

# Veritas Storage Foundation™ and High Availability Solutions Application Note: Support for HP-UX Integrity Virtual Machines

HP-UX 11i v3

5.1 Service Pack 1



# Veritas Storage Foundation™ and High Availability Solutions Application Note: Support for HP-UX Integrity Virtual Machines

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.1 SP1

Document version: 5.1SP1.2

## Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 website at the following URL:

[www.symantec.com/business/support/index.jsp](http://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](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportolutions@symantec.com</a>

## Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

<https://sort.symantec.com/documents>

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](mailto: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>

# Veritas Storage Foundation™ and High Availability Solutions Support for HP-UX Integrity Virtual Machines

This document includes the following topics:

- [Introduction](#)
- [HP Integrity Virtual Machines terminology](#)
- [About HP Integrity Virtual Machines](#)
- [Supported Storage Foundation and HP IVM versions](#)
- [Supported VCS and IVM versions](#)
- [Supported configurations using IVM](#)
- [Storage Foundation supported configurations using IVM](#)
- [Storage Foundation High Availability supported configurations using IVM](#)
- [Storage Foundation Cluster File System supported configurations using IVM](#)
- [Migrating a Veritas Volume Manager diskgroup from a physical environment to a virtual environment \(P2V\)](#)
- [Advantages of using a VMHost-based Storage Foundation stack](#)

- [Limitations with SF on VMGuests](#)
- [Limitations with SF on VMHosts](#)
- [Limitations with VCS on VMGuests](#)

## 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 the Veritas Storage Foundation and High Availability products on HP-UX 11i v3, refer to the following documentation:

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

You can download these documents from: <https://sort.symantec.com/documents>

---

**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.

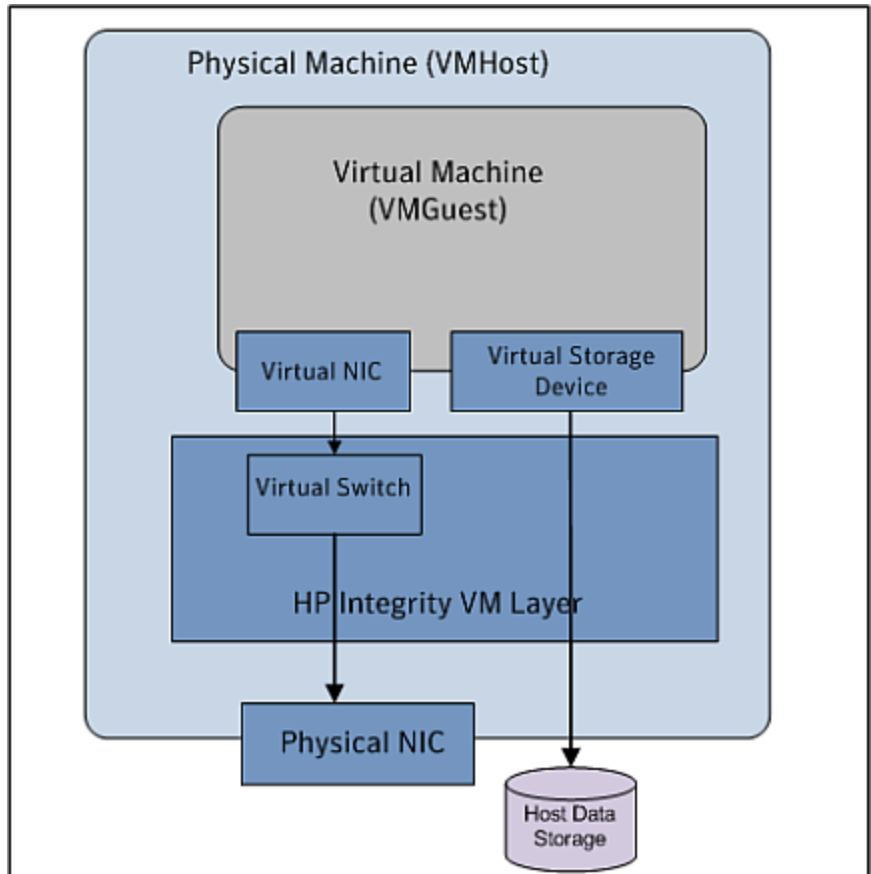
**Table 1-1** Terminology (*continued*)

Term	Definition
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 package.
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.
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)	<p>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.</p> <p>VCS supports both AVIO and VIO configurations for storage and networking devices in an IVM environment.</p>

## 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 v2	5.0 MP2	3.5	HP-UX 11i v2	5.0 MP2
		3.5	HP-UX 11i v3 March 2009 or later	5.0, 5.0.1
HP-UX 11i v3	5.0.1	4.0	HP-UX 11i v2	5.0 MP2
		4.0	HP-UX 11i v3 March 2009 or later	5.0, 5.0.1
		4.1	HP-UX 11i v2	5.0 MP2
		4.1	HP-UX 11i v3 March 2009 or later	5.0, 5.0.1
		4.2	HP-UX 11i v2	5.0 MP2
		4.2	HP-UX 11i v3 March 2010 or later	5.0, 5.0.1
HP-UX 11i v3	5.1 SP1	4.2	HP-UX 11i v2	5.0 MP2
			HP-UX 11i v3 March 2010 or later	5.0, 5.0.1, 5.1 SP1
		4.3	HP-UX 11i v3 March 2011 or later	5.0.1, 5.1 SP1
HP-UX 11i v3	5.1 SP1	6.1	HP-UX 11i v3 September 2012 or later	5.0.1, 5.1 SP1

**Note:** HP IVM 4.2 is certified with Veritas Storage Foundation 5.0.1 Rolling Patch 2.

---

**Note:** HP IVM 6.1 is certified with Veritas Storage Foundation 5.1 Service Pack 1 Rolling Patch 2.

---

## Supported VCS and IVM versions

[Table 1-3](#) describes the supported VCS and IVM versions on the host and guest systems.

**Table 1-3** Supported VCS and IVM versions

VCS version	Integrity VM version	Host OS version	Guest OS version	Supported configuration
5.0.1 on HP-UX 11i v3	4.0	HP-UX 11i v3 September 2008 or later	HP-UX 11i v2 HP-UX 11i v3	<ul style="list-style-type: none"> <li>■ VM-VM See <a href="#">“Cluster among VMGuests (VM-VM)”</a> on page 19.</li> <li>■ VM-PM See <a href="#">“Cluster among VMGuests and physical machines (VM-PM)”</a> on page 23.</li> <li>■ PM-PM See <a href="#">“Cluster among VMHosts (PM-PM)”</a> on page 26.</li> </ul>

**Table 1-3** Supported VCS and IVM versions (*continued*)

VCS version	Integrity VM version	Host OS version	Guest OS version	Supported configuration
5.0.1 on HP-UX 11i v3	4.1	HP-UX 11i v3 March 2009 or later	HP-UX 11i v2 HP-UX 11i v3	<ul style="list-style-type: none"> <li>■ VM-VM See <a href="#">“Cluster among VMGuests (VM-VM)”</a> on page 19.</li> <li>■ VM-PM See <a href="#">“Cluster among VMGuests and physical machines (VM-PM)”</a> on page 23.</li> <li>■ PM-PM See <a href="#">“Cluster among VMHosts (PM-PM)”</a> on page 26.</li> </ul>
5.0.1 on HP-UX 11i v3	4.2	HP-UX 11i v3 March 2010 or later	HP-UX 11i v2 HP-UX 11i v3	<ul style="list-style-type: none"> <li>■ VM-VM See <a href="#">“Cluster among VMGuests (VM-VM)”</a> on page 19.</li> <li>■ VM-PM See <a href="#">“Cluster among VMGuests and physical machines (VM-PM)”</a> on page 23.</li> <li>■ PM-PM See <a href="#">“Cluster among VMHosts (PM-PM)”</a> on page 26.</li> </ul>

**Table 1-3** Supported VCS and IVM versions (*continued*)

VCS version	Integrity VM version	Host OS version	Guest OS version	Supported configuration
5.1 SP1 on HP-UX 11i v3	4.3	HP-UX 11i v3 March 2011 or later	HP-UX 11i v2 HP-UX 11i v3	<ul style="list-style-type: none"> <li>■ VM-VM See <a href="#">“Cluster among VMGuests (VM-VM)”</a> on page 19.</li> <li>■ VM-PM See <a href="#">“Cluster among VMGuests and physical machines (VM-PM)”</a> on page 23.</li> <li>■ PM-PM See <a href="#">“Cluster among VMHosts (PM-PM)”</a> on page 26.</li> </ul>
5.1 SP1 RP2 on HP-UX 11iv3	6.1	HP-UX 11i v3 September 2012 or later	HP-UX 11iv3 September 2012 or later	<ul style="list-style-type: none"> <li>■ VM-VM See <a href="#">“Cluster among VMGuests (VM-VM)”</a> on page 19.</li> <li>■ VM-PM See <a href="#">“Cluster among VMGuests and physical machines (VM-PM)”</a> on page 23.</li> <li>■ PM-PM See <a href="#">“Cluster among VMHosts (PM-PM)”</a> on page 26.</li> </ul>

---

**Note:** HP IVM 4.2 is certified with Veritas Cluster Server 5.0.1 Rolling Patch 2.

---



---

**Note:** HP IVM 4.3 is certified with Veritas Cluster Server 5.1 Service Pack 1 Rolling Patch 1.

---

## 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 (SFCFS) either on the VMHost or on the VMGuest or on both. VMGuests, support both single-node and multiple-node high availability configurations.

Table 1-4 shows the support matrix for the various deployment models.

**Table 1-4** Supported configurations using IVM

		Deployment on the VMGuest			
		SF on VMGuest	SFHA on VMGuest	SFCFS on VMGuest	SF not installed on VMGuest
Deployment on the VMHost/ backend device	SF on VMHost	Supported See <a href="#">“SF on both VMGuest and VMHost”</a> on page 18.	Not Supported	Not Supported	Supported See <a href="#">“SF on VMHost only”</a> on page 17.
	SFHA on VMHost	Supported See <a href="#">Figure 1-17</a> on page 28.	Not Supported	Not Supported	Supported See <a href="#">Figure 1-16</a> on page 28.
	SFCFS on VMHost	Not Supported	Not Supported	Not Supported	Not Supported
	Whole Disk on VMHost (SF is not used)	Supported See <a href="#">“SF on VMGuest only”</a> on page 16.	Supported* See <a href="#">Figure 1-9</a> on page 22.	Supported* See <a href="#">“SFCFS on VMGuest only”</a> on page 29.	Not applicable

---

**Warning:** \* indicates that these configurations are supported with fencing enabled for IVM 6.1.

---

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

SF	See <a href="#">“Storage Foundation supported configurations using IVM”</a> on page 16.
SFHA	See <a href="#">“Storage Foundation High Availability supported configurations using IVM”</a> on page 18.
SFCFS	See <a href="#">“Storage Foundation Cluster File System supported configurations using IVM”</a> on page 29.

## Storage Foundation supported configurations using IVM

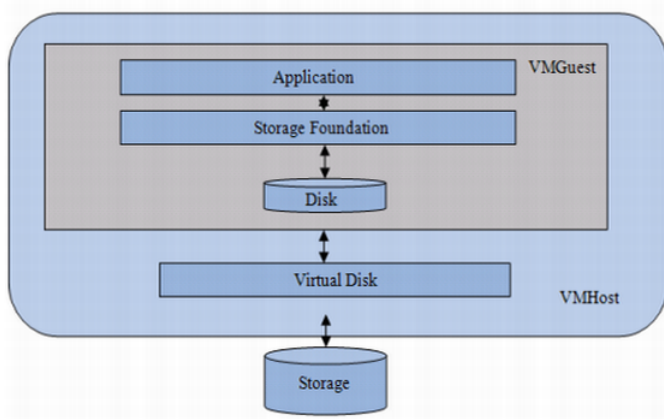
Symantec recommends the following deployment models:

SF on VMGuest only	See <a href="#">“SF on VMGuest only”</a> on page 16.
SF on VMHost only	See <a href="#">“SF on VMHost only”</a> on page 17.
SF on both VMGuest and VMHost	See <a href="#">“SF on both VMGuest and VMHost”</a> on page 18.

### SF on VMGuest only

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

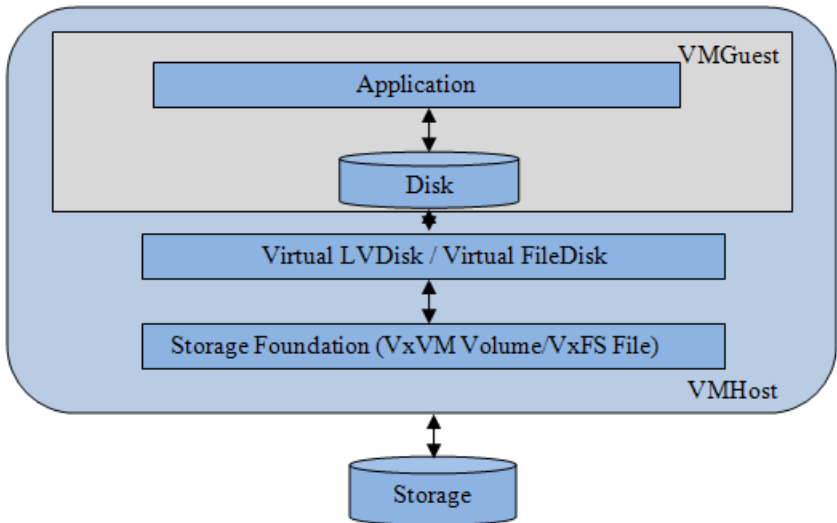
Figure 1-2 SF on VMGuest only



## SF on VMHost only

Figure 1-3 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.

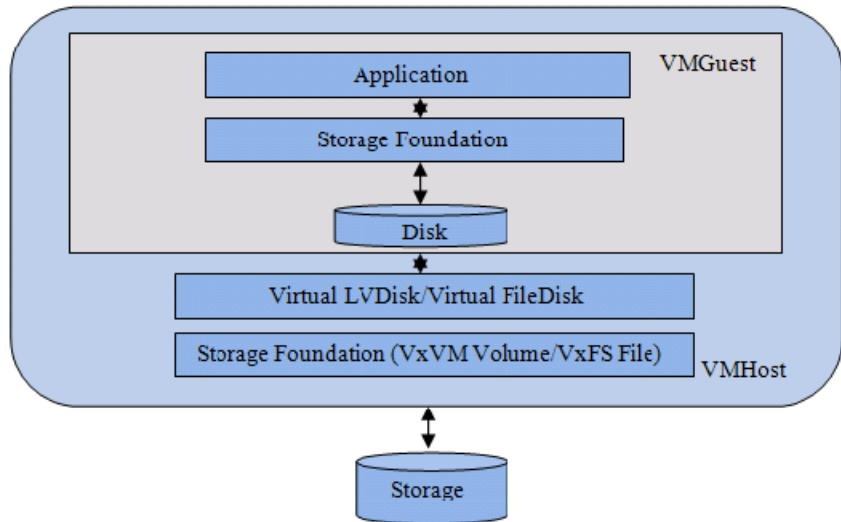
Figure 1-3 SF on VMHost only



## SF on both VMGuest and VMHost

Figure 1-4 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 1-4** 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 19.

---

**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 23.

- 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 26.

## Cluster among VMGuests (VM-VM)

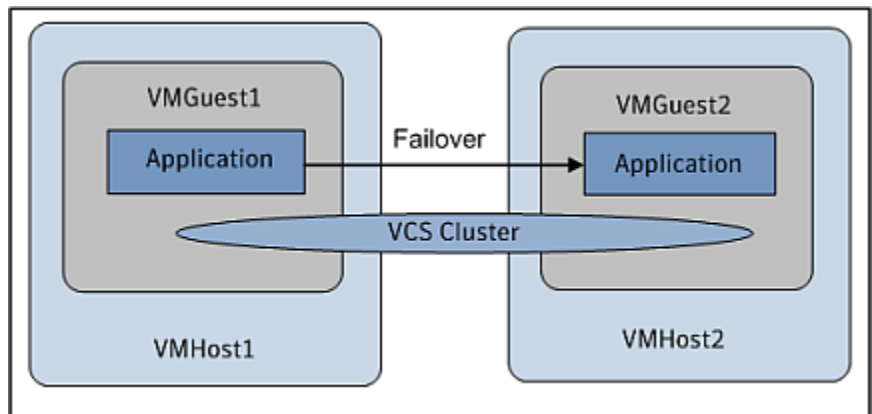
The following configurations are supported:

- Cluster among VMGuests on two different VMHosts  
See “[Cluster among VMGuests on two different VMHosts](#)” on page 19.
- Cluster among VMGuests on the same VMHost  
See “[Cluster among VMGuests on the same VMHost](#)” on page 20.

### Cluster among VMGuests on two different VMHosts

Figure 1-5 shows a configuration in which a cluster is formed between two VMGuests on different VMHosts.

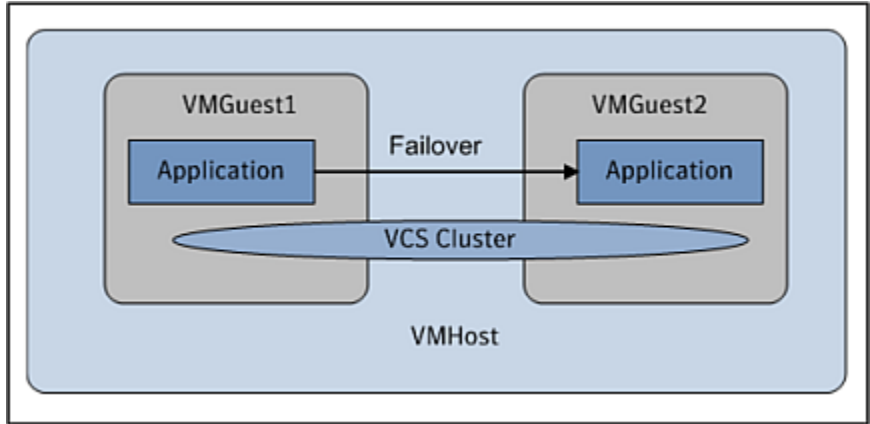
**Figure 1-5** VCS cluster between VMGuests on two different VMHosts



## Cluster among VMGuests on the same VMHost

Cluster among VMGuests on the same VMHost 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 1-6** VCS cluster between VMGuests on the same VMHost

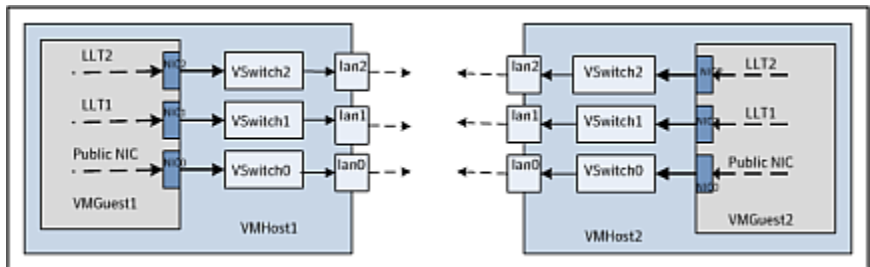


## Network configuration

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

Figure 1-7 shows a cluster between VMGuest1 and VMGuest2.

**Figure 1-7** 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.

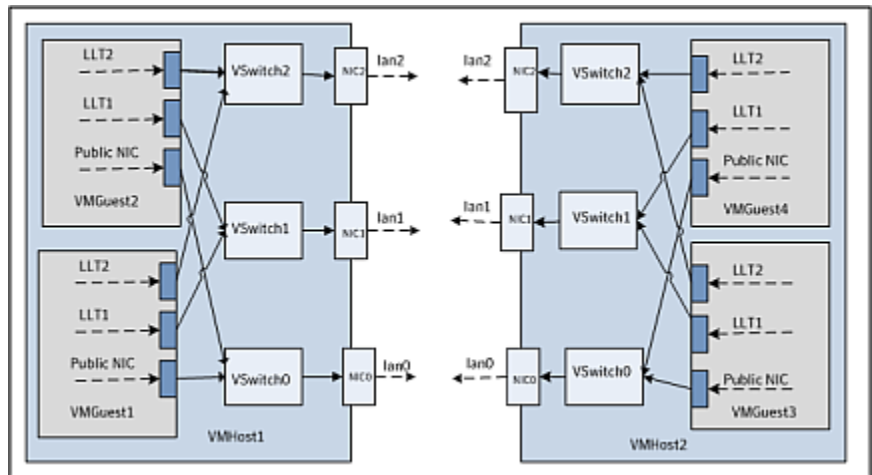
The network connections for VMGuest1 are as follows:

- 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 1-8 shows the network configuration for multiple VMGuests.

**Figure 1-8** Cluster among multiple VMGuests



## Storage configuration

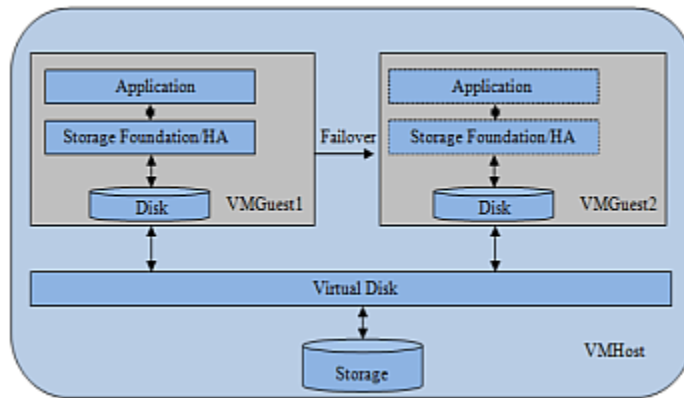
Figure 1-9 shows a deployment in which SFHA is installed only on the VMGuest and whole disk is exported from the VMHost.

---

**Warning:** Data corruption can occur because fencing is disabled.

---

**Figure 1-9** 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 30.

## 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 package 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

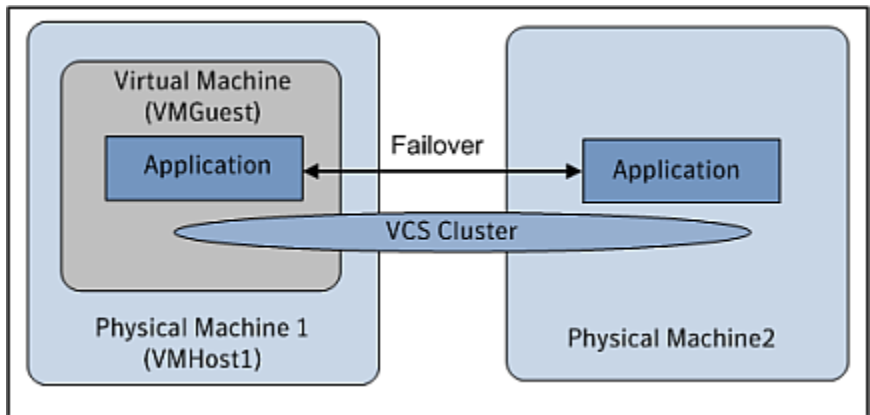
/opt/VRTSvcs/bin/vcsenv file on all the VMGuests. This will prevent the VCS engine from missing heartbeats with GAB on a loaded system during migration.

```
VCS_GAB_TIMEOUT=30000
export VCS_GAB_TIMEOUT
```

## Cluster among VMGuests and physical machines (VM-PM)

Figure 1-10 shows a cluster between a VMGuest and a physical machine. VCS is installed on the virtual machine and the physical machine.

Figure 1-10 A VM-PM cluster



---

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

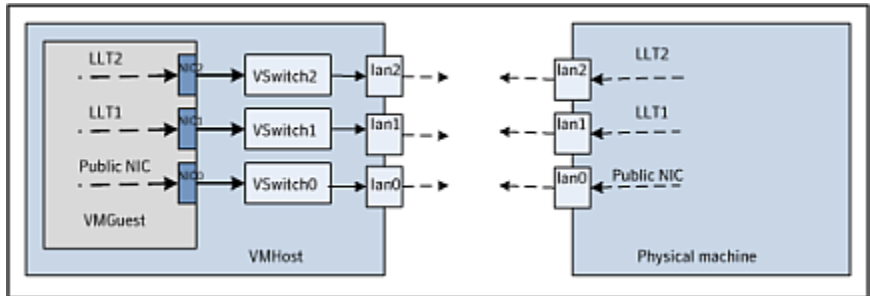
---

### 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 1-11 shows the network configuration for a VM-PM configuration.

**Figure 1-11** Network configuration for a VM-PM configuration

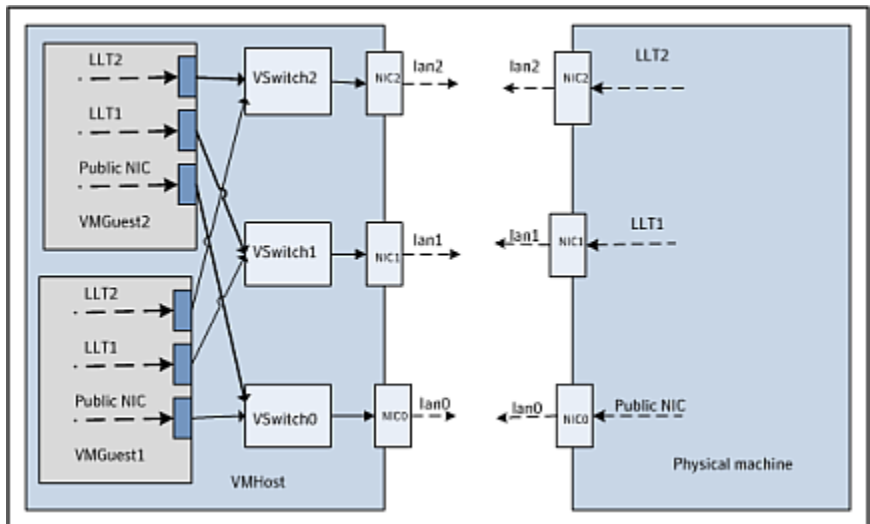


The network connections for the VMGuest are as follows:

- 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 1-12 shows the network configuration consisting of a physical machine and two VMGuests on the same VMHost.

**Figure 1-12** Network configuration for two VMGuests

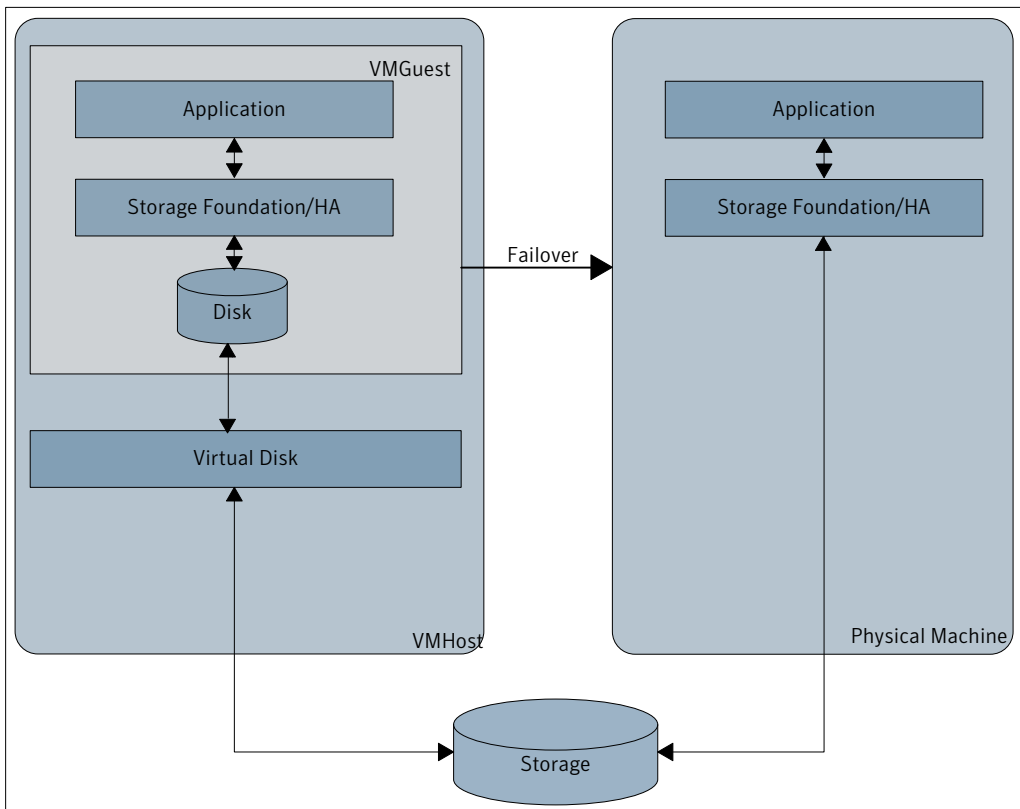


## Storage configuration

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 1-13 shows the storage configuration for a VM-PM setup.

**Figure 1-13** 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**

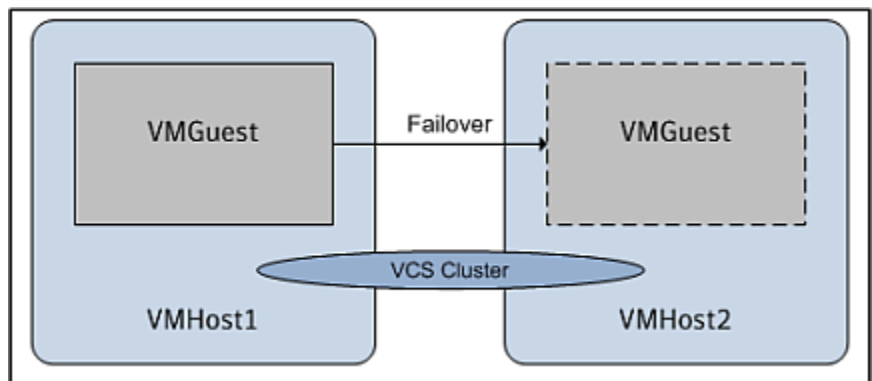
- Ensure that CPU and memory resources are available on the VMHosts.
- Install the HP Integrity VM package on the VMHosts.
- Create virtual switches to enable networking for VMGuests.
- Ensure that backing storage is available for VMGuests.
- Create the VMGuests.
- Install the operating system in the 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 1-14 shows a VCS cluster between VMHost1 and VMHost2.

**Figure 1-14** 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 29.

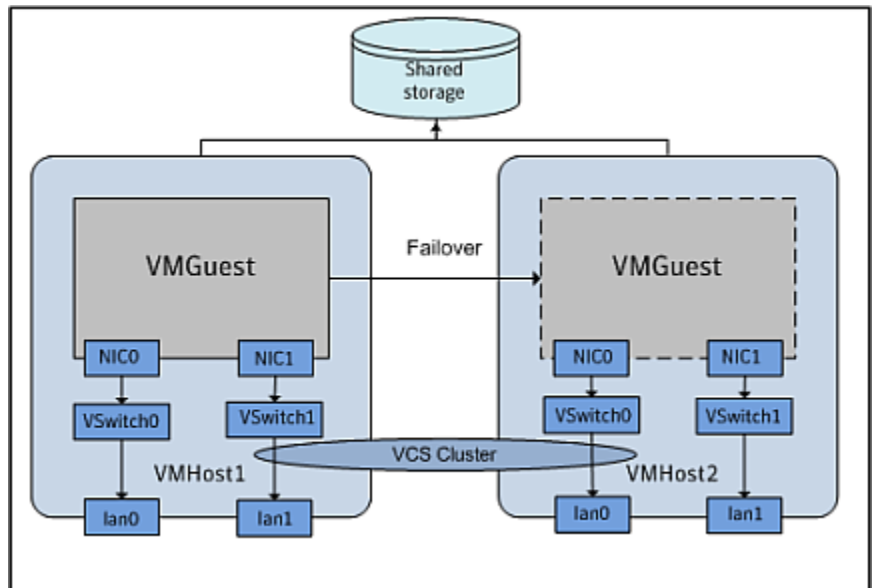
## Network and storage considerations

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 and Configuration Guide*.

[Figure 1-15](#) shows the network and storage organization for the PM-PM configuration.

**Figure 1-15** Network and storage organization for the PM-PM configuration



[Figure 1-16](#) 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 1-16** SFHA on the VMHost only

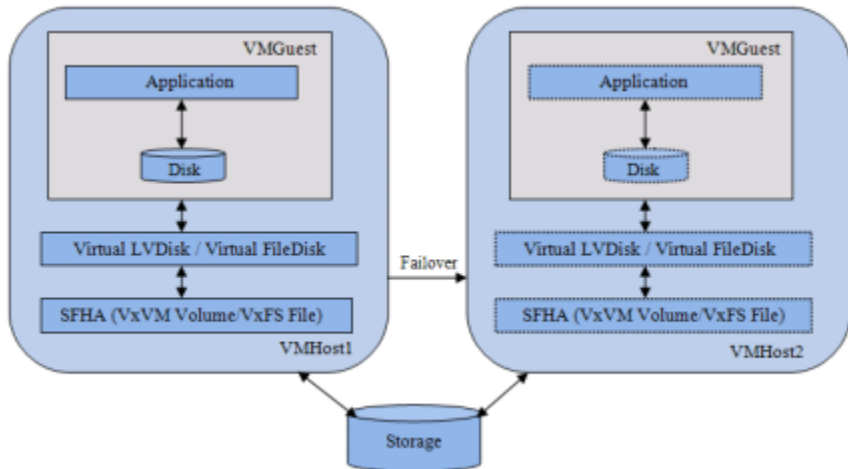
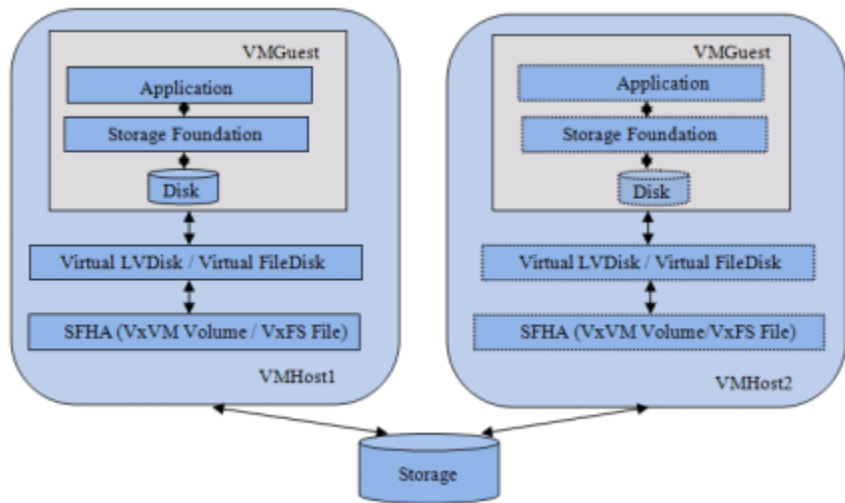


Figure 1-17 shows a configuration in which VMHosts form a VCS cluster and SF is installed in the VMGuest. VMHost can export a VxVM volume or VxFS file to the VMGuest. VCS monitors the VMGuests and its associated or dependent SF resources.

**Figure 1-17** 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 package 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 supported configurations using IVM

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

## SFCFS on VMGuest only

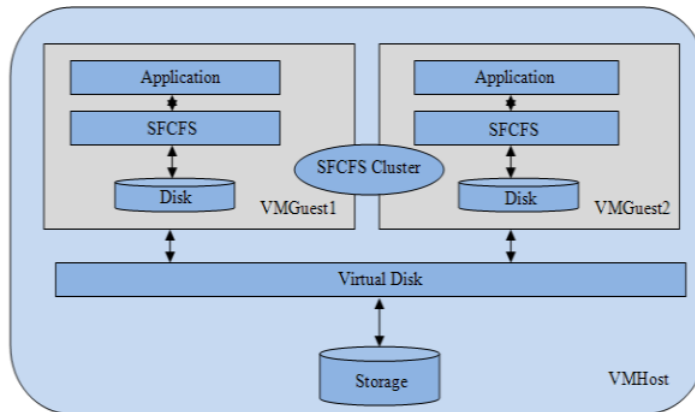
[Figure 1-18](#) shows a deployment in which SFCFS is installed only on the VMGuest and the whole disk is exported from the VMHost.

---

**Warning:** Data corruption can occur as fencing is disabled.

---

**Figure 1-18** SFCFS on VMGuest only



## 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 `vx dg deport dgname` command:

```
# vx dg 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 dgroup
```

- 8 Mount the file systems which are part of the volumes in the diskgroup.
- 9 Start the applications on the VMGuest.

## Advantages of using a VMHost-based Storage Foundation stack

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

## 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.

---

**Note:** With IVM 6.1 NPIV is supported and hence, all the above features are supported.

---

- SCSI-3 PGR-based I/O Fencing is supported for IVM 6.1 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.
- For IVM version 3.5, the total length of the device identifier as supported by DMP in the VMGuest, is limited to 64 characters. When you export the VxVM volumes as backing stores from the VMHost to the VMGuest, the device identifier includes the VxVM volume path. In this case, the disk group and the volume name together cannot exceed 41 characters. When you export a VMHost Veritas File System (VxFS) file to the VMGuest, the length of the file path cannot exceed 54 characters. This length also includes the slash '/' characters.

## 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

- Controlling applications running within VMGuests is not supported in a PM-PM configuration.
- The VM-VM configuration does not manage VMGuests failovers as VCS is running within the VMGuests.
- SCSI-3 PGR-based I/O Fencing is supported for IVM 6.1 in the VMGuest.
- Suspend and Resume of VMGuests is not supported by VCS with HP IVM 6.1 as well as HP IVM 4.3.