Veritas Storage Foundation™ and High Availability Solutions 6.0.1 Virtualization Guide - HP-UX

September 2012

Symantec™

Veritas Storage Foundation and High Availability Solutions Virtualization Guide

Product version: 6.0.1

Document version: 6.0.1 Rev 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Contents

Chapter 1

Overview

This chapter includes the following topics:

Introduction

This document provides information about support for HP Integrity Virtual Machines (IVMs) with Veritas Storage Foundation and High Availability Solutions.

Review this entire document before installing your Veritas Storage Foundation and High Availability products in an HP IVM environment.

For information about Veritas Storage Foundation and High Availability Solutions 6.0 on HP-UX, refer to the following documentation:

- *Veritas Cluster Server Release Notes*
- *Veritas Storage Foundation Release Notes*
- *Veritas Storage Foundation Cluster File System High Availability Release Notes*
- *Veritas Cluster Server Installation Guide*
- *Veritas Storage Foundation Installation Guide*
- *Veritas Storage Foundation Cluster File System High Availability Installation Guide*

Note: Veritas Storage Foundation for Oracle RAC is not supported in an IVM environment.

HP Integrity Virtual Machines terminology

Table 1-1 describes the terminology that is helpful in configuring the Veritas software for HP Integrity Virtual Machines.

Table 1-1 Terminology

Term	Definition
Attached I/O	A device given to a virtual machine without being virtualized by the VMHost.
Shared I/O	A device on the VMHost that is virtualized and shared among different VMGuests.
VMGuest	A virtual machine with its own operating system, resources, and identity within a physical host.
VMHost	An HP Integrity Server that has virtual machines running within it. It hosts the IVM depot.
VM-PM	A Veritas Cluster Server (VCS) supported configuration in which a cluster is formed among the VMGuests and physical machines.
PM-PM	A VCS supported configuration in which a cluster is formed among the VMHosts and is used to manage VMGuests.
VM-VM	A VCS supported configuration in which a cluster is formed among the VMGuests.
Backing store	A device on the VMHost, such as a network adapter, disk, or file that is allocated to the VMGuests.
Online VM guest migration	A technology to migrate a running VMGuest and its applications from one VMHost to another without service interruption.
VSwitch	A network switch emulated in software that enables and controls network connections between the VMGuests and physical networks.
Virtual Disk	An emulated SCSI disk whose virtual media comes from a VM Host disk LUN.

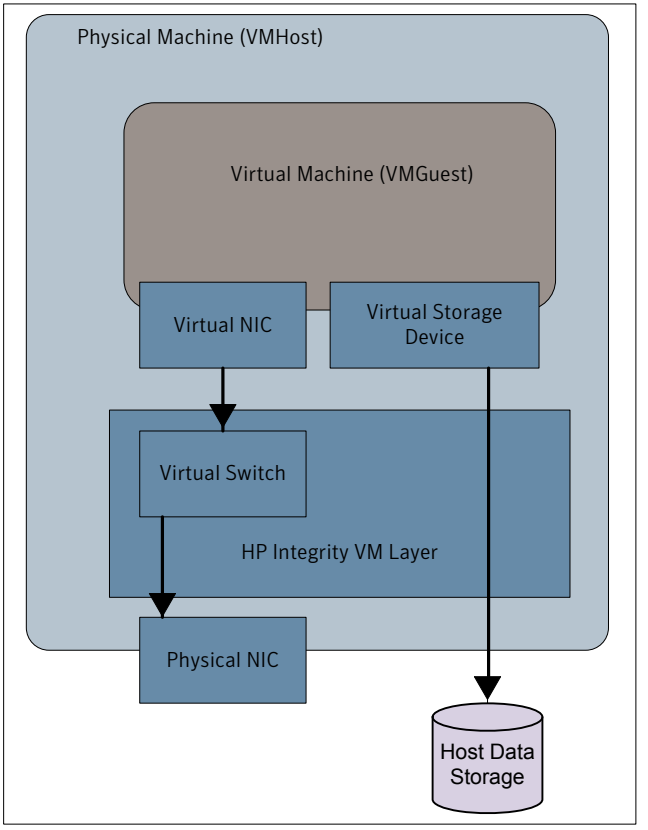
Table 1-1 Terminology *(continued)*

Term	Definition
Virtual LvDisk	An emulated SCSI disk whose virtual media is provided by a raw VM Host VxVM volume.
Virtual FileDisk	An emulated SCSI disk whose virtual media comes from a VM Host file.
Accelerated Virtual I/O (AVIO)	This new technology from HP delivers a streamlined I/O path for both storage and networking resulting in significant performance improvements for I/O workloads in an IVM environment. VCS supports both AVIO and VIO configurations for storage and networking devices in an IVM environment.

About HP Integrity Virtual Machines

HP Integrity Virtual Machines (IVMs) is a hosted hypervisor virtualization technology within the HP Virtual Server Environment, which lets you create multiple virtual servers with shared resources within a single HP Integrity server or nPartition.

Figure 1-1 HP Integrity Virtual Machines architecture



As shown in Figure 1-1, a virtual machine (VMGuest) runs within the physical machine (VMHost). The virtual machine is connected to a virtual storage device and a virtual switch (VSwitch).

For more information about virtual switches, virtual storage devices, and Integrity Virtual Machines, refer to the HP documentation.

Supported Storage Foundation and HP IVM versions

Table 1-2 describes the supported Storage Foundation (SF) and HP IVM versions.

Table 1-2 Supported SF and HP IVM versions

VMHost OS	SF on VMHost	IVM version	VMGuest OS	SF on VMGuest
HP-UX 11i v3	6.0.1	4.2	HP-UX 11i v2	5.0 MP2
		4.2	HP-UX 11i v3 March 2010	5.0, 5.0.1, 5.1 SP1, 6.0, 6.0.1
		4.3	HP-UX 11i v3 March 2011 HP-UX 11i v3 September 2011	5.0.1, 5.1 SP1, 6.0, 6.0.1

Supported VCS and IVM versions

Table 1-3 describes the VCS and supported IVM versions on the host and guest systems.

Table 1-3 Supported VCS and HP IVM versions

VMHost OS	VCS on VMHost	IVM version	VMGuest OS	VCS on VMGuest	Supported Configuration
HP-UX 11i v3	6.0.1	4.2	HP-UX 11i v2	5.0 MP2	■ PM-PM See "Cluster among VMHosts (PM-PM) " on page 28.
		4.2	HP-UX 11i v3	5.0.1, 5.1 SP1	■ PM-PM See "Cluster among VMHosts (PM-PM) " on page 28.
		4.2	HP-UX 11i v3	6.0, 6.0.1	■ VM-VM See "Cluster among VMGuests (VM-VM)" on page 20. ■ VM-PM See "Cluster among VMGuests and physical machines (VM-PM)" on page 24. ■ PM-PM See "Cluster among VMHosts (PM-PM) " on page 28.
		4.3	HP-UX 11i v3 March 2011 HP-UX 11i v3 September 2011	6.0, 6.0.1	■ VM-VM See "Cluster among VMGuests (VM-VM)" on page 20. ■ VM-PM See "Cluster among VMGuests and physical machines (VM-PM)" on page 24. ■ PM-PM See "Cluster among VMHosts (PM-PM) " on page 28.

Chapter 2

Supported configurations

This chapter includes the following topics:

Supported configurations using IVM

Storage Foundation and High Availability supports various combinations of physical machines (VMHost) and virtual machines (VMGuest) running within the physical machines. You can install Veritas Storage Foundation and High Availability Solutions and Veritas Storage Foundation Cluster File System HA (SFCFSHA) either on the VMHost or on the VMGuest or on both. VMGuests, support both single-node and multiple-node high availability configurations.

Table 2-1 shows the support matrix for the various deployment models.

Table 2-1 Supported configurations using IVM

		Deployment on the VMGuest			
Deployment on the VMHost/ backend device		SF on VMGuest	SFHA on VMGuest	SFCFSHA on VMGuest	SF not installed on VMGuest
	SF on VMHost	Supported See Figure 2-3 on page 19.	Not Supported	Not Supported	Supported See Figure 2-2 on page 18.
	SFHA on VMHost	Supported See Figure 2-16 on page 31.	Not Supported	Not Supported	Supported See Figure 2-15 on page 30.
	SFCFSHA on VMHost	Not Supported	Not Supported	Not Supported	Not Supported
	Whole Disk on VMHost (SF is not used)	Supported See Figure 2-1 on page 17.	Supported* See Figure 2-8 on page 23.	Supported* See Figure 2-17 on page 33.	Not applicable

Warning: * Indicates that these configurations are supported with fencing disabled.

The following sections describe the deployment models for SF, SFHA, and SFCFSHA supported configurations using IVM.

SF — See "Storage Foundation supported configurations using IVM" on page 16.

SFHA — See "Storage Foundation High Availability supported configurations using IVM" on page 19.

SFCFSHA — See "Storage Foundation Cluster File System High Availability supported configurations using IVM" on page 32.

Storage Foundation supported configurations using IVM

Symantec recommends the following deployment models:

SF on VMGuest only See "SF on VMGuest only" on page 17.

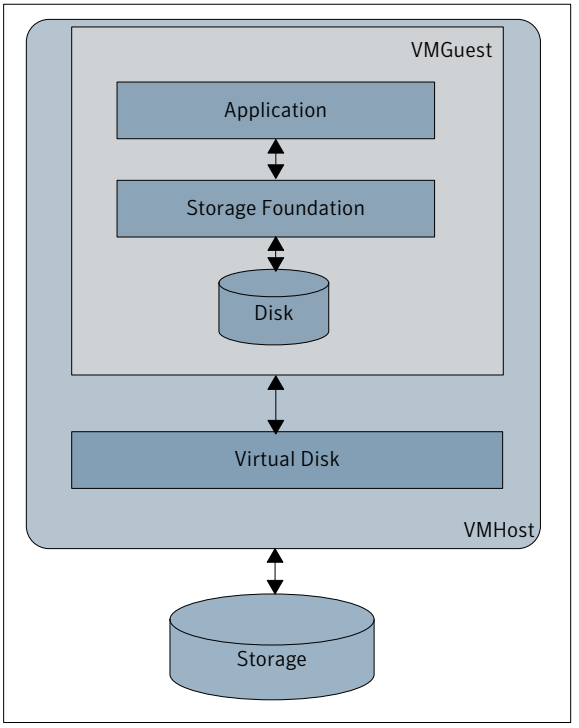
SF on VMHost only See "SF on VMHost only" on page 17.

SF on both VMGuest and VMHost See "SF on both VMGuest and VMHost" on page 18.

SF on VMGuest only

Figure 2-1 shows a deployment in which SF is installed on the VMGuest and whole disk is exported to the VMGuest from the VMHost.

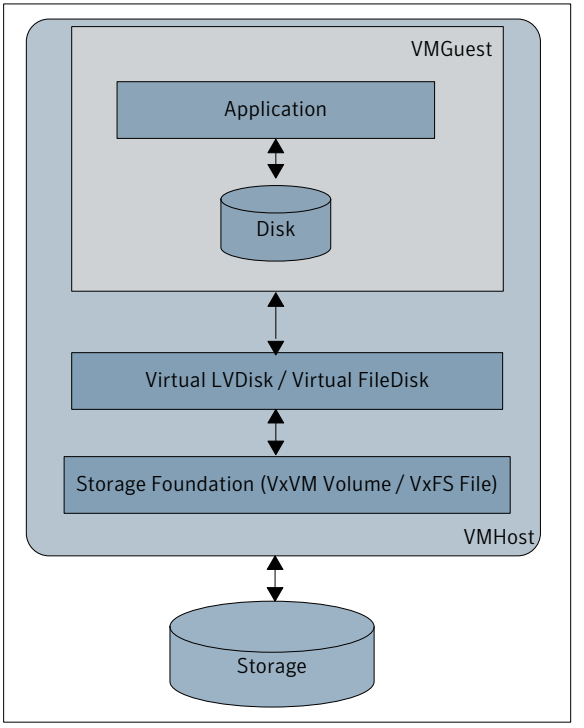
Figure 2-1 SF on VMGuest only



SF on VMHost only

Figure 2-2 shows a deployment in which SF is installed on the VMHost. The VMHost can export VxVM volumes or VxFS files as virtual disks to the VMGuest.

Figure 2-2 SF on VMHost only



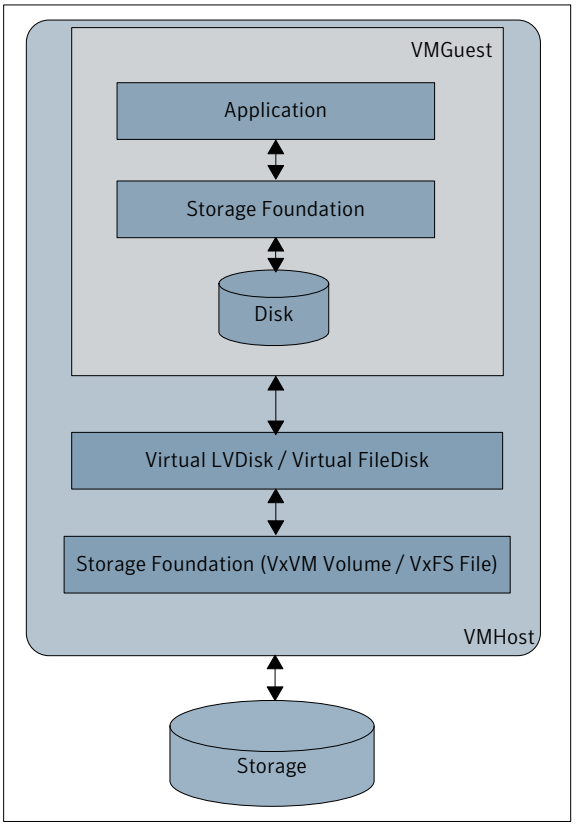
Advantages of using a VMHost-based Storage Foundation stack

- DMP is centralized in the VMHost. As a result, the VMHost performs all the multi-pathing operations using DMP.
- The VMHost performs all the storage provisioning for the VMGuest using VxVM volumes and VxFS Files.

SF on both VMGuest and VMHost

Figure 2-3 shows a deployment in which SF is installed on both VMGuest and VMHost. The VMHost can export VxVM volumes or VxFS files as virtual disks to the VMGuest.

Figure 2-3 SF on both VMGuest and VMHost



Storage Foundation High Availability supported configurations using IVM

Storage Foundation High Availability (SFHA) supports the following configurations using IVM:

- Cluster among VMGuests (VM-VM)
  A cluster is formed among VMGuests. The VMGuests can be on the same VMHost or on different VMHosts. VCS is installed on the VMGuests.
  In this configuration, VCS manages the applications running within the VMGuests.
  See "Cluster among VMGuests (VM-VM)" on page 20.

Note: For failover of VMGuests, refer to the PM-PM configuration.

- Cluster among VMGuests and physical machines (VM-PM)
  A cluster is formed among VMGuests and physical machines. VCS is installed on the VMGuests and physical machines.
  This configuration is a typical VCS application clustering.
  See "Cluster among VMGuests and physical machines (VM-PM)" on page 24.
- Cluster among VMHosts (PM-PM)
  The VMHosts form a cluster. In this configuration, VCS does not monitor applications running within VMGuests.
  See "Cluster among VMHosts (PM-PM) " on page 28.

Cluster among VMGuests (VM-VM)

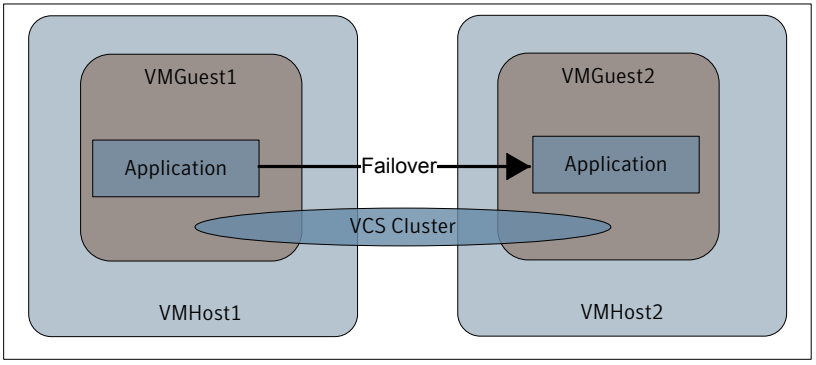
The following configurations are supported:

- Cluster among VMGuests on two different VMHosts
  See "Cluster among VMGuests on two different VMHosts" on page 20.
- Cluster among VMGuests on the same VMHost
  See "Cluster among VMGuests on the same VMHost" on page 21.

Cluster among VMGuests on two different VMHosts

Figure 2-4 shows a configuration in which a cluster is formed between two VMGuests on different VMHosts.

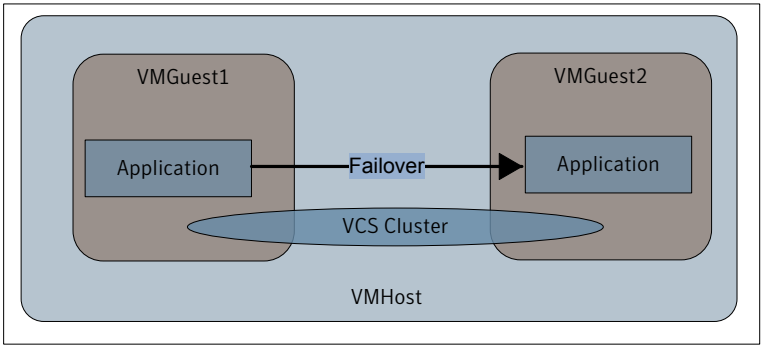
Figure 2-4 VCS cluster between VMGuests on two different VMHosts



Cluster among VMGuests on the same VMHost

Figure 2-5 shows a configuration in which a cluster is formed between two VMGuests on the same VMHost. This configuration is not generally recommended because it introduces a single point of failure.

Figure 2-5 VCS cluster between VMGuests on the same VMHost



I/O fencing support

Non-SCSI3, CP server based fencing is supported.

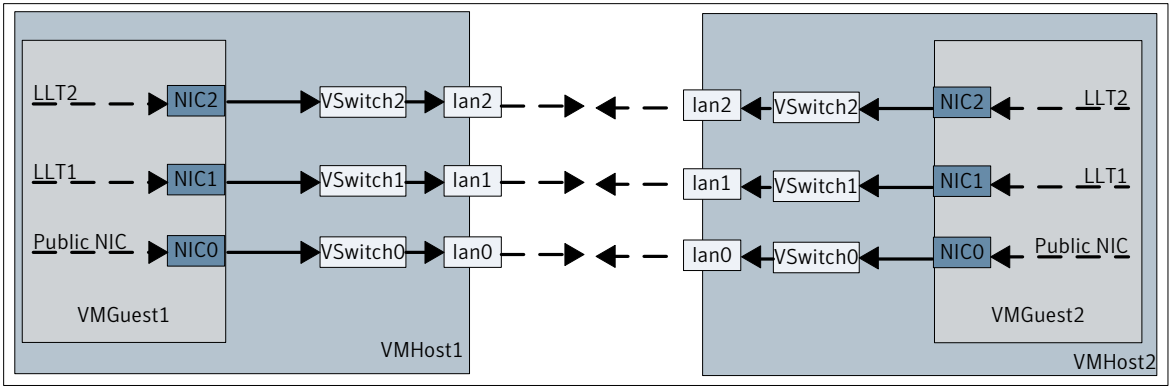
SCSI3 fencing is not supported.

Network configuration

This section describes the network considerations for a VM-VM cluster.

Figure 2-6 shows a cluster between VMGuest1 and VMGuest2.

Figure 2-6 Network configuration for a VM-VM cluster



VMHost1 and VMHost2 have three physical network interface cards (NICs). lan0 is a public NIC, and lan1 and lan2 are private NICs. The private NICs of VMHost1 and VMHost2 are connected to each other through private heartbeat links.

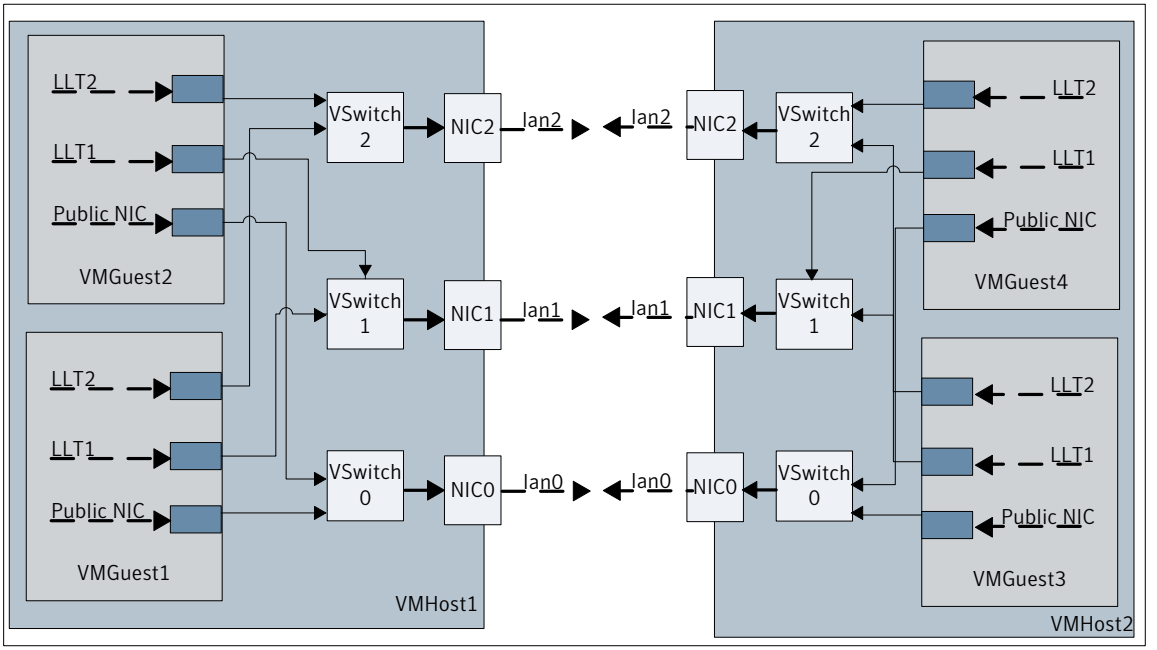
The network connections for VMGuest1 are as follows:

- A virtual switch VSwitch0 is mapped to the public physical NIC lan0 on VMHost1. A virtual NIC, NIC0 on VMGuest1, is connected to VSwitch0.
- A virtual switch VSwitch1 is mapped to the private physical NIC, lan1 on VMHost1. A virtual NIC named NIC1 on VMGuest1 is connected to VSwitch1.
- A virtual switch VSwitch2 is mapped to another private physical NIC lan2 on VMHost1. A virtual NIC named NIC2 is connected to VSwitch2.

Set up public and private heartbeat network connections for VMGuest2 on the other node in a similar manner. The VSwitch names can be different on both the cluster nodes.

Figure 2-7 shows the network configuration for multiple VMGuests.

Figure 2-7 Cluster among multiple VMGuests

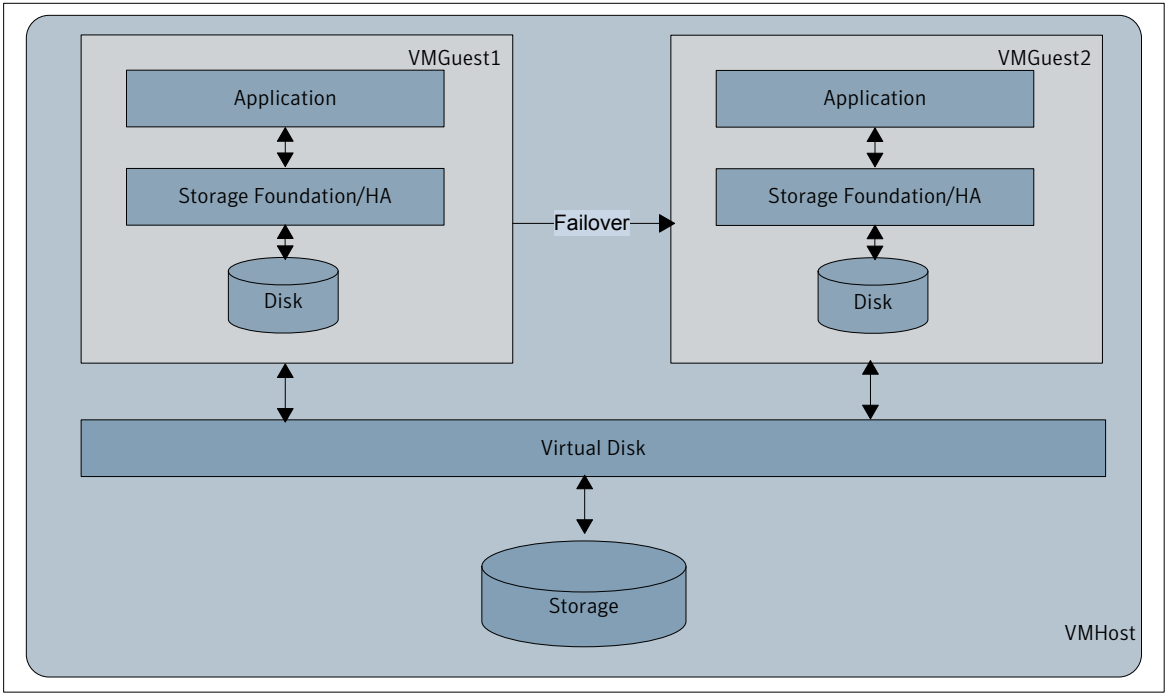


Storage configuration

Figure 2-8 shows a deployment in which SFHA is installed only on the VMGuest and whole disk is exported from the VMHost.

Warning: Data corruption can occur because fencing is disabled.

Figure 2-8 SFHA on the VMGuest only



In this scenario, you can migrate the VxVM disk group from the physical environment to the virtual environment (P2V).

See "Migrating a Veritas Volume Manager diskgroup from a physical environment to a virtual environment (P2V)" on page 43.

Setting up VMGuests for a VM-VM configuration

Following is a high-level overview for setting up VMGuests. For detailed instructions, refer to HP documentation.

To set up VMGuests

- Ensure that CPU and memory resources are available on the VMHosts.

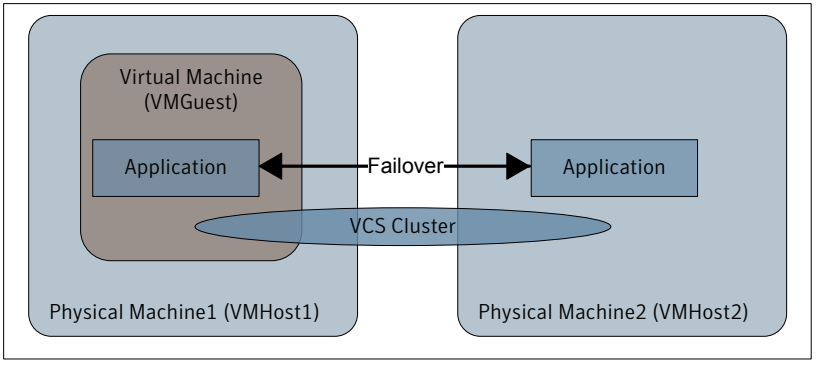
- Install the HP Integrity VM depot on the VMHosts.
- Create virtual switches to enable networking for VMGuests.
- Ensure that backing storage is available for VMGuests.
- Create VMGuests.
- Install the operating system in the VMGuests.
- Repeat the above steps for all the VMGuests in the cluster.
- Install VCS on all the VMGuests. For information about installing VCS, refer to the *Veritas Cluster Server Installation Guide*.
- Configure the resources that you want VCS to manage.
- If you intend to use the online VM guest migration feature, Symantec recommends that you set the VCS_GAB_TIMEOUT value in the /opt/VRTSvcs/bin/vcsenv file on all the VMGuests. This will prevent the VCS engine from missing heartbeats with GAB on a loaded system during migration.

```
VCS_GAB_TIMEOUT=30000
export VCS_GAB_TIMEOUT
```

Cluster among VMGuests and physical machines (VM-PM)

Figure 2-9 shows a cluster between a VMGuest and a physical machine. VCS is installed on the virtual machine and the physical machine.

Figure 2-9 A VM-PM cluster



Note: Symantec recommends that physical machines should not host any virtual machines.

I/O fencing support

Non-SCSI3, CP server based fencing is supported.

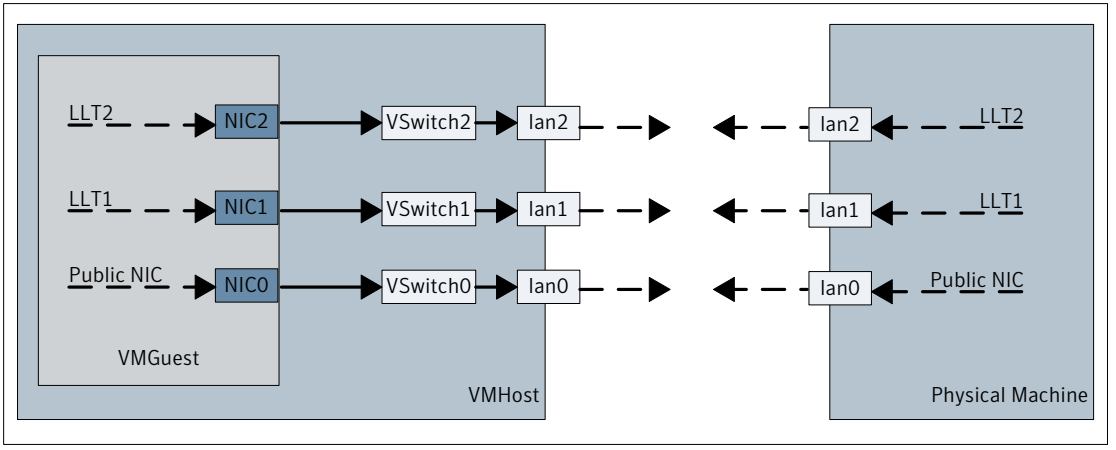
SCSI3 fencing is not supported.

Network configuration

The network connection for the physical machine is similar to any other node in a VCS cluster. The VMGuest is connected to the physical machine through VSwitches and a physical NIC on its VMHost.

Figure 2-10 shows the network configuration for a VM-PM configuration.

Figure 2-10 Network configuration for a VM-PM configuration

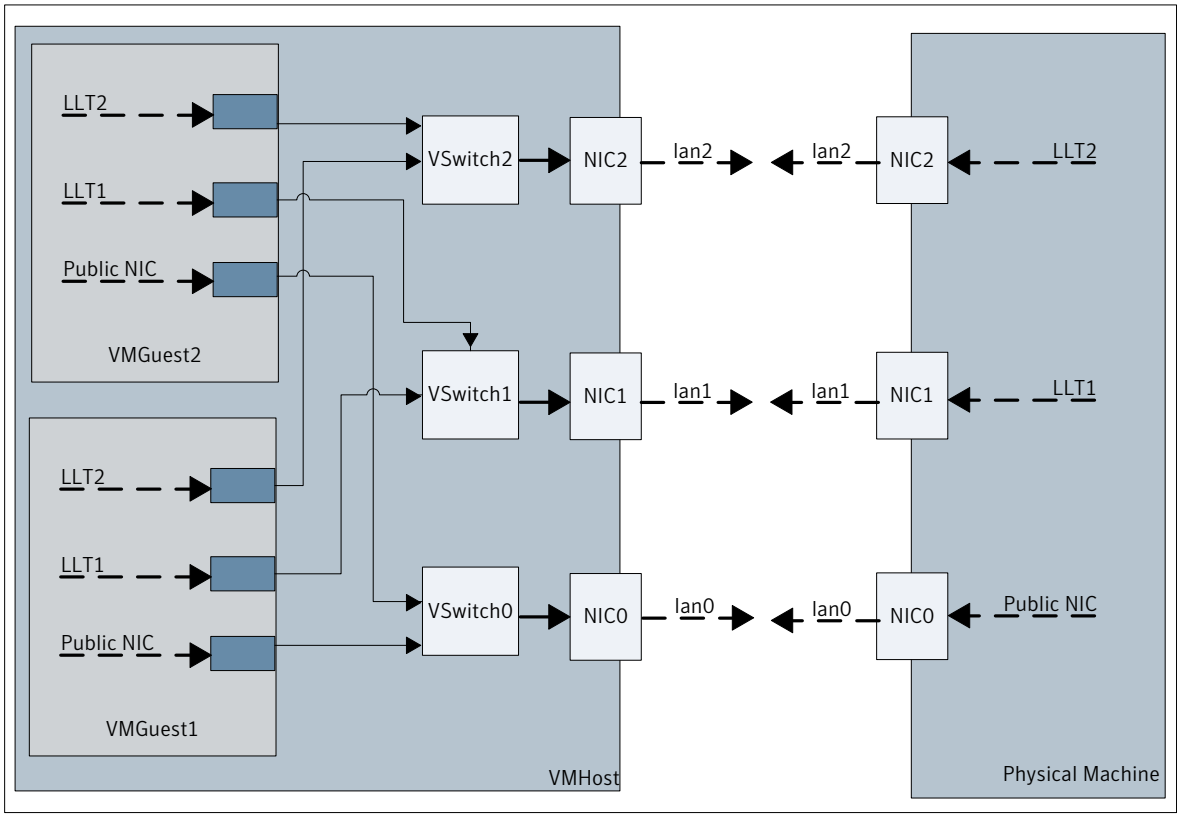


The network connections for the VMGuest are as follows:

- A virtual switch VSwitch0 is mapped to public physical NIC lan0 on VMHost. A virtual NIC, NIC0 on VMGuest is connected to VSwitch0.
- A virtual switch Vswitch1 is mapped to the private NIC lan1 on VMHost. A virtual NIC, NIC1 on VMGuest is connected to VSwitch1.
- A virtual switch Vswitch2 is mapped to the private NIC lan2 on VMHost. A virtual NIC, NIC2 on VMGuest is connected to VSwitch2.

Figure 2-11 shows the network configuration consisting of a physical machine and two VMGuests on the same VMHost.

Figure 2-11 Network configuration for two VMGuests

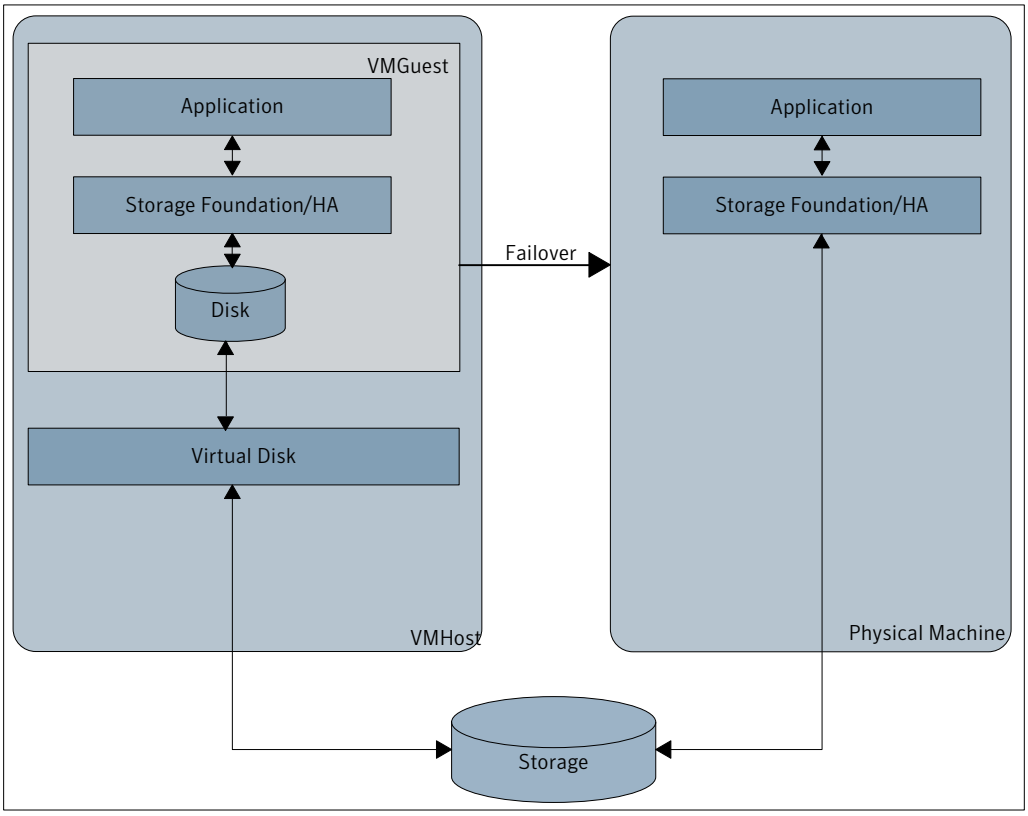


Storage configuration

A raw disk backing store is supported for VMGuests in the VM-PM cluster. A whole disk can be provided to the virtual machine. If the disk contains a private disk group, it will also be visible from within the VMguest.

Figure 2-12 shows the storage configuration for a VM-PM setup.

Figure 2-12 Storage configuration for a VM-PM setup



Note: The VM-PM configuration does not support CVM backing stores.

Setting up a VM-PM cluster

Following are the high-level steps for setting up a VM-PM cluster. For detailed instructions, refer to HP documentation.

To set up a VM-PM cluster

- Ensure that CPU and memory resources are available on the VMHosts.
- Install the HP Integrity VM depot on the VMHosts.
- Create virtual switches to enable networking for VMGuests.
- Ensure that backing storage is available for VMGuests.
- Create the VMGuests.

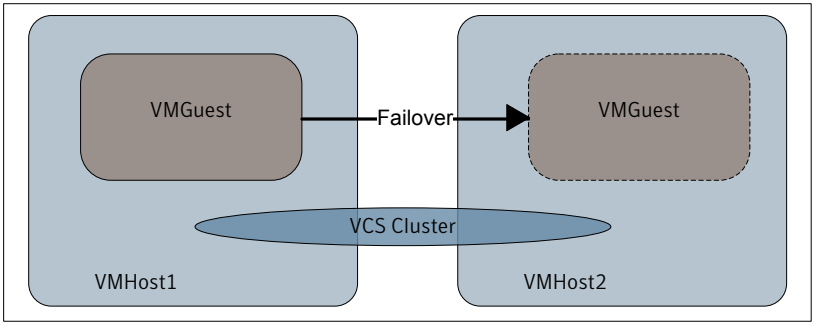
- Install the operating system in the VMGuests.
- Repeat the above steps for all the VMGuests in the cluster.
- Install VCS on all the physical machines and VMGuests which are to be part of the cluster. For information about installing VCS, refer to the *Veritas Cluster Server Installation Guide*.
- Configure the resources that you want VCS to manage.

Cluster among VMHosts (PM-PM)

In this configuration, VCS manages a VMGuest as a resource.

Figure 2-13 shows a VCS cluster between VMHost1 and VMHost2.

Figure 2-13 A PM-PM configuration



If the VMGuest on one of the VMHost faults, it is failed over to the other VMHost.

For a successful failover of VMGuests across the VMHosts in a cluster, ensure that the VMGuests are configured consistently for the following attributes:

- VMGuest name
- VSwitch configuration
- Backing storage configuration

The storage for the VMGuests must be accessible to all the VMHosts in the cluster.

VCS includes two new bundled agents, HPVirtualMachine agent and HPVSwitch agent. The HPVirtualMachine agent manages the VMGuests and the HPVSwitch agent manages the virtual switch.

See "Bundled agents for IVM to be used in a PM-PM configuration" on page 32.

I/O fencing support

SCSI3 fencing is supported.

In the event of a network partition, I/O fencing will panic VMHosts in one sub-cluster. This will cause all the VMGuests getting failed over to the VMHosts in the surviving sub-cluster.

Network and storage considerations

The network configuration and storage configuration for the VMHosts is the same as the nodes in VCS cluster configurations.

For information on configuring VCS, refer to the *Veritas Cluster Server Installation Guide*.

Figure 2-14 shows the network and storage organization for the PM-PM configuration.

Figure 2-14 Network and storage organization for the PM-PM configuration

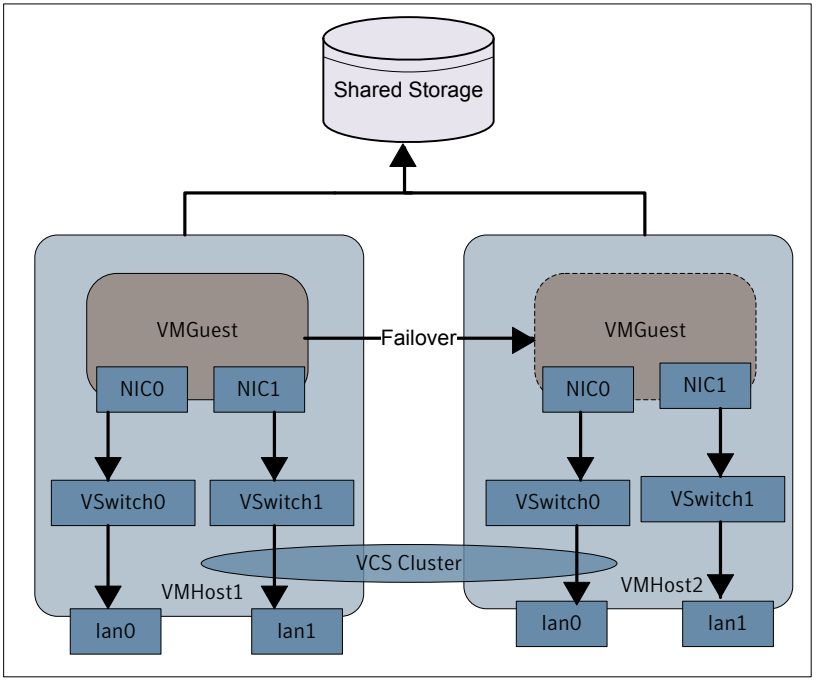


Figure 2-15 shows a deployment in which SFHA is installed only on the VMHost and VxVM volume or VxFS files are exported to the VMGuest as Virtual disks. VCS monitors the virtual machines and their associated or dependent SF resources.

Figure 2-15 SFHA on the VMHost only

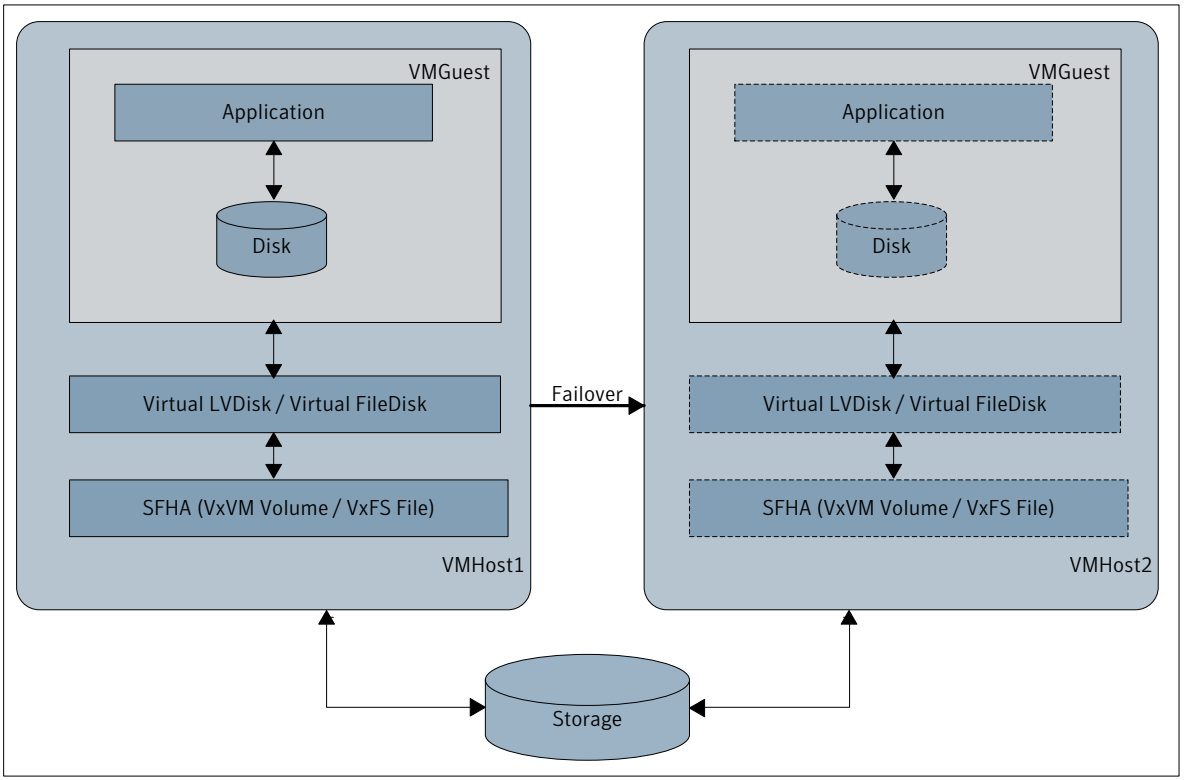
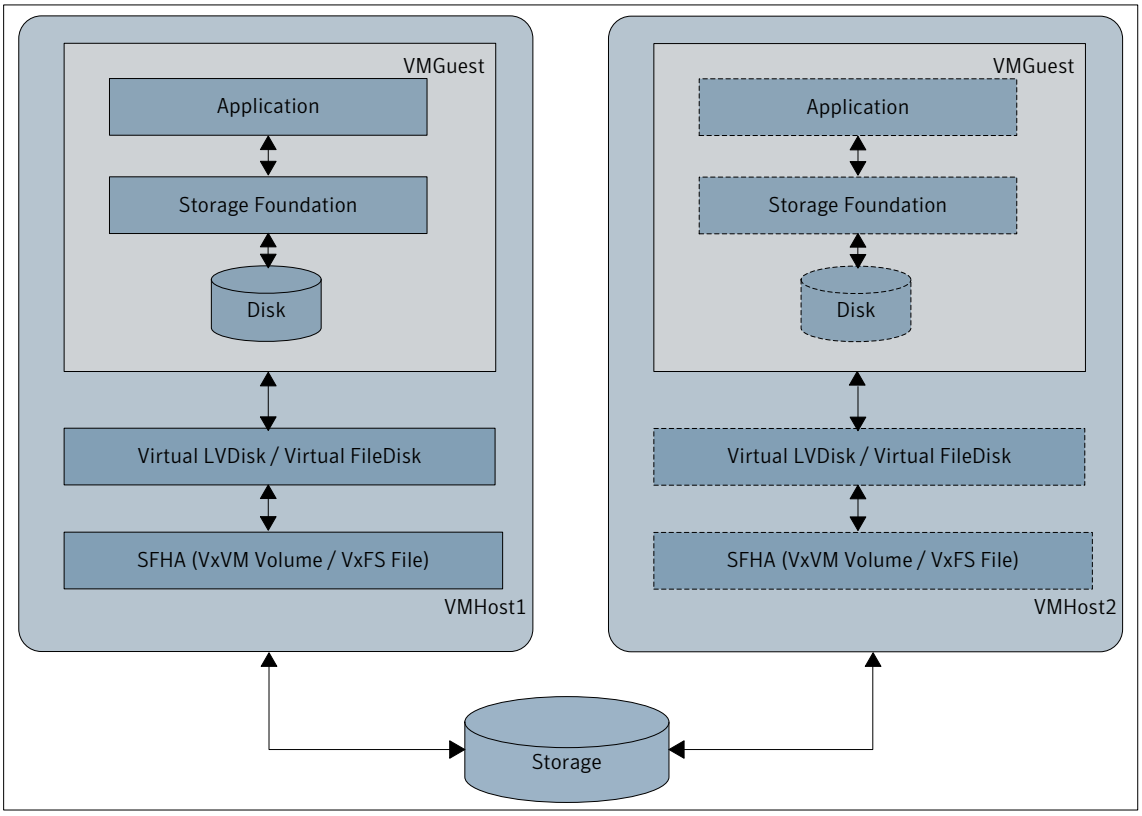


Figure 2-16 shows a configuration in which VMHosts form a VCS cluster and SF is installed in the VMGuest. VMHost can export a VxVM volume or VxFS file to the VMGuest. VCS monitors the VMGuests and its associated or dependent SF resources.

Figure 2-16 SF on VMGuest and SFHA on VMHost



VCS also supports a whole disk as a backing store to the VMGuest. The whole disk must be exported as a virtual disk to the VMGuest.

Setting up VMGuests for the PM-PM configuration

Following is an overview for setting up the VMGuests. For detailed instructions, refer to HP documentation.

To set up VMGuests

- Ensure that CPU and memory resources are available on the VMHosts.
- Install the HP Integrity VM depot on the VMHosts.
- Create virtual switches to enable networking for VMGuests.
- Ensure that backing storage is available for VMGuests.
- Create VMGuests.

- The backing storage for the VMGuest must be accessible to all the VMHosts in the cluster.
- Configure the resources that you want VCS to manage.

Bundled agents for IVM to be used in a PM-PM configuration

The following agents are used to manage VMGuests running on VMHosts.

- HPVirtualMachine agent
- HPVSwitch agent

Note: The HPVirtualMachine agent does not wait for the operating system to load completely. The agent reports the state of the resource as ONLINE immediately after the operating system starts booting.

For information on these agents, refer to the *Veritas Cluster Server Bundled Agents Reference Guide*.

Storage Foundation Cluster File System High Availability supported configurations using IVM

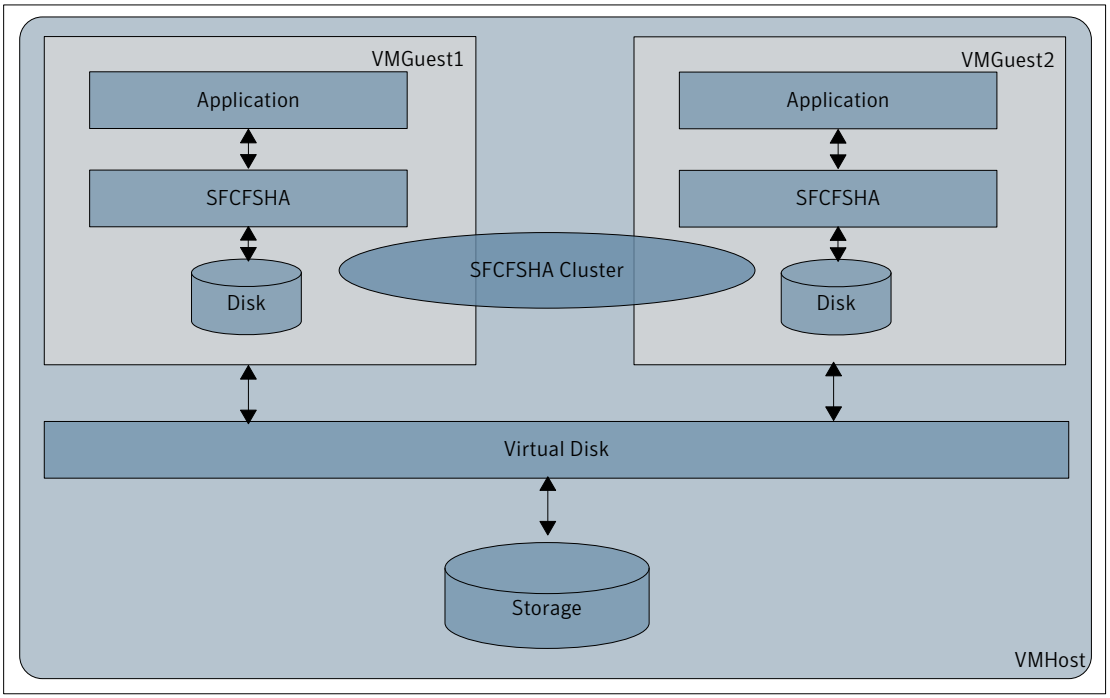
This section explains the deployment models for Veritas Storage Foundation Cluster File System High Availability.

SFCFSHA on VMGuest only

Figure 2-17 shows a deployment in which SFCFSHA is installed only on the VMGuest and the whole disk is exported from the VMHost.

Warning: Data corruption can occur as fencing is disabled.

Figure 2-17 SFCFSHA on VMGuest only



Chapter 3

Migrating virtual machine in VCS environment

This chapter includes the following topics:

About migrating Virtual Machine in VCS environment

VCS supports live or online migration, also known as Virtual Machine Migration for HP Integrity Virtual Machines (IVM). Online migration enables a running guest and its applications to be moved from one VM Host to another without service interruption. All guest I/O connections to storage and networks remain active throughout the online migration, and the guest and all its applications continue operating without a reboot or an application restart.

The basic virtual machine migration environment includes a source machine and a target machine. Both the machines must:

- Run Integrity VMs and must be able to run the guests.
- Conform to their operating system requirements and restrictions.
- Provide the allocated resources to the guest.

With the `hpvmmigrate` command, you can move the following to a target VM Host system:

- An offline or non-running virtual machine (offline migration)
- A live and online virtual machine (online migration) running a guest operating system
- Applications from a source VM Host system

For offline migration, you can use the `hpvmmigrate` command on HP Integrity Virtual Machines Version 1.2 and later. The Online VM Migration feature for online guests is available starting with HP Integrity Virtual Machine Version 4.2.

Reasons for VM migration

Online migration:

- Vacating a VM Host system: With Online VM Migration, you can migrate all your guests from a VM Host to one or more other VM Hosts without interrupting the workload activity on the guests. A common reason to do this operation is for the maintenance of the VM Host system, such as hardware, firmware, or software.
- Targeting a particular VM Host: You might also want to migrate an active guest workload to a particular VM Host to take advantage of a particular resource or feature on that target VM Host without losing application availability.
- Balancing VM Host workloads: You might want to segregate guests to balance the workload on VM Hosts. Perhaps, you may also want to group workloads together that have similar special resource requirements.
- Optimizing physical resource utilization: You can conveniently "park" idle, near-idle, or just currently less-critical guest workloads together on a smaller or less powerful machine.

Offline migration:

- The guest might have stopped, so you need to move the configuration information offline.
- Migrating the virtual machine offline does not use the VMHost resources (like memory and CPUs) on the source and target VM Hosts.

- The source and target VM Hosts might have different processor types that prevent online migration.
- The source VMHost might be running a version of Integrity VM prior to Version 4.2, which does not support Online VM Migration.
- You can offline migrate guests between different processor families.

Prerequisites for Virtual Machine Migration

VCS requirements:

- Verify that the value of IntentionalOffline attribute for HPVirtualMachine type is set to 1. (The default value is 1.)
- Make sure that the HPVirtualMachine resource for the VMGuest that you plan to migrate is in a steady state OFFLINE or ONLINE.
- To rename the VMGuest when you migrate it, make sure that the VMName attribute for the HPVirtualMachine resource in VCS is localized with the target VMGuest name for the target VMHost system. When you rename it, VCS can continue to monitor the renamed VMGuest after migration.

IVM Requirements:

- Enable password-less SSH between source and target hosts for superuser.
- Make sure that you do not create VMGuest on the target VMHost if you are migrating for the first time.
- The source VMHost and the target VMHost must be running Integrity VM (IVM) and must be able to run the guests.
- Both machines must be able to provide the allocated resources to the guest. For example, if the guest uses 2-GB memory on one machine, it must be able to use the same amount of memory on the other machine. Similarly, if the source machine can provide a guest with four vCPUs, then the target machine must also be able to provide the same number of vCPUs.
- All resources used by the guest must be configured symmetrically on both the source and target VMHosts. A symmetric configuration includes:
  - A common local area network (LAN)
  - Identical subnet and vSwitch connectivity

Note: Create virtual switch (public/private) with the same name in the servers which you want to host the GuestVM.

- Common access for Storage Area Network (SAN) based storage, such as RAW Disk, CVM/CFS, NFS exported storage.

Refer to the following references in HP Integrity VM documentation for more information:

- For more details on migration requirments refer to *Migrating Virtual Machines of HP Integrity Virtual Machines Installation, Configuration and Administration guide*.
- For IVM Installation Requirements refer to *Installation Requirements of HP Integrity Virtual Machines Installation, Configuration and Administration guide*.

Supported deployment models for Virtual Machine migration with VCS

The following are the supported deployment models for HP Integrity Virtual Machine migration with VCS:

- Migrating VMGuest when VCS is installed in the VMHost that manages the guest domain (PM-PM)
- Migrating VMGuest when VCS is installed in the VMHost system and single-node VCS is installed inside the VMGuest system to monitor applications inside the VMGuest. (PM-PM with single-node VCS in VMGuest)
- Migrating VMGuest when VCS is installed in the VMGuests to manage applications (VM-VM)

Migrating VMGuest when VCS is installed in the VMHost that manages the guest domain (PM-PM)

To perform a Live migration when you have VCS installed in the VMHost that manages the VMGuest.

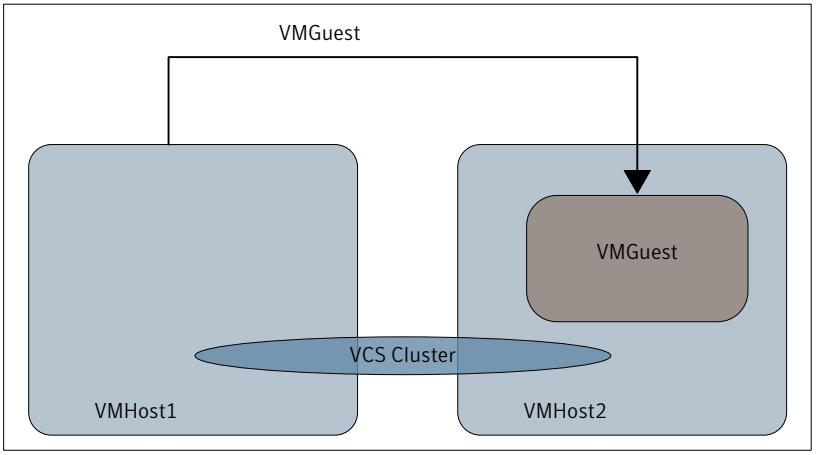
Use the `hpvmmigrate` command for migration:

For example:

```
hpvmmigrate -o -P VMGuest -h VMHost2
```

For further options to `hpvmmigrate` command, please refer to the `hpvmmigrate` man page.

Figure 3-1 Migration of VMGuest from VMHost1 to VMHost2 with cluster between VMHosts



Migrating VMGuest when VCS is installed in the VMHost and single-node VCS is installed inside the VMGuest to monitor applications inside the VMGuest

Use the `hpvmmigrate` command for migration to perform a migration when:

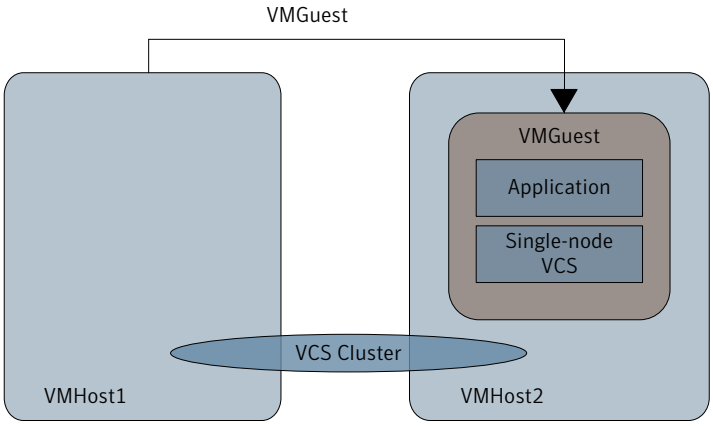
- VCS is installed in the VMHost system
- VMHost is managing an application in the VMGuest
- Single-node VCS installed in the VMGuest monitors the application in VMGuest

For example:

```
hpvmmigrate -o -P VMGuest -h VMHost2
```

For further options to the `hpvmmigrate` command, please refer to the `hpvmmigrate` man page.

Figure 3-2 Migration of VMGuest from VMHost1 to VMHost2 with single node VCS monitoring applications in VMGuest



Migrating VMGuest when VCS is installed in the VMGuests to manage applications

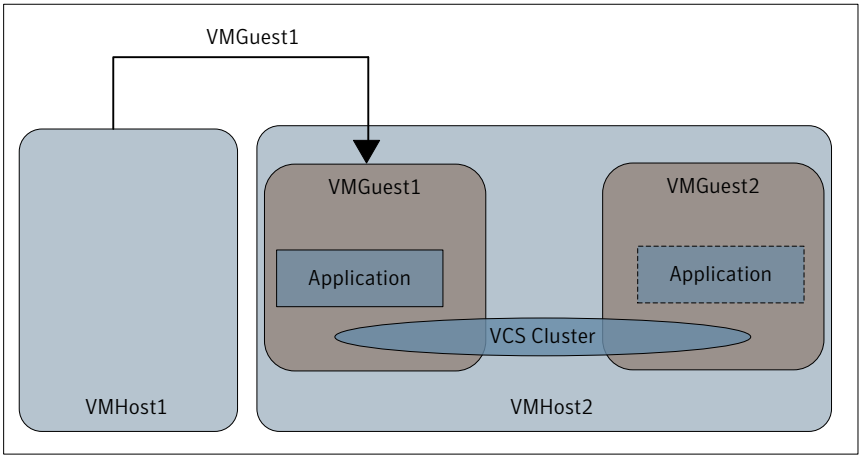
Use the `hpvmmigrate` to migrate the VMGuest when VCS cluster is configured between VMGuests to manage the applications in the VMGuests.

For example:

```
VMHost1# hpvmmigrate -P VMGuest1 -h VMHost2
```

For further options to the `hpvmmigrate` command, please refer to the `hpvmmigrate` man page.

Figure 3-3 Migration of VMGuest1 from VMHost1 to VMHost2 with cluster between VMGuests



Chapter 4

Migrating a Veritas Volume Manager diskgroup

This chapter includes the following topics:

Migrating a Veritas Volume Manager diskgroup from a physical environment to a virtual environment (P2V)

You can migrate the Veritas Volume Manager disk group from the physical environment to the virtual environment (P2V).

Warning: If you use a Cross Platform Data Sharing (CDS) disk group on the physical server, you must migrate the data to a non-CDS disk group.

To execute the P2V migration:

1. Stop all the applications on the physical server.
2. Unmount any file systems which belong to the disk group that is being migrated.
3. Deport the disk group from the VMHost using the vxdg deport command:

   ```
   # vxdg deport dgname
   ```

4. Export all the disks which are a part of the disk group to the VMGuest.

5 Rescan the devices on the VMGuest using the following command

```
# ioscan -fnC disk
```

6 Rescan the devices under Volume Manager using the following command

```
# vxdisk scandisks
```

7 Import the disk group on the VMGuest using the vxdg import command:

```
# vxdg import dgname
```

8 Mount the file systems which are part of the volumes in the diskgroup.

9 Start the applications on the VMGuest.

Chapter 5

Limitations

This chapter includes the following topics:

Limitation with VM migration in VCS environment

- Migration when a cluster between VMHost and VMGuest is formed (PM-VM configuration), is not supported.

Limitations with SF on VMGuests

- The Cross Platform Data Sharing (CDS) feature is enabled by default. The HP VMGuest does not support CDS. This restriction renders some of the CDS related features unusable. The CDS feature relies on SCSI mode sense data from the backend disk. HP IVM virtualizes the backend devices. As a result, the actual mode sense data is not available in the VMGuest. To create a VxVM disk group in the IVM environment, disable the CDS feature before creating a new diskgroup. To disable CDS, edit the `/etc/default/vxdg` file, and set the attribute-value pair cds=*off*. Alternatively, you can use the following command to set this attribute for a disk group:

  ```
  # vxdg -g diskgroup set cds=on|off
  ```

Note: To migrate from a non-HP IVM environment to an HP IVM environment using CDS disk groups, migrate all the CDS disk groups to non-CDS disk groups. This migration involves data movement.

- The VMGuest does not support the Enclosure Based Naming scheme (EBN) feature. As a result, some features like the following are not supported:
  - Enclosure information is not available in the VMGuest. Therefore, all LUNs are claimed under the DISKS category.
  - Mirroring across enclosures is also not supported.
- SCSI-3 PGR-based I/O Fencing is not supported in the VMGuest. CFS is only supported when fencing is disabled. HP IVM does not support SCSI-3 PGR in the VMGuest for virtualized disks. However, Non-SCSI-3 Fencing with CP Server is supported.

Limitations with SF on VMHosts

- VxFS drivers in the VMGuest cannot currently interact with the VxVM drivers in the VMHost. In such a configuration, some features like the following, which require direct VxVM-VxFS coordination, are rendered unusable:
  - Before taking a data consistent snapshot of a VxVM volume containing a VxFS file system, you must shut down the application and unmount the filesystem.
  - The resize operation on a filesystem on the VMGuest with an underlying device that is backed by a VxVM volume in the VMHost, has some restrictions. You must separately resize the VxVM volume and the filesystem in the VMGuest.
  - The grow operation on a VxFS file system in the VMGuest with an underlying device that is backed by a VxVM volume, has restrictions. You must first grow the volume in the VMHost using the vxassist(1m) command. You can then grow the file system in the VMGuest using the `fsadm` command.
  - To shrink a VxFS file system, you should first shrink the file system in the VMGuest and then shrink the volume in the VMHost. To shrink the filesystem use the `fsadm` command. To shrink the volume, use the vxassist(1m) command.
- You cannot export a volume set to the VMGuest.
- SmartSync features functioning at the file-level are not supported.

Limitations with VCS on VMGuests

- The VM-VM configuration does not manage VMGuests failovers as VCS is running within the VMGuests.
- SCSI3 I/O fencing is not supported in the VMGuest as SCSI3 PGR is not available inside the VMGuests. However, Non-SCSI3 fencing is supported.
- HPVSwitch agent does not manage virtual NIC on the VMGuest.
- The agent cannot detect if the operating system running in the guest hangs. Even if the HPVirtualMachine reports the VMGuest state as ONLINE, it does not mean that the OS running within the guest is functioning properly.

Limitations with VCS on VMHosts

- Controlling applications running within VMGuests is not possible in a PM-PM configuration without single-node VCS in the VMGuest.