Contact	Enter the name and other details of the administrator for the distributed switch.

6 Click OK.

vSphere Networking Update 1 - VMware vSphere 7.0, page 34

Objective 4.2
Identify how to configure different types of datastores.

Types of Datastores

Depending on the storage you use, datastores can be of different types.
vCenter Server and ESXi support the following types of datastores.

Table 17-1. Types of Datastores

Datastore Type	Description
VMFS (version 5 and 6)	Datastores that you deploy on block storage devices use the vSphere Virtual Machine File System (VMFS) format. VMFS is a special high-performance file system format that is optimized for storing virtual machines. See Understanding VMFS Datastores.
NFS (version 3 and 4.1)	An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume. The volume is located on a NAS server. The ESXi host mounts the volume as an NFS datastore, and uses it for storage needs. ESXi supports versions 3 and 4.1 of the NFS protocol. See Understanding Network File System Datastores
vSAN	vSAN aggregates all local capacity devices available on the hosts into a single datastore shared by all hosts in the vSAN cluster. See the *Administering VMware vSAN* documentation.
vVol	vVols datastore represents a storage container in vCenter Server and vSphere Client. See Chapter 22 Working with VMware vSphere Virtual Volumes (vVols).

Depending on your storage type, some of the following tasks are available for the datastores.

- Create datastores. You can use the vSphere Client to create certain types of datastores.
- Perform administrative operations on the datastores. Several operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.
- Organize the datastores. For example, you can group them into folders according to business practices. After you group the datastores, you can assign the same permissions and alarms on the datastores in the group at one time.
- Add the datastores to datastore clusters. A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create the datastore cluster, you can use Storage DRS to manage storage resources. For information about datastore clusters, see the *vSphere Resource Management* documentation.

Understanding VMFS Datastores

To store virtual disks, ESXi uses datastores. The datastores are logical containers that hide specifics of physical storage from virtual machines and provide a uniform model for storing the virtual machine files. The datastores that you deploy on block storage devices use the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing virtual machines.

Use the vSphere Client to set up the VMFS datastore in advance on the block-based storage device that your ESXi host discovers. The VMFS datastore can be extended to span over several physical storage devices that include SAN LUNs and local storage. This feature allows you to pool storage and gives you flexibility in creating the datastore necessary for your virtual machines.

You can increase the capacity of the datastore while the virtual machines are running on the datastore. This ability lets you add new space to your VMFS datastores as your virtual machine requires it. VMFS is designed for concurrent access from multiple physical machines and enforces the appropriate access controls on the virtual machine files.

Versions of VMFS Datastores

Several versions of the VMFS file system have been released since its introduction. Currently, ESXi supports VMFS5 and VMFS6.

For all supported VMFS version, ESXi offers complete read and write support. On the supported VMFS datastores, you can create and power on virtual machines.

Table 17-2. Host Access to VMFS Versions

VMFS	ESXi
VMFS6	Read and write
VMFS5	Read and write

The following table compares major characteristics of VMFS5 and VMFS6. For additional information, see *Configuration Maximums*.

Table 17-3. Comparing VMFS5 and VMFS6

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

RDM	Yes	Yes

When you work with VMFS datastores, consider the following:

- Datastore Extents. A spanned VMFS datastore must use only homogeneous storage devices, either 512n, 512e, or 4Kn. The spanned datastore cannot extend over devices of different formats.
- Block Size. The block size on a VMFS datastore defines the maximum file size and the amount of space a file occupies. VMFS5 and VMFS6 datastores support the block size of 1 MB.
- Storage vMotion. Storage vMotion supports migration across VMFS, vSAN, and vVols datastores. vCenter Server performs compatibility checks to validate Storage vMotion across different types of datastores.
- Storage DRS. VMFS5 and VMFS6 can coexist in the same datastore cluster. However, all datastores in the cluster must use homogeneous storage devices. Do not mix devices of different formats within the same datastore cluster.
- Device Partition Formats. Any new VMFS5 or VMFS6 datastore uses GUID partition table (GPT) to format the storage device. The GPT format enables you to create datastores larger than 2 TB. If your VMFS5 datastore has been previously upgraded from VMFS3, it continues to use the master boot record (MBR) partition format, which is characteristic for VMFS3. Conversion to GPT happens only after you expand the datastore to a size larger than 2 TB.

vSphere Storage Update 1 - VMware vSphere 7.0, page 175

Creating Datastores

You use the New Datastore wizard to create your datastores. Depending on the type of your storage and storage needs, you can create a VMFS, NFS, or vVols datastore.

A vSAN datastore is automatically created when you enable vSAN. For information, see the *Administering VMware vSAN* documentation.

You can also use the New Datastore wizard to manage VMFS datastore copies.

- Create a VMFS Datastore

  VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that the host discovers, including Fibre Channel, iSCSI, and local storage devices.

- Create an NFS Datastore

  You can use the New Datastore wizard to mount an NFS volume.

- Create a vVols Datastore

  You use the New Datastore wizard to create a vVols datastore.

Create a VMFS Datastore

VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that the host discovers, including Fibre Channel, iSCSI, and local storage devices.

Prerequisites

1 Install and configure any adapters that your storage requires.

2 To discover newly added storage devices, perform a rescan. See Storage Rescan Operations.

3 Verify that storage devices you are planning to use for your datastores are available. See Storage Device Characteristics.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select Storage > New Datastore.

3 Select VMFS as the datastore type.

4 Enter the datastore name and if necessary, select the placement location for the datastore.

The system enforces a 42 character limit for the datastore name.

5 Select the device to use for your datastore.

Important The device you select must not have any values displayed in the Snapshot Volume column. If a value is present, the device contains a copy of an existing VMFS datastore. For information on managing datastore copies, see Managing Duplicate VMFS Datastores.

6 Specify the datastore version.

Option	Description
VMFS6	Default format on all hosts that support VMFS6. The ESXi hosts of version 6.0 or earlier cannot recognize the VMFS6 datastore.
VMFS5	VMFS5 datastore supports access by the ESXi hosts of version 6.7 or earlier.

7 Define configuration details for the datastore.

Note The required minimum size for a VMFS6 datastore is 2 GB.

a Specify partition configuration.

Option	Description
Use all available partitions	Dedicates the entire disk to a single VMFS datastore. If you select this option, all file systems and data currently stored on this device are destroyed.
Use free space	Deploys a VMFS datastore in the remaining free space of the disk.

b If the space allocated for the datastore is excessive for your purposes, adjust the capacity values in the Datastore Size field.

By default, the entire free space on the storage device is allocated.

c For VMFS6, specify the block size and define space reclamation parameters. See Space Reclamation Requests from VMFS Datastores.

8 In the Ready to Complete page, review the datastore configuration information and click Finish.

Results

The datastore on the SCSI-based storage device is created. It is available to all hosts that have access to the device.

What to do next

After you create the VMFS datastore, you can perform the following tasks:

- Change the capacity of the datastore. See Increase VMFS Datastore Capacity.
- Edit space reclamation settings. See Change Space Reclamation Settings.
- Enable shared vmdk support. See Enable or Disable Support for Clustered Virtual Disks on the VMFS6 Datastore.

Create an NFS Datastore

You can use the New Datastore wizard to mount an NFS volume.

Prerequisites

- Set up NFS storage environment.
- If you plan to use Kerberos authentication with the NFS 4.1 datastore, make sure to configure the ESXi hosts for Kerberos authentication.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select Storage > New Datastore.

3 Select NFS as the datastore type and specify an NFS version.

- NFS 3
- NFS 4.1

Important If multiple hosts access the same datastore, you must use the same protocol on all hosts.

4 Enter the datastore parameters.

Option	Description
Datastore name	The system enforces a 42 character limit for the datastore name.
Folder	The mount point folder name
Server	The server name or IP address. You can use IPv6 or IPv4 formats. With NFS 4.1, you can add multiple IP addresses or server names if the NFS server supports trunking. The ESXi host uses these values to achieve multipathing to the NFS server mount point.

5 Select Mount NFS read only if the volume is exported as read-only by the NFS server.

6 To use Kerberos security with NFS 4.1, enable Kerberos and select an appropriate Kerberos model.

Option	Description
Use Kerberos for authentication only (krb5)	Supports identity verification
Use Kerberos for authentication and data integrity (krb5i)	In addition to identity verification, provides data integrity services. These services help to protect the NFS traffic from tampering by checking data packets for any potential modifications.

If you do not enable Kerberos, the datastore uses the default AUTH_SYS security.

7 If you are creating a datastore at the data center or cluster level, select hosts that mount the datastore.

8 Review the configuration options and click Finish.

Create a vVols Datastore

You use the New Datastore wizard to create a vVols datastore.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select Storage > New Datastore.

3 Select vVol as the datastore type.

4 Enter the datastore name and select a backing storage container from the list of storage containers.

Make sure to use the name that does not duplicate another datastore name in your data center environment.

If you mount the same vVols datastore to several hosts, the name of the datastore must be consistent across all hosts.

5 Select the hosts that require access to the datastore.

6 Review the configuration options and click Finish.

What to do next

After you create the vVols datastore, you can perform such datastore operations as renaming the datastore, browsing datastore files, unmounting the datastore, and so on.

You cannot add the vVols datastore to a datastore cluster.

vSphere Storage Update 1 - VMware vSphere 7.0, page 199

Administrative Operations for Datastores

After creating datastores, you can perform several administrative operations on the datastores. Certain operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.

- Change Datastore Name

  Use the vSphere Client to change the name of an existing datastore. You can rename the datastore that has virtual machines running on it without any negative impact.

- Unmount Datastores

When you unmount a datastore, it remains intact, but can no longer be seen from the hosts that you specify. The datastore continues to appear on other hosts, where it remains mounted.

- Mount Datastores

  You can mount a datastore you previously unmounted. You can also mount a datastore on additional hosts, so that it becomes a shared datastore.

- Remove VMFS Datastores

  You can delete any type of VMFS datastore, including copies 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.

- Use Datastore Browser

  Use the datastore file browser to manage contents of your datastores. You can browse folders and files that are stored on the datastore. You can also use the browser to upload files and perform administrative tasks on your folders and files.

- Turn Off Storage Filters

  When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices.

Change Datastore Name

Use the vSphere Client to change the name of an existing datastore. You can rename the datastore that has virtual machines running on it without any negative impact.

Note If the host is managed by vCenter Server, you cannot rename the datastore by directly accessing the host from the VMware Host Client. You must rename the datastore from vCenter Server.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore to rename, and select Rename.

3 Enter a new datastore name.

  The system enforces a 42 character limit for the datastore name.

Results

The new name appears on all hosts that have access to the datastore.

Unmount Datastores

When you unmount a datastore, it remains intact, but can no longer be seen from the hosts that you specify. The datastore continues to appear on other hosts, where it remains mounted.

Do not perform any configuration operations that might result in I/O to the datastore while the unmounting is in progress.

Note Make sure that the datastore is not used by vSphere HA Heartbeating. vSphere HA Heartbeating does not prevent you from unmounting the datastore. However, if the datastore

is used for heartbeating, unmounting it might cause the host to fail and restart any active virtual machine.

Prerequisites

When appropriate, before unmounting datastores, make sure that the following prerequisites are met:

- No virtual machines reside on the datastore.
- Storage DRS does not manage the datastore.
- Storage I/O Control is disabled for this datastore.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore and select Unmount Datastore.

3 If the datastore is shared, select the hosts from which to unmount the datastore.

4 Confirm that you want to unmount the datastore.

Results

After you unmount a VMFS datastore from all hosts, the datastore is marked as inactive. If you unmount an NFS or a vVols datastore from all hosts, the datastore disappears from the inventory. You can mount the unmounted VMFS datastore. To mount the NFS or vVols datastore that has been removed from the inventory, use the New Datastore wizard.

What to do next

If you unmounted the VMFS datastore as a part of a storage removal procedure, you can now detach the storage device that is backing the datastore. See Detach Storage Devices.

Mount Datastores

You can mount a datastore you previously unmounted. You can also mount a datastore on additional hosts, so that it becomes a shared datastore.

A VMFS datastore that has been unmounted from all hosts remains in inventory, but is marked as inaccessible. You can use this task to mount the VMFS datastore to a specified host or multiple hosts.

If you have unmounted an NFS or a vVols datastore from all hosts, the datastore disappears from the inventory. To mount the NFS or vVols datastore that has been removed from the inventory, use the New Datastore wizard.

A datastore of any type that is unmounted from some hosts while being mounted on others, is shown as active in the inventory.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore to mount and select one of the following options:

   - Mount Datastore
   - Mount Datastore on Additional Hosts

3 Whether you see one or another option depends on the type of datastore you use.

4 Select the hosts that should access the datastore and click OK.

5 To list all hosts that share the datastore, navigate to the datastore, and click the Hosts tab.

Remove VMFS Datastores

You can delete any type of VMFS datastore, including copies 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.

Note The delete operation for the datastore permanently deletes all files associated with virtual machines on the datastore. Although you can delete the datastore without unmounting, it is preferable that you unmount the datastore first.

Prerequisites

- Remove or migrate all virtual machines from the datastore.
- Unmount the datastore from all hosts.
- Disable Storage DRS for the datastore.
- Disable Storage I/O Control for the datastore.
- Make sure that the datastore is not used for vSphere HA heartbeating.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore to remove, and select Delete Datastore.

3 Confirm that you want to remove the datastore.

Use Datastore Browser

Use the datastore file browser to manage contents of your datastores. You can browse folders and files that are stored on the datastore. You can also use the browser to upload files and perform administrative tasks on your folders and files.

Procedure

1 Open the datastore browser.

   a Display the datastore in the inventory.

   b Right-click the datastore and select Browse Files.

2 Explore the contents of the datastore by navigating to existing folders and files.

3 Perform administrative tasks by using the icons and options.

Icons and Options	Descriptions
Upload Files	Upload a file to the datastore.
Upload Folder (Available only in the vSphere Client)	Upload a folder to the datastore.
Download	Download from the datastore.
New Folder	Create a folder on the datastore.
Copy to	Copy selected folders or files to a new location, either on the same datastore or on a different datastore.
Move to	Move selected folders or files to a new location, either on the same datastore or on a different datastore.
Rename to	Rename selected files.
Delete	Delete selected folders or files.
Inflate	Convert a selected thin virtual disk to thick. This option applies only to thin-provisioned disks.

Upload Files or Folders to Datastores

Use the datastore file browser to upload files to datastores on the ESXi host. If you use the vSphere Client, you can also upload folders.

In addition to their traditional use as storage for virtual machines files, datastores can serve to store data or files related to virtual machines. For example, you can upload ISO images of operating systems from a local computer to a datastore on the host. You then use these images to install guest operating systems on the new virtual machines.

Note You cannot upload files directly to the vVols datastores. You must first create a folder on the vVols datastore, and then upload the files into the folder. The created folders in vVols datastores for block storage have a limited storage capacity space of 4GB. The vVols datastore supports direct uploads of folders.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.
   a Display the datastore in the inventory.
   b Right-click the datastore and select Browse Files.
2 (Optional) Create a folder to store the file or folder.
3 Upload the file or folder.

Option	Description
Upload a file	a Select the target folder and click Upload Files. b Locate the item to upload on the local computer and click Open.
Upload a folder (available only in the vSphere Client)	a Select the datastore or the target folder and click Upload Folders. b Locate the item to upload on the local computer and click Ok.

4 Refresh the datastore file browser to see the uploaded files or folders on the list.

What to do next

You might experience problems when deploying an OVF template that you previously exported and then uploaded to a datastore. For details and a workaround, see the VMware Knowledge Base article 2117310.

Download Files from Datastores

Use the datastore file browser to download files from the datastore available on your ESXi host to your local computer.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.
   a Display the datastore in the inventory.
   b Right-click the datastore and select Browse Files.
2 Navigate to the file to download and click Download.
3 Follow the prompts to save the file to your local computer.

Move or Copy Datastore Folders or Files

Use the datastore browser to move or copy folders or files to a new location, either on the same datastore or on a different datastore.

Note Virtual disk files are moved or copied without format conversion. If you move a virtual disk to a datastore that belongs to a host different from the source host, you might need to convert the virtual disk. Otherwise, you might not be able to use the disk.

You cannot copy VM files across vCenter Servers.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.
   a Display the datastore in the inventory.
   b Right-click the datastore and select Browse Files.
2 Browse to an object you want to move or copy, either a folder or a file.
3 Select the object and click Move to or Copy to.
4 Specify the destination location.
5 (Optional) Select Overwrite files and folders with matching names at the destination.
6 Click OK.

Rename Datastore Files

Use the datastore browser to rename files.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.
   a Display the datastore in the inventory.
   b Right-click the datastore and select Browse Files.
2 Browse to a file you want to rename.
3 Select the file and click Rename to.
4 Specify the new name and click OK.

Inflate Thin Virtual Disks

If you created a virtual disk in the thin format, you can change the format to thick.

You use the datastore browser to inflate the thin virtual disk.

Prerequisites

- Make sure that the datastore where the virtual machine resides has enough space.
- Make sure that the virtual disk is thin.
- Remove snapshots.
- Power off your virtual machine.

Procedure

1 In the vSphere Client, navigate to the folder of the virtual disk you want to inflate.
   a Navigate to the virtual machine.
   b Click the Datastores tab.

      The datastore that stores the virtual machine files is listed.
   c Right-click the datastore and select Browse Files.

      The datastore browser displays contents of the datastore.
2 Expand the virtual machine folder and browse to the virtual disk file that you want to convert.

   The file has the `.vmdk` extension and is marked with the virtual disk () icon.
3 Select the virtual disk file and click Inflate.

Note The option might not be available if the virtual disk is thick or when the virtual machine is running.

Results

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Turn Off Storage Filters

When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices.

Prerequisites

Before you change the device filters, consult with the VMware support team.

Procedure

1 Browse to the vCenter Server instance.

2 Click the Configure tab.

3 Under Settings, click Advanced Settings, and click EDIT SETTINGS.

4 Specify the filter to turn off.

In the Name and Value text boxes at the bottom of the page, enter appropriate information.

Name	Value
config.vpxd.filter.vmfsFilter	False
config.vpxd.filter.rdmFilter	False
config.vpxd.filter.sameHostsAndTransportsFilter	False
config.vpxd.filter.hostRescanFilter	False Note If you turn off this filter, your hosts continue to perform a rescan each time you present a new LUN to a host or a cluster.

5 Click ADD, and click SAVE to save your changes.

You are not required to restart the vCenter Server system.

Storage Filtering

vCenter Server provides storage filters to help you avoid storage device corruption or performance degradation that might be caused by an unsupported use of storage devices. These filters are available by default.

Table 17-6. Storage Filters

Filter Name	Description
config.vpxd.filter.vmfsFilter (VMFS Filter)	Filters out storage devices, or LUNs, that are already used by a VMFS datastore on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with another VMFS datastore or to be used as an RDM.
config.vpxd.filter.rdmFilter (RDM Filter)	Filters out LUNs that are already referenced by an RDM on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with VMFS or to be used by a different RDM. For your virtual machines to access the same LUN, the virtual machines must share the same RDM mapping file. For information about this type of configuration, see the *vSphere Resource Management* documentation.
config.vpxd.filter.sameHostsAndTransportsFilter (Same Hosts and Transports Filter)	Filters out LUNs ineligible for use as VMFS datastore extents because of host or storage type incompatibility. Prevents you from adding the following LUNs as extents: • LUNs not exposed to all hosts that share the original VMFS datastore. • LUNs that use a storage type different from the one the original VMFS datastore uses. For example, you cannot add a Fibre Channel extent to a VMFS datastore on a local storage device.

config.vpxd.filter.hostRescanFilter (Host Rescan Filter)	Automatically rescans and updates VMFS datastores after you perform datastore management operations. The filter helps provide a consistent view of all VMFS datastores on all hosts managed by vCenter Server. Note If you present a new LUN to a host or a cluster, the hosts automatically perform a rescan no matter whether you have the Host Rescan Filter on or off.

vSphere Storage Update 1 - VMware vSphere 7.0, page 207

Objective 4.3
Identify how to configure vSphere HA.

How vSphere HA Works

vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

When you create a vSphere HA cluster, a single host is automatically elected as the primary host. The primary host communicates with vCenter Server and monitors the state of all protected virtual machines and of the secondary hosts. Different types of host failures are possible, and the primary host must detect and appropriately deal with the failure. The primary host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The primary host uses network and datastore heartbeating to determine the type of failure.


Sphere HA Clusters
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:vSphereHAClusters)

Primary and Secondary Hosts

When you add a host to a vSphere HA cluster, an agent is uploaded to the host and configured to communicate with other agents in the cluster. Each host in the cluster functions as a primary host or a secondary host.

When vSphere HA is enabled for a cluster, all active hosts (that are not in standby, maintenance mode or not disconnected) participate in an election to choose the cluster's primary host. The host that mounts the greatest number of datastores has an advantage in the election. Only one primary host typically exists per cluster and all other hosts are secondary hosts. If the primary host fails, is shut down or put in standby mode, or is removed from the cluster a new election is held.

The primary host in a cluster has several responsibilities:

- Monitoring the state of secondary hosts. If a secondary host fails or becomes unreachable, the primary host identifies which virtual machines must be restarted.
- Monitoring the power state of all protected virtual machines. If one virtual machine fails, the primary host ensures that it is restarted. Using a local placement engine, the primary host also determines where the restart takes place.
- Managing the lists of cluster hosts and protected virtual machines.
- Acting as the vCenter Server management interface to the cluster and reporting the cluster health state.

The secondary hosts primarily contribute to the cluster by running virtual machines locally, monitoring their runtime states, and reporting state updates to the primary host. A primary host can also run and monitor virtual machines. Both secondary hosts and primary hosts implement the VM and Application Monitoring features.

One of the functions performed by the primary host is to orchestrate restarts of protected virtual machines. A virtual machine is protected by a primary host after vCenter Server observes that the virtual machine's power state has changed from powered off to powered on in response to a user action. The primary host persists the list of protected virtual machines in the cluster's datastores. A newly elected primary host uses this information to determine which virtual machines to protect.

Note If you disconnect a host from a cluster, the virtual machines registered to that host are unprotected by vSphere HA.

Host Failure Types

The primary host of a VMware vSphere® High Availability cluster is responsible for detecting the failure of secondary hosts. Depending on the type of failure detected, the virtual machines running on the hosts might need to be failed over.

In a vSphere HA cluster, three types of host failure are detected:

- Failure. A host stops functioning.
- Isolation. A host becomes network isolated.
- Partition. A host loses network connectivity with the primary host.

The primary host monitors the liveness of the secondary hosts in the cluster. This communication happens through the exchange of network heartbeats every second. When the primary host stops receiving these heartbeats from a secondary host, it checks for host liveness before declaring the host failed. The liveness check that the primary host performs is to determine whether the secondary host is exchanging heartbeats with one of the datastores. See Datastore Heartbeating . Also, the primary host checks whether the host responds to ICMP pings sent to its management IP addresses.

If a primary host cannot communicate directly with the agent on a secondary host, the secondary host does not respond to ICMP pings. If the agent is not issuing heartbeats, it is viewed as failed. The host's virtual machines are restarted on alternate hosts. If such a secondary host is exchanging heartbeats with a datastore, the primary host assumes that the secondary host is in a network partition or is network isolated. So, the primary host continues to monitor the host and its virtual machines. See Network Partitions.

Host network isolation occurs when a host is still running, but it can no longer observe traffic from vSphere HA agents on the management network. If a host stops observing this traffic, it attempts to ping the cluster isolation addresses. If this pinging also fails, the host declares that it is isolated from the network.

The primary host monitors the virtual machines that are running on an isolated host. If the primary host observes that the VMs power off, and the primary host is responsible for the VMs, it restarts them.

Note If you ensure that the network infrastructure is sufficiently redundant and that at least one network path is always available, host network isolation is less likely to occur.

Proactive HA Failures

A Proactive HA failure occurs when a host component fails, which results in a loss of redundancy or a noncatastrophic failure. However, the functional behavior of the VMs residing on the host is not yet affected. For example, if a power supply on the host fails, but other power supplies are available, that is a Proactive HA failure.

If a Proactive HA failure occurs, you can automate the remediation action taken in the vSphere Availability section of the vSphere Client. The VMs on the affected host can be evacuated to other hosts and the host is either placed in Quarantine mode or Maintenance mode.

Note Your cluster must use vSphere DRS for the Proactive HA failure monitoring to work.

Determining Responses to Host Issues

If a host fails and its virtual machines must be restarted, you can control the order in which the virtual machines are restarted with the VM restart priority setting. You can also configure how vSphere HA responds if hosts lose management network connectivity with other hosts by using the host isolation response setting. Other factors are also considered when vSphere HA restarts a virtual machine after a failure.

The following settings apply to all virtual machines in the cluster in the case of a host failure or isolation. You can also configure exceptions for specific virtual machines. See Customize an Individual Virtual Machine.

Host Isolation Response

Host isolation response determines what happens when a host in a vSphere HA cluster loses its management network connections, but continues to run. You can use the isolation response to have vSphere HA power off virtual machines that are running on an isolated host and restart them on a non-isolated host. Host isolation responses require that Host Monitoring Status is enabled. If Host Monitoring Status is disabled, host isolation responses are also suspended. A host determines that it is isolated when it is unable to communicate with the agents running on the other hosts, and it is unable to ping its isolation addresses. The host then executes its isolation response. The responses are Power off and restart VMs or Shutdown and restart VMs. You can customize this property for individual virtual machines.

Note If a virtual machine has a restart priority setting of Disabled, no host isolation response is made.

To use the Shutdown and restart VMs setting, you must install VMware Tools in the guest operating system of the virtual machine. Shutting down the virtual machine provides the advantage of preserving its state. Shutting down is better than powering off the virtual machine, which does not flush most recent changes to disk or commit transactions. Virtual machines that are in the process of shutting down take longer to fail over while the shutdown completes. Virtual Machines that have not shut down in 300 seconds, or the time specified in the advanced option `das.isolationshutdowntimeout`, are powered off.

After you create a vSphere HA cluster, you can override the default cluster settings for Restart Priority and Isolation Response for specific virtual machines. Such overrides are useful for virtual machines that are used for special tasks. For example, virtual machines that provide infrastructure services like DNS or DHCP might need to be powered on before other virtual machines in the cluster.

A virtual machine "split-brain" condition can occur when a host becomes isolated or partitioned from a primary host and the primary host cannot communicate with it using heartbeat datastores. In this situation, the primary host cannot determine that the host is alive and so declares it dead. The primary host then attempts to restart the virtual machines that are running on the isolated or partitioned host. This attempt succeeds if the virtual machines remain running on the isolated/partitioned host and that host lost access to the virtual machines' datastores when it became isolated or partitioned. A split-brain condition then exists because there are two instances of the virtual machine. However, only one instance is able to read or write the virtual machine's virtual disks. VM Component Protection can be used to prevent this split-brain condition. When you enable VMCP with the aggressive setting, it monitors the datastore accessibility of powered-on virtual machines, and shuts down those that lose access to their datastores.

To recover from this situation, ESXi generates a question on the virtual machine that has lost the disk locks for when the host comes out of isolation and cannot reacquire the disk locks. vSphere HA automatically answers this question, allowing the virtual machine instance that has lost the disk locks to power off, leaving just the instance that has the disk locks.

Virtual Machine Dependencies

You can create dependencies between groups of virtual machines. To do so, you must first create the VM groups in the vSphere Client by going to the Configure tab for the cluster and selecting VM/Host Groups. Once the groups have been created, you can create restart dependency rules between the groups by browsing toVM/Host Rules and in the Type drop-down menu, select Virtual Machines to Virtual Machines. These rules can specify that certain VM groups cannot be restarted until other, specified VM groups have been Ready first.

Factors Considered for Virtual Machine Restarts

After a failure, the cluster's primary host attempts to restart affected virtual machines by identifying a host that can power them on. When choosing such a host, the primary host considers a number of factors.

File accessibility

Before a virtual machine can be started, its files must be accessible from one of the active cluster hosts that the primary can communicate with over the network

Virtual machine and host compatibility

If there are accessible hosts, the virtual machine must be compatible with at least one of them. The compatibility set for a virtual machine includes the effect of any required VM-Host affinity rules. For example, if a rule only permits a virtual machine to run on two hosts, it is considered for placement on those two hosts.

Resource reservations

Of the hosts that the virtual machine can run on, at least one must have sufficient unreserved capacity to meet the memory overhead of the virtual machine and any resource reservations. Four types of reservations are considered: CPU, Memory, vNIC, and Virtual flash. Also, sufficient network ports must be available to power on the virtual machine.

Host limits

In addition to resource reservations, a virtual machine can only be placed on a host if doing so does not violate the maximum number of allowed virtual machines or the number of in-use vCPUs.

Feature constraints

If the advanced option has been set that requires vSphere HA to enforce VM to VM anti-affinity rules, vSphere HA does not violate this rule. Also, vSphere HA does not violate any configured per host limits for fault tolerant virtual machines.
If no hosts satisfy the preceding considerations, the primary host issues an event stating that there are not enough resources for vSphere HA to start the VM and tries again when the cluster conditions have changed. For example, if the virtual machine is not accessible, the primary host tries again after a change in file accessibility.

VM and Application Monitoring

VM Monitoring restarts individual virtual machines if their VMware Tools heartbeats are not received within a set time. Similarly, Application Monitoring can restart a virtual machine if the heartbeats for an application it is running are not received. You can enable these features and configure the sensitivity with which vSphere HA monitors non-responsiveness.

When you enable VM Monitoring, the VM Monitoring service (using VMware Tools) evaluates whether each virtual machine in the cluster is running by checking for regular heartbeats and I/O activity from the VMware Tools process running inside the guest. If no heartbeats or I/O activity are received, this is most likely because the guest operating system has failed or VMware Tools is not being allocated any time to complete tasks. In such a case, the VM Monitoring service determines that the virtual machine has failed and the virtual machine is rebooted to restore service.

Occasionally, virtual machines or applications that are still functioning properly stop sending heartbeats. To avoid unnecessary resets, the VM Monitoring service also monitors a virtual machine's I/O activity. If no heartbeats are received within the failure interval, the I/O stats interval (a cluster-level attribute) is checked. The I/O stats interval determines if any disk or network activity has occurred for the virtual machine during the previous two minutes (120 seconds). If not, the virtual machine is reset. This default value (120 seconds) can be changed using the advanced option `das.iostatsinterval`.

To enable Application Monitoring, you must first obtain the appropriate SDK (or be using an application that supports VMware Application Monitoring) and use it to set up customized heartbeats for the applications you want to monitor. After you have done this, Application Monitoring works much the same way that VM Monitoring does. If the heartbeats for an application are not received for a specified time, its virtual machine is restarted.

You can configure the level of monitoring sensitivity. Highly sensitive monitoring results in a more rapid conclusion that a failure has occurred. While unlikely, highly sensitive monitoring might lead to falsely identifying failures when the virtual machine or application in question is actually still working, but heartbeats have not been received due to factors such as resource constraints. Low sensitivity monitoring results in longer interruptions in service between actual failures and virtual machines being reset. Select an option that is an effective compromise for your needs.

You can also specify custom values for both monitoring sensitivity and the I/O stats interval by selecting the Custom checkbox.

Table 2-1. VM Monitoring Settings

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

After failures are detected, vSphere HA resets virtual machines. The reset ensures that services remain available. To avoid resetting virtual machines repeatedly for nontransient errors, by default, virtual machines will be reset only three times during a certain configurable time interval. After virtual machines have been reset three times, vSphere HA makes no further attempts to reset the virtual machines after subsequent failures until after the specified time has elapsed. You can configure the number of resets using the Maximum per-VM resets custom setting.

Note The reset statistics are cleared when a virtual machine is powered off then back on, or when it is migrated using vMotion to another host. This causes the guest operating system to reboot, but is not the same as a 'restart' in which the power state of the virtual machine is changed.

VM Component Protection

If VM Component Protection (VMCP) is enabled, vSphere HA can detect datastore accessibility failures and provide automated recovery for affected virtual machines.

VMCP provides protection against datastore accessibility failures that can affect a virtual machine running on a host in a vSphere HA cluster. When a datastore accessibility failure occurs, the affected host can no longer access the storage path for a specific datastore. You can determine the response that vSphere HA will make to such a failure, ranging from the creation of event alarms to virtual machine restarts on other hosts.

Note When you use the VM Component Protection feature, your ESXi hosts must be version 6.0 or higher.

Types of Failure

There are two types of datastore accessibility failure:

PDL

PDL (Permanent Device Loss) is an unrecoverable loss of accessibility that occurs when a storage device reports the datastore is no longer accessible by the host. This condition cannot be reverted without powering off virtual machines.

APD

APD (All Paths Down) represents a transient or unknown accessibility loss or any other unidentified delay in I/O processing. This type of accessibility issue is recoverable.

Configuring VMCP

VM Component Protection is configured in the vSphere Client. Go to the Configure tab and click vSphere Availability and Edit. Under Failures and Responses you can select Datastore with PDL or Datastore with APD. The storage protection levels you can choose and the virtual machine remediation actions available differ depending on the type of database accessibility failure.

PDL Failures

Under Datastore with PDL, you can select Issue events or Power off and restart VMs.

APD Failures

The response to APD events is more complex and accordingly the configuration is more fine-grained. You can select Issue events, Power off and restart VMs--conservative restart policy, or Power off and restart VMs--aggressive restart policy

---

Note If either the Host Monitoring or VM Restart Priority settings are disabled, VMCP cannot perform virtual machine restarts. Storage health can still be monitored and events can be issued, however.

Network Partitions

When a management network failure occurs for a vSphere HA cluster, a subset of the cluster's hosts might be unable to communicate over the management network with the other hosts. Multiple partitions can occur in a cluster.

A partitioned cluster leads to degraded virtual machine protection and cluster management functionality. Correct the partitioned cluster as soon as possible.

- Virtual machine protection. vCenter Server allows a virtual machine to be powered on, but it can be protected only if it is running in the same partition as the primary host that is responsible for it. The primary host must be communicating with vCenter Server. A primary host is responsible for a virtual machine if it has exclusively locked a system-defined file on the datastore that contains the virtual machine's configuration file.

- Cluster management. vCenter Server can communicate with the primary host, but only a subset of the secondary hosts. As a result, changes in configuration that affect vSphere HA might not take effect until after the partition is resolved. This failure could result in one of the partitions operating under the old configuration, while another uses the new settings.

Datastore Heartbeating

When the primary host in a VMware vSphere® High Availability cluster cannot communicate with a secondary host over the management network, the primary host uses datastore heartbeating to determine whether the secondary host has failed, is in a network partition, or

is network isolated. If the secondary host has stopped datastore heartbeating, it is considered to have failed and its virtual machines are restarted elsewhere.

VMware vCenter Server® selects a preferred set of datastores for heartbeating. This selection is made to maximize the number of hosts that have access to a heartbeating datastore and minimize the likelihood that the datastores are backed by the same LUN or NFS server.

You can use the advanced option `das.heartbeatdsperhost` to change the number of heartbeat datastores selected by vCenter Server for each host. The default is two and the maximum valid value is five.

vSphere HA creates a directory at the root of each datastore that is used for both datastore heartbeating and for persisting the set of protected virtual machines. The name of the directory is .vSphere-HA. Do not delete or modify the files stored in this directory, because this can have an impact on operations. Because more than one cluster might use a datastore, subdirectories for this directory are created for each cluster. Root owns these directories and files and only root can read and write to them. The disk space used by vSphere HA depends on several factors including which VMFS version is in use and the number of hosts that use the datastore for heartbeating. With vmfs3, the maximum usage is 2GB and the typical usage is 3MB. With vmfs5, the maximum and typical usage is 3MB. vSphere HA use of the datastores adds negligible overhead and has no performance impact on other datastore operations.

vSphere HA limits the number of virtual machines that can have configuration files on a single datastore. See *Configuration Maximums* for updated limits. If you place more than this number of virtual machines on a datastore and power them on, vSphere HA protects virtual machines only up to the limit.

Note A vSAN datastore cannot be used for datastore heartbeating. Therefore, if no other shared storage is accessible to all hosts in the cluster, there can be no heartbeat datastores in use. However, if you have storage that is accessible by an alternate network path independent of the vSAN network, you can use it to set up a heartbeat datastore.

---

vSphere HA Security

vSphere HA is enhanced by several security features.

Select firewall ports opened

vSphere HA uses TCP and UDP port 8182 for agent-to-agent communication. The firewall ports open and close automatically to ensure they are open only when needed.

Configuration files protected using file system permissions

vSphere HA stores configuration information on the local storage or on ramdisk if there is no local datastore. These files are protected using file system permissions and they are accessible only to the root user. Hosts without local storage are only supported if they are managed by Auto Deploy.

Detailed logging

The location where vSphere HA places log files depends on the version of host.

- For ESXi 5.x hosts, vSphere HA writes to syslog only by default, so logs are placed where syslog is configured to put them. The log file names for vSphere HA are prepended with `fdm`, fault domain manager, which is a service of vSphere HA.
- For legacy ESXi 4.x hosts, vSphere HA writes to `/var/log/vmware/fdm` on local disk, as well as syslog if it is configured.
- For legacy ESX 4.x hosts, vSphere HA writes to `/var/log/vmware/fdm`.

Secure vSphere HA logins

vSphere HA logs onto the vSphere HA agents using a user account, vpxuser, created by vCenter Server. This account is the same account used by vCenter Server to manage the host. vCenter Server creates a random password for this account and changes the password periodically. The time period is set by the vCenter Server `VirtualCenter.VimPasswordExpirationInDays` setting. Users with administrative privileges on the root folder of the host can log in to the agent.

Secure communication

All communication between vCenter Server and the vSphere HA agent is done over SSL. Agent-to-agent communication also uses SSL except for election messages, which occur over UDP. Election messages are verified over SSL so that a rogue agent can prevent only the host on which the agent is running from being elected as a primary host. In this case, a configuration issue for the cluster is issued so the user is aware of the problem.

Host SSL certificate verification required

vSphere HA requires that each host have a verified SSL certificate. Each host generates a self-signed certificate when it is booted for the first time. This certificate can then be regenerated or replaced with one issued by an authority. If the certificate is replaced, vSphere HA needs to be reconfigured on the host. If a host becomes disconnected from vCenter Server after its certificate is updated and the ESXi or ESX Host agent is restarted, then vSphere HA is automatically reconfigured when the host is reconnected to vCenter Server. If the disconnection does not occur because vCenter Server host SSL certificate verification is disabled at the time, verify the new certificate and reconfigure vSphere HA on the host.

vSphere Availability Update 1 - VMware vSphere 7.0, page 11

Creating a vSphere HA Cluster

vSphere HA operates in the context of a cluster of ESXi (or legacy ESX) hosts. You must create a cluster, populate it with hosts, and configure vSphere HA settings before failover protection can be established.

When you create a vSphere HA cluster, you must configure a number of settings that determine how the feature works. Before you do this, identify your cluster's nodes. These nodes are the ESXi hosts that will provide the resources to support virtual machines and that vSphere HA will use for failover protection. You should then determine how those nodes are to be connected to one another and to the shared storage where your virtual machine data resides. After that networking architecture is in place, you can add the hosts to the cluster and finish configuring vSphere HA.

You can enable and configure vSphere HA before you add host nodes to the cluster. However, until the hosts are added, your cluster is not fully operational and some of the cluster settings are unavailable. For example, the Specify a Failover Host admission control policy is unavailable until there is a host that can be designated as the failover host.

Note The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled for all virtual machines residing on hosts that are in (or moved into) a vSphere HA cluster. Automatic startup is not supported when used with vSphere HA.

---

vSphere HA Checklist

The vSphere HA checklist contains requirements that you must be aware of before creating and using a vSphere HA cluster.

Review this list before you set up a vSphere HA cluster. For more information, follow the appropriate cross reference.

- All hosts must be licensed for vSphere HA.
- A cluster must contain at least two hosts.

- All hosts must be configured with static IP addresses. If you are using DHCP, you must ensure that the address for each host persists across reboots.
- All hosts must have at least one management network in common. The best practice is to have at least two management networks in common. You should use the VMkernel network with the Management traffic checkbox enabled. The networks must be accessible to each other and vCenter Server and the hosts must be accessible to each other on the management networks. See Best Practices for Networking.
- To ensure that any virtual machine can run on any host in the cluster, all hosts must have access to the same virtual machine networks and datastores. Similarly, virtual machines must be located on shared, not local, storage otherwise they cannot be failed over in the case of a host failure.

Note vSphere HA uses datastore heartbeating to distinguish between partitioned, isolated, and failed hosts. So if some datastores are more reliable in your environment, configure vSphere HA to give preference to them.

- For VM Monitoring to work, VMware tools must be installed. See VM and Application Monitoring.
- vSphere HA supports both IPv4 and IPv6. See Other vSphere HA Interoperability Issues for considerations when using IPv6.
- For VM Component Protection to work, hosts must have the All Paths Down (APD) Timeout feature enabled.
- To use VM Component Protection, clusters must contain ESXi 6.0 hosts or later.
- Only vSphere HA clusters that contain ESXi 6.0 or later hosts can be used to enable VMCP. Clusters that contain hosts from an earlier release cannot enable VMCP, and such hosts cannot be added to a VMCP-enabled cluster.
- If your cluster uses Virtual Volume datastores, when vSphere HA is enabled a configuration Virtual Volume is created on each datastore by vCenter Server. In these containers, vSphere HA stores the files it uses to protect virtual machines. vSphere HA does not function correctly if you delete these containers. Only one container is created per Virtual Volume datastore.

Create a vSphere HA Cluster in the vSphere Client

To enable your cluster for vSphere HA, you must first create an empty cluster. After you plan the resources and networking architecture of your cluster, use the vSphere Client to add hosts to the cluster and specify the cluster's vSphere HA settings.

A vSphere HA-enabled cluster is a prerequisite for vSphere Fault Tolerance.

Prerequisites

- Verify that all virtual machines and their configuration files reside on shared storage.
- Verify that the hosts are configured to access the shared storage so that you can power on the virtual machines by using different hosts in the cluster.
- Verify that hosts are configured to have access to the virtual machine network.
- Verify that you are using redundant management network connections for vSphere HA. For information about setting up network redundancy, see Best Practices for Networking.
- Verify that you have configured hosts with at least two datastores to provide redundancy for vSphere HA datastore heartbeating.

- Connect vSphere Client to vCenter Server by using an account with cluster administrator permissions.

Procedure

1 In the vSphere Client, browse to the data center where you want the cluster to reside and click New Cluster.

2 Complete the New Cluster wizard.

   Do not turn on vSphere HA (or DRS).

3 Click OK to close the wizard and create an empty cluster.

4 Based on your plan for the resources and networking architecture of the cluster, use the vSphere Client to add hosts to the cluster.

5 Browse to the cluster and enable vSphere HA.

   a Click the Configure tab.
   b Select vSphere Availability and click Edit.
   c Select vSphere HA.

6 Under Failures and Responses select Enable Host Monitoring.

   With Host Monitoring enabled, hosts in the cluster can exchange network heartbeats and vSphere HA can take action when it detects failures. Host Monitoring is required for the vSphere Fault Tolerance recovery process to work properly.

7 Select a setting for VM Monitoring.

   Select VM Monitoring Only to restart individual virtual machines if their heartbeats are not received within a set time. You can also select VM and Application Monitoring to enable application monitoring.

8 Click OK.

Results

You have a vSphere HA cluster, populated with hosts.

What to do next

Configure the appropriate vSphere HA settings for your cluster.

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

See Configuring vSphere Availability Settings.

Configuring vSphere Availability Settings

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

In the vSphere Client, you can configure following the vSphere HA settings:

Failures and responses

Provide settings here for host failure responses, host isolation, VM monitoring, and VM Component Protection.

Admission Control

Enable or disable admission control for the vSphere HA cluster and choose a policy for how it is enforced.

Heartbeat Datastores

Specify preferences for the datastores that vSphere HA uses for datastore heartbeating.

Advanced Options

Customize vSphere HA behavior by setting advanced options.

Configuring Responses to Failures

The Failure and Responses pane of the vSphere HA settings allows you to configure how your cluster should function when problems are encountered.

In this part of the vSphere Client, you can determine the specific responses the vSphere HA cluster has for host failures and isolation. You can also configure VM Component Protection (VMCP) actions when Permanent Device Loss (PDL) and All Paths Down (APD) situations occur and you can enable VM monitoring.

The following tasks are available:

Procedure

1 Respond to Host Failure

   You can set specific responses to host failures that occur in your vSphere HA cluster.

2 Respond to Host Isolation

   You can set specific responses to host isolation that occurs in your vSphere HA cluster.

3 Configure VMCP Responses

   Configure the response that VM Component Protection (VMCP) makes when a datastore encounters a PDL or APD failure.

4 Enable VM Monitoring

   You can turn on VM and Application Monitoring and also set the monitoring sensitivity for your vSphere HA cluster.

Respond to Host Failure

You can set specific responses to host failures that occur in your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses and then expand Host Failure Response.

5 Select from the following configuration options.

Option	Description
Failure Response	If you select Disabled, this setting turns off host monitoring and VMs are not restarted when host failures occur. If Restart VMs is selected, VMs are failed over based on their restart priority when a host fails.
Default VM Restart Priority	The restart priority determines the order in which virtual machines are restarted when the host fails. Higher priority virtual machines are started first. If multiple hosts fail, all virtual machines are migrated from the first host in order of priority, then all virtual machines from the second host in order of priority, and so on.
VM Restart Priority Condition	A specific condition must be selected as well as a delay after that condition has been met, before vSphere HA is allowed to continue to the next VM restart priority.

6 Click OK.

Results

Your settings for the host failure response take effect.

Respond to Host Isolation

You can set specific responses to host isolation that occurs in your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses and expand Response for Host Isolation.

5 To configure the host isolation response, select Disabled, Shut down and restart VMs, or Power off and restart VMs.

6 Click OK.

Results

Your setting for the host isolation response takes effect.

Configure VMCP Responses

Configure the response that VM Component Protection (VMCP) makes when a datastore encounters a PDL or APD failure.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses, and expand either Datastore with PDL or Datastore with APD .

5 If you clicked Datastore with PDL, you can set the VMCP failure response for this type of issue, either Disabled, Issue Events, or Power off and restart VMs.

6 If you clicked Datastore with APD, you can set the VMCP failure response for this type of issue, either Disabled, Issue Events, Power off and restart VMs--Conservative restart policy, or Power off and restart VMs--Aggressive restart policy. You can also set Response recovery, which is the number of minutes that VMCP waits before taking action.

7 Click OK.

Results

Your settings for the VMCP failure response take effect.

Enable VM Monitoring

You can turn on VM and Application Monitoring and also set the monitoring sensitivity for your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses and expand VM Monitoring.

5 Select VM Monitoring and Application Monitoring.

These settings turn on VMware Tools heartbeats and application heartbeats, respectively.

6 To set the heartbeat monitoring sensitivity, move the slider between Low and High or select Custom to provide custom settings.

7 Click OK.

Results

Your monitoring settings take effect.

Configure Proactive HA

You can configure how Proactive HA responds when a provider has notified its health degradation to vCenter, indicating a partial failure of that host.

This page is editable only if you have enabled vSphere DRS.

Procedure

1 In the vSphere Client, browse to the Proactive HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Select Turn on Proactive HA.

5 Click Proactive HA Failures and Responses.

6 Select from the following configuration options.

Option	Description

Automation Level	Determine whether host quaratine or maintenance mode and VM migrations are recommendations or automatic • Manual. vCenter Server suggests migration recommendations for virtual machines. • Automated. Virtual machines are migrated to healthy hosts and degraded hosts are entered into quarantine or maintenance mode depending on the configured Proactive HA automation level.
Remediation	Determine what happens to partially degraded hosts. • Quarantine mode for all failures. Balances performance and availability, by avoiding the usage of partially degraded hosts provided that virtual machine performance is unaffected. • Quarantine mode for moderate and Maintenance mode for severe failure (Mixed). Balances performance and availability, by avoiding the usage of moderately degraded hosts provided that virtual machine performance is unaffected. Ensures that virtual machines do not run on severely failed hosts. • Maintenance mode for all failures. Ensures that virtual machines do not run on partially failed hosts. `Host.Config.Quarantine` and `Host.Config.Maintenance` privileges are required to put hosts in Quarantine mode and Maintenance mode, respectively.

To enable Proactive HA providers for this cluster, select the check boxes. Providers appear when their corresponding vSphere Client plugin has been installed and the providers monitor every host in the cluster. To view or edit the failure conditions supported by the provider, click the edit link.

7 Click OK.

Configure Admission Control

After you create a cluster, you can configure admission control to specify whether virtual machines can be started if they violate availability constraints. The cluster reserves resources so that failover can occur for all running virtual machines on the specified number of hosts.

The Admission Control page appears only if you enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Admission Control to display the configuration options.

5 Select a number for the Host failures cluster tolerates. This is the maximum number of host failures that the cluster can recover from or guarantees failover for.

6 Select an option for Define host failover capacity by.

Option	Description
Cluster resource percentage	Specify a percentage of the cluster's CPU and memory resources to reserve as spare capacity to support failovers.
Slot Policy (powered-on VMs)	Select a slot size policy that covers all powered on VMs or is a fixed size. You can also calculate how many VMs require multiple slots.

Dedicated failover hosts	Select hosts to use for failover actions. Failovers can still occur on other hosts in the cluster if a default failover host does not have enough resources.
Disabled	Select this option to disable admission control and allow virtual machine power ons that violate availability constraints.

7 Set the percentage for the Performance degradation VMs tolerate.

This setting determines what percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure.

8 Click OK.

Results

Your admission control settings take effect.

Configure Heartbeat Datastores

vSphere HA uses datastore heartbeating to distinguish between hosts that have failed and hosts that reside on a network partition. With datastore heartbeating, vSphere HA can monitor hosts when a management network partition occurs and continue to respond to failures.

You can specify the datastores that you want to be used for datastore heartbeating.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Heartbeat Datastores to display the configuration options for datastore heartbeating.

5 To instruct vSphere HA about how to select the datastores and how to treat your preferences, select from the following options.

Table 2-3.

Datastore Heartbeating Options
Automatically select datastores accessible from the host
Use datastores only from the specified list
Use datastores from the specified list and complement automatically if needed

6 In the Available heartbeat datastores pane, select the datastores that you want to use for heartbeating.

The listed datastores are shared by more than one host in the vSphere HA cluster. When a datastore is selected, the lower pane displays all the hosts in the vSphere HA cluster that can access it.

7 Click OK.

Set Advanced Options

To customize vSphere HA behavior, set advanced vSphere HA options.

Prerequisites

Verify that you have cluster administrator privileges.

Note Because these options affect the functioning of vSphere HA, change them with caution.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Advanced Options.

5 Click Add and type the name of the advanced option in the text box.

You can set the value of the option in the text box in the Value column.

6 Repeat step 5 for each new option that you want to add and click OK.

Results

The cluster uses the options that you added or modified.

What to do next

Once you have set an advanced vSphere HA option, it persists until you do one the following:

- Using the vSphere Client, reset its value to the default value.
- Manually edit or delete the option from the fdm.cfg file on all hosts in the cluster.

vSphere HA Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

Table 2-4. vSphere HA Advanced Options

Option	Description
`das.isolationaddress[...]`	Sets the address to ping to determine if a host is isolated from the network. This address is pinged only when heartbeats are not received from any other host in the cluster. If not specified, the default gateway of the management network is used. This default gateway has to be a reliable address that is available, so that the host can determine if it is isolated from the network. You can specify multiple isolation addresses (up to 10) for the cluster: `das.isolationAddressX`, where X = 0-9. Typically you should specify one per management network. Specifying too many addresses makes isolation detection take too long.
`das.usedefaultisolationaddress`	By default, vSphere HA uses the default gateway of the console network as an isolation address. This option specifies whether or not this default is used (true|false).
`das.isolationshutdowntimeout`	The period of time the system waits for a virtual machine to shut down before powering it off. This only applies if the host's isolation response is Shut down VM. Default value is 300 seconds.
`das.slotmeminmb`	Defines the maximum bound on the memory slot size. If this option is used, the slot size is the smaller of this value or the maximum memory reservation plus memory overhead of any powered-on virtual machine in the cluster.
`das.slotcpuinmhz`	Defines the maximum bound on the CPU slot size. If this option is used, the slot size is the smaller of this value or the maximum CPU reservation of any powered-on virtual machine in the cluster.
`das.vmmemoryminmb`	Defines the default memory resource value assigned to a virtual machine if its memory reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default

	is 0 MB.
das.vmcpuminmhz	Defines the default CPU resource value assigned to a virtual machine if its CPU reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default is 32MHz.
das.iostatsinterval	Changes the default I/O stats interval for VM Monitoring sensitivity. The default is 120 (seconds). Can be set to any value greater than, or equal to 0. Setting to 0 disables the check. Note Values of less than 50 are not recommended since smaller values can result in vSphere HA unexpectedly resetting a virtual machine.
das.ignoreinsufficienthbdatastore	Disables configuration issues created if the host does not have sufficient heartbeat datastores for vSphere HA. Default value is false.
das.heartbeatdsperhost	Changes the number of heartbeat datastores required. Valid values can range from 2-5 and the default is 2.
das.config.fdm.isolationPolicyDelaySec	The number of seconds system waits before executing the isolation policy once it is determined that a host is isolated. The minimum value is 30. If set to a value less than 30, the delay will be 30 seconds.
das.respectvmvmantiaffinityrules	Determines if vSphere HA enforces VM-VM anti-affinity rules. The default value is "true" and rules are enforced even if vSphere DRS is not enabled. In this case, vSphere HA does not fail over a virtual machine if doing so violates a rule, but it issues an event reporting there are insufficient resources to perform the failover. This option can also be set to "false", whereby the rules are not enforced. See vSphere Resource Management for more information on anti-affinity rules.
das.maxresets	The maximum number of reset attempts made by VMCP. If a reset operation on a virtual machine affected by an APD situation fails, VMCP retries the reset this many times before giving up
das.maxterminates	The maximum number of retries made by VMCP for virtual machine termination.
das.terminateretryintervalsec	If VMCP fails to terminate a virtual machine, this is the number of seconds the system waits before it retries a terminate attempt
das.config.fdm.reportfailoverfailevent	When set to 1, enables generation of a detailed per-VM event when an attempt by vSphere HA to restart a virtual machine is unsuccessful. Default value is 0. In versions earlier than vSphere 6.0, this event is generated by default.
vpxd.das.completemetadataupdateintervalsec	The period of time (seconds) after a VM-Host affinity rule is set during which vSphere HA can restart a VM in a DRS-disabled cluster, overriding the rule. Default value is 300 seconds.
das.config.fdm.memReservationMB	By default vSphere HA agents run with a configured memory limit of 250 MB. A host might not allow this reservation if it runs out of reservable capacity. You can use this advanced option to lower the memory limit to avoid this issue. Only integers greater than 100, which is the minimum value, can be specified. Conversely, to prevent problems during primary agent elections in a large cluster (containing 6,000 to 8,000 VMs) you should raise this limit to 325 MB. Note Once this limit is changed, for all hosts in the cluster you must run the Reconfigure HA task. Also, when a new host is added to the cluster or an existing host is rebooted, this task should be performed on those hosts in order to update this memory setting.
das.reregisterrestartdisabledvms	When vSphere HA is disabled on a specific VM this option ensures that the VM is registered on another host after a failure. This allows you to power-on that VM without needing to re-register it manually. Note When this option is used, vSphere HA does not power on the VM, but only registers it.
das.respectvmhostsoftaffinityrules	Determines if vSphere HA restarts a respective VM on a host that belongs to the same VM-Host group. If no such host is available or if the value of this option is set to “false”, vSphere HA restarts the VM on any available host in the cluster. In vSphere 6.5, the default value is "true". This value might not be visibly defined in the advanced HA options of the cluster. If you want to disable the option, you must manually set this option as "false" in the

advanced HA options for the cluster.

Note If you change the value of any of the following advanced options, you must disable and then re-enable vSphere HA before your changes take effect.

- `das.isolationaddress[...]`
- `das.usedefaultisolationaddress`
- `das.isolationshutdowntimeout`

Customize an Individual Virtual Machine

Each virtual machine in a vSphere HA cluster is assigned the cluster default settings for VM Restart Priority, Host Isolation Response, VM Component Protection, and VM Monitoring. You can specify specific behavior for each virtual machine by changing these defaults. If the virtual machine leaves the cluster, these settings are lost.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Under Configuration, select VM Overrides and click Add.

4 Use the + button to select virtual machines to which to apply the overrides.

5 Click OK.

6 (Optional) You can change other settings, such as the Automation level, VM restart priority, Response for Host Isolation, VMCP settings,VM Monitoring, or VM monitoring sensitivity settings.

Note You can view the cluster defaults for these settings by first expanding Relevant Cluster Settings and then expanding vSphere HA.

7 Click OK.

Results

The virtual machine's behavior now differs from the cluster defaults for each setting that you changed.

vSphere Availability Update 1 - VMware vSphere 7.0, page 34

Objective 4.4
Identify how to configure vSphere DRS.

vSphere DRS

vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs.

Note If you try to enable DRS on a cluster where there are issues with the vCLS VMs, a warning message is displayed on the Cluster Summary page.

Note If DRS is on but there are issues with the vCLS VMs, you must resolve these issues for DRS to operate. A warning message is displayed on the Cluster Summary page.

If DRS is non-functional this does not mean that DRS is disabled. Existing DRS settings and resource pools survive across a lost vCLS VMs quorum. vCLS health turns Unhealthy only in a DRS enabled cluster when vCLS VMs are not running and the first instance of DRS is skipped because of this. vCLS health will stay Degraded on a non-DRS enabled cluster when at least one vCLS VM is not running.

vSphere Resource Management Update 1 - VMware vSphere 7.0, page 77

DRS Cluster Requirements

Hosts that are added to a DRS cluster must meet certain requirements to use cluster features successfully.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Shared Storage Requirements

A DRS cluster has certain shared storage requirements.

Ensure that the managed hosts use shared storage. Shared storage is typically on a SAN, but can also be implemented using NAS shared storage.

See the *vSphere Storage* documentation for information about other shared storage.

Shared VMFS Volume Requirements

A DRS cluster has certain shared VMFS volume requirements.

Configure all managed hosts to use shared VMFS volumes.

- Place the disks of all virtual machines on VMFS volumes that are accessible by source and destination hosts.
- Ensure the VMFS volume is sufficiently large to store all virtual disks for your virtual machines.
- Ensure all VMFS volumes on source and destination hosts use volume names, and all virtual machines use those volume names for specifying the virtual disks.

Note Virtual machine swap files also need to be on a VMFS accessible to source and destination hosts (just like `.vmdk` virtual disk files). This requirement does not apply if all source and destination hosts are ESX Server 3.5 or higher and using host-local swap. In that case, vMotion with swap files on unshared storage is supported. Swap files are placed on a VMFS by default, but administrators might override the file location using advanced virtual machine configuration options.

Processor Compatibility Requirements

A DRS cluster has certain processor compatibility requirements.

To avoid limiting the capabilities of DRS, you should maximize the processor compatibility of source and destination hosts in the cluster.

vMotion transfers the running architectural state of a virtual machine between underlying ESXi hosts. vMotion compatibility means that the processors of the destination host must be able

to resume execution using the equivalent instructions where the processors of the source host were suspended. Processor clock speeds and cache sizes might vary, but processors must come from the same vendor class (Intel versus AMD) and the same processor family to be compatible for migration with vMotion.

Processor families are defined by the processor vendors. You can distinguish different processor versions within the same family by comparing the processors' model, stepping level, and extended features.

Sometimes, processor vendors have introduced significant architectural changes within the same processor family (such as 64-bit extensions and SSE3). VMware identifies these exceptions if it cannot guarantee successful migration with vMotion.

vCenter Server provides features that help ensure that virtual machines migrated with vMotion meet processor compatibility requirements. These features include:

- Enhanced vMotion Compatibility (EVC) – You can use EVC to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.

  Configure EVC from the Cluster Settings dialog box. The hosts in a cluster must meet certain requirements for the cluster to use EVC. For information about EVC and EVC requirements, see the *vCenter Server and Host Management* documentation.

- CPU compatibility masks – vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migrations with vMotion. By applying CPU compatibility masks to individual virtual machines, you can hide certain CPU features from the virtual machine and potentially prevent migrations with vMotion from failing due to incompatible CPUs.

vMotion Requirements for DRS Clusters

A DRS cluster has certain vMotion requirements.

To enable the use of DRS migration recommendations, the hosts in your cluster must be part of a vMotion network. If the hosts are not in the vMotion network, DRS can still make initial placement recommendations.

To be configured for vMotion, each host in the cluster must meet the following requirements:

- vMotion does not support raw disks or migration of applications clustered using Microsoft Cluster Service (MSCS).

- vMotion requires a private Gigabit Ethernet migration network between all of the vMotion enabled managed hosts. When vMotion is enabled on a managed host, configure a unique network identity object for the managed host and connect it to the private migration network.

Create a Cluster

A cluster is a group of hosts. When a host is added to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts within it.

Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Prerequisites

- Verify that you have sufficient permissions to create a cluster object.
- Verify that a data center exists in the inventory.
- If you want to use vSAN, it must be enabled before you configure vSphere HA.

Procedure

1 Browse to a data center in the vSphere Client.

2 Right-click the data center and select New Cluster.

3 Enter a name for the cluster.

4 Select DRS and vSphere HA cluster features.

Option	Description
To use DRS with this cluster	a Select the DRS Turn ON check box. b Select an automation level and a migration threshold.
To use HA with this cluster	a Select the vSphere HA Turn ON check box. b Select whether to enable host monitoring and admission control. c If admission control is enabled, specify a policy. d Select a VM Monitoring option. e Specify the virtual machine monitoring sensitivity.

5 Select an Enhanced vMotion Compatibility (EVC) setting.

EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.

6 Click OK.

Results

The cluster is added to the inventory.

What to do next

Add hosts and resource pools to the cluster.

Note Under the Cluster Summary page, you can see Cluster Services which displays vSphere Cluster Services health status.

Edit Cluster Settings

When you add a host to a DRS cluster, the host's resources become part of the cluster's resources. In addition to this aggregation of resources, with a DRS cluster you can support cluster-wide resource pools and enforce cluster-level resource allocation policies.

The following cluster-level resource management capabilities are also available.

Load Balancing

The distribution and usage of CPU and memory resources for all hosts and virtual machines in the cluster are continuously monitored. DRS compares these metrics to an ideal resource

usage given the attributes of the cluster's resource pools and virtual machines, the current demand, and the imbalance target. DRS then provides recommendations or performs virtual machine migrations accordingly. See Virtual Machine Migration. When you power on a virtual machine in the cluster, DRS attempts to maintain proper load balancing by either placing the virtual machine on an appropriate host or making a recommendation. See Admission Control and Initial Placement.

Power management

When the vSphere Distributed Power Management (DPM) feature is enabled, DRS compares cluster and host-level capacity to the demands of the cluster's virtual machines, including recent historical demand. DRS then recommends you place hosts in standby, or places hosts in standby power mode when sufficient excess capacity is found. DRS powers-on hosts if capacity is needed. Depending on the resulting host power state recommendations, virtual machines might need to be migrated to and from the hosts as well. See Managing Power Resources.

Affinity Rules
You can control the placement of virtual machines on hosts within a cluster, by assigning affinity rules. See Using DRS Affinity Rules.

Prerequisites

You can create a cluster without a special license, but you must have a license to enable a cluster for vSphere DRS or vSphere HA.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Procedure

1 Browse to a cluster in the vSphere Client.

2 Click the Configure tab and click Services.

3 Under vSphere DRS click Edit.

4 Under DRS Automation, select a default automation level for DRS.

Automation Level	Action
Manual	• Initial placement: Recommended host is displayed. • Migration: Recommendation is displayed.
Partially Automated	• Initial placement: Automatic. • Migration: Recommendation is displayed.
Fully Automated	• Initial placement: Automatic. • Migration: Recommendation is run automatically.

5 Set the Migration Threshold for DRS.

6 Select the Predictive DRS check box. In addition to real-time metrics, DRS responds to forecasted metrics provided by vRealize Operations server. You must also configure Predictive DRS in a version of vRealize Operations that supports this feature

7 Select Virtual Machine Automation check box to enable individual virtual machine automation levels.

Override for individual virtual machines can be set from the VM Overrides page.

8 Under Additional Options, select a check box to enforce one of the default policies.

Option	Description
VM Distribution	For availability, distribute a more even number of virtual machines across hosts. This is secondary to DRS load balancing.
Memory Metric for Load Balancing	Load balance based on consumed memory of virtual machines rather than active memory. This setting is only recommended for clusters where host memory is not over-committed. Note This setting is no longer supported and will not be displayed in vCenter 7.0.
CPU Over-Commitment	Control CPU over-commitment in the cluster.
Scalable Shares	Enable scalable shares for the resource pools on this cluster.

9 Under Power Management, select Automation Level.

10 If DPM is enabled, set the DPM Threshold.

11 Click OK.

What to do next

Note Under the Cluster Summary page, you can see Cluster Services which displays vSphere Cluster Services health status.

You can view memory utilization for DRS in the vSphere Client. To find out more, see:

Viewing Distributed Resource Scheduler Memory Utilization (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_drs)

Set a Custom Automation Level for a Virtual Machine

After you create a DRS cluster, you can customize the automation level for individual virtual machines to override the cluster's default automation level.

For example, you can select Manual for specific virtual machines in a cluster with full automation, or Partially Automated for specific virtual machines in a manual cluster.

If a virtual machine is set to Disabled, vCenter Server does not migrate that virtual machine or provide migration recommendations for it.

Procedure

1 Browse to the cluster in the vSphere Client.

2 Click the Configure tab and click Services.

3 Under Services, select vSphere DRS and click Edit. Expand DRS Automation.

4 Select the Enable individual virtual machine automation levels check box.

5 To temporarily disable any individual virtual machine overrides, deselect the Enable individual virtual machine automation levels check box.

Virtual machine settings are restored when the check box is selected again.

6 To temporarily suspend all vMotion activity in a cluster, put the cluster in manual mode and deselect the Enable individual virtual machine automation levels check box.

7 Select one or more virtual machines.

8 Click the Automation Level column and select an automation level from the drop-down menu.

Option	Description
Manual	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.
Partially Automated	Initial placement is performed automatically. Migration recommendations are displayed, but do not run.
Disabled	vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

9 Click OK.

Results

Note Other VMware products or features, such as vSphere vApp and vSphere Fault Tolerance, might override the automation levels of virtual machines in a DRS cluster. Refer to the product-specific documentation for details.

Disable DRS

You can turn off DRS for a cluster.

When DRS is disabled, the cluster's resource pool hierarchy and affinity rules are not reestablished when DRS is turned back on. If you disable DRS, the resource pools are removed from the cluster. To avoid losing the resource pools, save a snapshot of the resource pool tree on your local machine. You can use the snapshot to restore the resource pool when you enable DRS.

Procedure

1 Browse to the cluster in the vSphere Client.

2 Click the Configure tab and click Services.

3 Under vSphere DRS, click Edit.

4 Deselect the Turn On vSphere DRS check box.

5 Click OK to turn off DRS.

6 (Optional) Choose an option to save the resource pool.

- Click Yes to save a resource pool tree snapshot on a local machine.
- Click No to turn off DRS without saving a resource pool tree snapshot.

Results

DRS is turned off.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Restore a Resource Pool Tree

You can restore a previously saved resource pool tree snapshot.

Prerequisites

- vSphere DRS must be turned ON.
- You can restore a snapshot only on the same cluster that it was taken.
- No other resource pools are present in the cluster.

Procedure

1 Browse to the cluster in the vSphere Client.

2 Right-click on the cluster and select Restore Resource Pool Tree.

3 Click Browse, and locate the snapshot file on your local machine.

4 Click Open.

5 Click OK to restore the resource pool tree.

vSphere Resource Management Update 1 - VMware vSphere 7.0, page 86

Objective 4.5
Identify how to configure EVC.

Enhanced vMotion Compatibility as a Virtual Machine Attribute

Enhanced vMotion Compatibility (EVC) is a cluster feature that ensures CPU compatibility between hosts in a cluster, so that you can seamlessly migrate virtual machines within the EVC cluster. You can also enable, disable, or change the EVC mode at the virtual machine level. The per-VM EVC feature facilitates the migration of the virtual machine beyond the cluster and across vCenter Server systems and data centers that have different processors.

Starting with vSphere 7.0 Update 1, you can take advantage of the EVC feature for Virtual Shared Graphics Acceleration (vSGA). vSGA allows multiple virtual machines to share GPUs installed on ESXi hosts and leverage the 3D graphics acceleration capabilities.

The EVC mode of a virtual machine is independent from the EVC mode defined at the cluster level. The cluster-based EVC mode limits the CPU features a host exposes to virtual machines. The per-VM EVC mode determines the set of host CPU features that a virtual machine requires to power on and migrate.

By default, when you power on a newly created virtual machine, it inherits the feature set of its parent EVC cluster or host. However, you can change the EVC mode for each virtual machine separately. You can raise or lower the EVC mode of a virtual machine. Lowering the EVC mode increases the CPU compatibility of the virtual machine. You can also use the API calls to customize the EVC mode further.

Cluster-Level EVC and Per-VM EVC

There are several differences between the way the EVC feature works at the host cluster level and at the virtual machine level.

- Unlike cluster-based EVC, you can change the per-VM EVC mode only when the virtual machine is powered off.

- With cluster-based EVC, when you migrate a virtual machine out of the EVC cluster, a power cycle resets the EVC mode that the virtual machine has. With Per-VM EVC, the EVC mode becomes an attribute of the virtual machine. A power cycle does not affect the compatibility of the virtual machine with different processors.

- When you configure EVC at the virtual machine level, the per-VM EVC mode overrides cluster-based EVC. If you do not configure per-VM EVC, when you power on the virtual machine, it inherits the EVC mode of its parent EVC cluster or host.

- If a virtual machine is in an EVC cluster and the per-VM EVC is also enabled, the EVC mode of the virtual machine cannot exceed the EVC mode of the EVC cluster in which the virtual machine runs. The baseline feature set that you configure for the virtual machine cannot contain more CPU features than the baseline feature set applied to the hosts in the EVC cluster. For example, if you configure a cluster with the Intel "Merom" Generation EVC mode, you should not configure a virtual machine with any other Intel baseline feature set. All other sets contain more CPU features than the Intel "Merom" Generation feature set and as a result of such configuration, the virtual machine fails to power on.

To learn more about EVC clusters, see the *vCenter Server and Host Management* guide.

Compatibility and Requirements

The per-VM EVC feature has the following requirements.

Compatibility	Requirement
Host compatibility	ESXi 6.7 or later.
vCenter Server compatibility	vCenter Server 6.7 or later.
Virtual machine compatibility	Virtual hardware version 14 or later.

To check EVC support for a specific processor or server model, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.

Configure the EVC Mode of a Virtual Machine

Per-VM EVC is disabled by default. You can enable, disable, and change the EVC mode of a virtual machine to ensure its seamless migration across clusters, vCenter Server systems, and data centers that have different processors.

To check what the EVC mode of a virtual machine is, see Determine the EVC Mode of a Virtual Machine.

Prerequisites

Power off the virtual machine

- Power off the virtual machine.

Procedure

1 Navigate to a virtual machine in the vCenter Server inventory.

2 On the Configure tab, select VMware EVC.

The pane shows details about the EVC mode of the virtual machine and CPUID details.

Important For newly created virtual machines, the EVC mode that shows in the VMware EVC pane is disabled.
For powered off virtual machines, the VMware EVC pane always shows the EVC status defined at the virtual machine level.

For powered on virtual machines with per-VM EVC enabled, the VMware EVC pane shows the EVC status defined at the virtual machine level.
For powered on virtual machines with per-VM EVC disabled, the VMware EVC pane shows the EVC mode that the virtual machine inherits from its parent EVC cluster or host.

3 Click the Edit button.

The Change EVC Mode dialog box opens.

4 In the Change EVC Mode dialog box, select whether to enable or disable EVC.

Option	Description
Disable EVC	The EVC feature is disabled for the virtual machine. When you power on the virtual machine, it inherits the feature set of its parent EVC cluster or host.
Enable EVC for AMD hosts	The EVC feature is enabled for AMD hosts.
Enable EVC for Intel hosts	The EVC feature is enabled for Intel hosts.
Custom	This option is visible only if you have customized the EVC mode of the virtual machine through the API calls.

5 (Optional) From the CPU Mode drop-down menu, select a baseline CPU feature set.

Important If the virtual machine is in an EVC cluster and the per-VM EVC mode exceeds the EVC mode for the cluster, the virtual machine fails to power on. The baseline CPU feature set for the virtual machine must not contain more CPU features than the baseline CPU feature set of the cluster.

6 (Required) From the Graphics Mode (vSGA) drop-down menu, select a baseline graphics feature set.

Note Graphics Mode (vSGA) applies only the Baseline Graphics set that includes features through Direct3D 10.1/OpenGL 3.3. The Baseline Graphics feature set is compatible with all supported features for ESXi 7.0 or earlier.

7 Click OK.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU and graphics features that a host must have in order for the virtual machine to migrate to that host and power on. The EVC mode of a virtual machine is independent from the EVC mode that you configure for the cluster in which the virtual machine runs.

The EVC mode of a virtual machine is determined when the virtual machine powers on. At power-on, the virtual machine also determines the EVC mode of the cluster in which it runs. If the EVC mode of a running virtual machine or the entire EVC cluster is raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not use any CPU features exposed by the new EVC mode until the virtual machine is powered off and powered on again.

For example, you create an EVC cluster that contains hosts with Intel processors and you set the EVC mode to Intel "Merom" Generation (Xeon Core 2). When you power on a virtual machine in this cluster, it runs in the Intel Merom Generation (Xeon Core 2) EVC mode. If you raise the EVC mode of the cluster to Intel "Penryn" Generation (Xeon 45 nm Core 2), the virtual machine retains the lower Intel "Merom" Generation (Xeon Core 2) EVC mode. To use the feature set of the higher EVC mode, such as SSE4.1, the virtual machine must be powered off and powered on again.

Procedure

1 Navigate to a cluster or a host in the vCenter Server inventory.

2 Click the VMs tab.

A list of all virtual machines in the selected cluster or on the selected host appears.

3 To verify the status of the CPU mode, check the EVC CPU Mode column.

a Click the angle icon next to any column title and select Show/Hide Columns > EVC CPU Mode.

The EVC CPU Mode column shows the CPU modes of all virtual machines in the cluster or on the host.

Important For each virtual machine, the EVC CPU Mode column displays the EVC mode defined at the virtual machine level.

However, if you do not configure per-VM EVC for a virtual machine, the virtual machine inherits the EVC mode of its parent cluster or host. As a result, for all virtual machines that do not have per-VM EVC configured, the EVC CPU Mode column displays the inherited EVC mode of the parent host or cluster.

If the virtual machine is in an EVC cluster, the EVC mode that you see in the EVC CPU Mode column is defined in the following manner.

- When the virtual machine is powered on, the EVC CPU Mode column displays either the per-VM EVC mode, or the cluster-level EVC mode.

Per-VM EVC	Cluster-Level EVC	EVC Mode for the Virtual Machine
Enabled	Enabled	Enabled. The EVC CPU Mode column displays the EVC mode of the virtual machine.
Disabled	Enabled	Enabled. The EVC CPU Mode column displays the EVC mode of the EVC cluster.

- When the virtual machine is powered off, the EVC CPU Mode column displays the per-VM EVC mode. If per-VM EVC is disabled, the EVC CPU Mode column for the virtual machine is empty.

When the virtual machine is not in an EVC cluster and per-VM EVC is not configured, the EVC mode that you see in the EVC CPU Mode column is defined in the following manner.

- When the virtual machine is powered on, the EVC CPU Mode column displays the EVC mode of the parent host.
- When the virtual machine is powered off, the EVC CPU Mode column is empty.

---

4 To verify the status of the graphics mode, check the EVC Graphics Mode (vSGA) column.

a Click the angle icon next to any column title and select Show/Hide Columns > EVC Graphics Mode (vSGA).

The EVC Graphics Mode (vSGA) column displays the baseline graphics features set. To view the baseline graphics, you must enable 3D graphics in the virtual machine.
For information on how to configure 3D graphics, see Configure 3D Graphics and Video Cards.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 266