Veritas Storage Foundation™ and Disaster Recovery Solutions for Microsoft Hyper-V™

Windows Server 2008 (x64), Windows Server 2008 R2 (x64)

6.0

October 2011

Symantec™

Veritas Storage Foundation™ and Disaster Recovery Solutions for Microsoft Hyper-V™

Product version: 6.0

Document version: 6.0.1

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

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

Section 1

Storage Foundation for Windows (SFW)

Chapter 1

Introduction to Storage Foundation for Windows solutions for Hyper-V environments

This chapter includes the following topics:

Advantages of running Storage Foundation for Windows in the Hyper-V parent

Veritas Storage Foundation for Windows (SFW) is a host-level volume manager that provides a means to virtualize storage seen by the host it runs on. SFW provides central-point control of that storage space.

By running SFW in the Hyper-V parent partition, SFW features and functionality extend to virtual machines (VMs), offering benefits that would otherwise be unavailable at the guest level.

See "How Storage Foundation for Windows manages storage for virtual machines" on page 14.

SFW has added the following features and functionality specifically to support Hyper-V VMs when running SFW in the Hyper-V parent:

- SFW live migration support
  You can configure the SFW storage on which the VMs reside to support VM live migration between nodes of a Microsoft failover cluster.
  Detailed instructions are available on how to implement live migration for VMs on SFW storage.
  See "About implementing Hyper-V virtual machine live migration on SFW storage" on page 18.
- SFW storage migration for VMs
  The SFW storage migration feature enables you to view and select VMs to migrate to different storage.
  Detailed instructions are available on how to implement the storage migration solution for VMs.
  See "About storage migration" on page 45.

SFW also offers advanced features and functionality, such as multi-pathing, replication, and snapshots, which further extend the capabilities of Windows in the datacenter. More information is available on how to use the following features and the benefits they provide in a Hyper-V environment:

- Using Dynamic Multi-pathing (DMP) to provide failover and load-balancing to the LUNs that host the VMs in the child partition (DMP Device Specific Modules option)
- Replicating VMs between sites (Veritas Volume Replicator option)
- Maintaining Quick Recovery snapshots of the VMs (FlashSnap option)

See "About using optional Storage Foundation for Windows features in the Hyper-V parent" on page 55.

How Storage Foundation for Windows manages storage for virtual machines

In virtual environments, managing the storage that is used by guests is not an easy task. Typically, the guest is separated from the physical storage. Veritas Storage Foundation for Windows (SFW) provides several solutions to make it easier to manage storage requirements for virtual machines.

With Hyper-V, guests reside on virtual hard disk (VHD) files, which in turn are located on volumes that reside on physical storage. Direct access to those volumes or the LUNs they reside on is not available from the guest. The VHD files are provisioned by the parent on storage accessed by the parent partition. As storage needs change in the guest VHDs, they may require additional space. It can be

difficult to effectively manage space requirements or to relocate a guest from one storage location to another.

Running Veritas Storage Foundation for Windows (SFW) in the parent provides the following storage management solutions for VHDs.

- The SFW storage migration feature enables you to view and select VMs to migrate to different storage.
  For details on using SFW for migrating VM to new storage, see the following:
  See "About storage migration" on page 45.
- SFW allows for dynamically growing the volumes that host the guest VHDs. As SFW allows for growth of all volume types, the volumes that host the VHD files can be configured for performance via RAID-5, striping or mirrored-stripes.
- In environments using thin provisioned storage, SFW can be configured to automatically grow volumes based on user- defined space thresholds and policies that set the amount to grow the volumes by and whether that growth should be restricted or unrestricted. This counters the effects of NTFS uncontrolled growth tendencies in a thin environment, by allowing the creation of small volumes on the thin storage, which will grow automatically as needed, triggering corresponding growth in the hardware.
- As a host-level volume manager, SFW also allows for mirroring volumes across arrays and, with its support for dynamic disk operations in a cluster, the creation of stretch or campus clusters.

Related documentation on Storage Foundation for Windows

This guide covers information specific to deploying Microsoft Hyper-V virtual machines with SFW.

The following table describes related documentation on SFW.

Table 1-1 Related documentation on SFW solutions

For information about	Refer to
Installation information	*Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide*
Information on all SFW features	*Veritas Storage Foundation Administrator's Guide*

Table 1-1 Related documentation on SFW solutions *(continued)*

For information about	Refer to
Information on Veritas Volume Replicator (VVR)	*Veritas Volume Replicator Administrator's Guide*
Implementing SFW snapshot solutions for applications	SFW Quick Recovery solutions guides. Guides are available for: ■ Microsoft Exchange 2007 and 2010 ■ Microsoft SQL 2005, 2008, and 2008 R2 ■ Microsoft SharePoint 2007 ■ Enterprise Vault
Implementing Microsoft cluster solutions with SFW for applications on physical machines	SFW Microsoft Clustering solutions guides. Guides are available for: ■ Microsoft Exchange 2007 ■ Microsoft SQL 2005, 2008, and 2008 R2 In addition, the following guide provides general guidelines for using Microsoft clustering with SFW storage for other applications or server roles: *Veritas Storage Foundation and High Availability Solutions, Solutions Guide*

Chapter 2

Implementing live migration support for SFW and Hyper-V Virtual Machines

This chapter includes the following topics:

About implementing Hyper-V virtual machine live migration on SFW storage

This chapter provides steps for configuring SFW Microsoft Hyper-V virtual machine live migration on a highly available failover cluster disk group resource.

Live Migration of a Hyper-V virtual machine (VM) is achieved through the use of Windows Server 2008 R2 Failover Cluster feature. Live Migration significantly increases availability of the virtual machines during planned and unplanned downtime.

Live migration produces significantly less downtime for the virtual machines that are being migrated. Users can have uninterrupted access to the migrating virtual machine. The guest operating system in the migrating virtual machine is unaware that the migration is taking place. In addition, physical host maintenance can be carried out with no effect on virtual machine availability; this maintenance can occur during normal business hours.

You can configure the SFW storage on which the virtual machine (VM) resides to support VM live migration between nodes of a Microsoft failover cluster.

Note: After upgrading from earlier versons of SFW, if there is a disk group resource already present in a cluster, then the disk group resource must be taken offline and the cluster service should be restarted so that the **LiveMigrationSupport** attribute for the disk group resource is dispalyed on the Failover Cluster Manager console. To successfully set it to **True**, you must configure the SFW messaging for Live Migration support between the cluster nodes using the SFW Configuration Utility for Hyper-V Live Migration Support through the Solution Configuration Center (SCC).

See "Using the SFW Configuration Utility for Hyper-V Live Migration Support through SCC" on page 27.

See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

Requirements for Veritas Storage Foundation for Windows (SFW)

Before installing Veritas Storage Foundation for Windows (SFW), review the following requirements.

Note: For SFW Hyper-V live migration support, only one virtual machine (VM) per disk group is a mandatory requirement. If multiple virtual machines reside on the same disk group, then before configuring live migration, use the Storage Migration wizard to migrate virtual hard disks and split the disk group using SFW to create separate disks groups.

See " Converting your existing Hyper-V configuration to live migration supported configuration" on page 52.

- Review the general installation requirements for installing SFW in the *Veritas Storage Foundation and High Availability Solutions for Windows Installation and Upgrade Guide*.
- Memory must be a minimum 4 GB of RAM per server for SFW.
- Processor can be either a x64 architecture-based computer with Intel processor that supports Intel Extended Memory 64 Technology (Intel EM64T) or an AMD processor that supports the AMD64 platform; Intel Itanium family IA64 processors are not supported.
- Disk partitions must be formatted for the NTFS file system.
- Memory must be a minimum 4 GB of RAM per server for SFW HA.
- Do not install SFW on servers that are assigned the role of a domain controller. Configuring a cluster on a domain controller is not supported.
- You must be a domain user.
  You must be a member of the local Administrators group on all nodes where you are installing.
- A minimum of two NICs is required. One NIC will be used exclusively for private network communication between the nodes of the cluster. The second NIC will be used for both private cluster communications and for public access to the cluster. Symantec recommends three NICs.
- Ensure that all systems used for a highly available solution have a shared storage.
- At least 2 systems are required for setting up Microsoft failover cluster nodes between host machines.

Tasks for deploying SFW Hyper-V virtual machine live migration support

To deploy SFW Hyper-V virtual machine live migration on the host side, perform the following tasks in the sequence shown.

Table 2-1 Process for configuring SFW Hyper-V virtual machine live migration

Action	Description
Review the requirements	See "About implementing Hyper-V virtual machine live migration on SFW storage" on page 18. See "Requirements for Veritas Storage Foundation for Windows (SFW)" on page 18.
Install Windows Server 2008 R2	See "Installing Windows Server 2008 R2" on page 21.
Prepare the host machines	■ Adding the Hyper-V role See "Adding the Hyper-V role" on page 22. ■ Adding the Failover Cluster feature on the host side See "Adding the Failover Cluster feature" on page 22. ■ Configuring failover cluster nodes on the host side See "Configuring failover cluster nodes " on page 22.
Install the SFW Microsoft Failover Cluster option	See "Installing the Veritas Storage Foundation Cluster Option for Microsoft Failover Cluster" on page 22.
Configure port and remote communication settings	See "Configuring ports and firewall settings" on page 26.
Configure SFW Configuration Utility for Hyper-V Live Migration Support through the Solutions Configurations Center (SCC)	See "Using the SFW Configuration Utility for Hyper-V Live Migration Support through SCC" on page 27. See "Configuring SFW Configuration Utility for Hyper-V Live Migration Support" on page 28. See "Unconfiguring SFW Configuration Utility for Hyper-V Live Migration Support" on page 31. See "Reconfiguring the SFW Configuration Utility for Hyper-V Live Migration Support" on page 33.

Table 2-1 Process for configuring SFW Hyper-V virtual machine live migration *(continued)*

Action	Description
Configure the storage	Use the Veritas Enterprise Administrator (VEA) console to create disk groups and volumes. **Note:** Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. To use these disks when you create your SFW cluster disk groups, you must first remove the physical disk resources from the cluster. Otherwise, a reservation conflict occurs. ■ Creating dynamic cluster disk groups See "Creating dynamic cluster disk groups" on page 34. ■ Creating dynamic volumes See "Creating dynamic volumes" on page 36. ■ See "Managing disk groups and volumes" on page 38. ■ Adding a Volume Manager Disk Group (VMDg) resource See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.
Create a virtual machine service group	See "Creating a virtual machine service group" on page 42.
Set the dependency of the virtual machine on the VMDg resource	See "Setting the dependency of the virtual machine on the VMDg resource" on page 43.

Installing Windows Server 2008 R2

Install Windows Server 2008 R2 operating systems. Refer to Microsoft documentation for details on installing Windows Server 2008 R2.

Preparing the host machines

For virtual machine live migration support, you need to add the Hyper-V role and configure a failover cluster on your host machines. Perform the following tasks in the order shown.

Adding the Hyper-V role

After installing Windows Server 2008 R2, the next step is to add the Hyper-V role to enable the live migration feature. To enable the Hyper-V role, refer to Microsoft Hyper-V documentation for details.

Adding the Failover Cluster feature

Install the Microsoft Failover Cluster feature on all host systems by using the Add Features option from the Server Manager. Refer to Microsoft documentation for details on installing the Failover Cluster feature.

Configuring failover cluster nodes

Configure a failover cluster on all of your host nodes. Refer to Microsoft documentation for details on how to add a failover cluster node. Ensure that you have fulfilled the clustering network requirements before you start creating the failover cluster nodes.

Verify that you have at least three network adapters (two NICs exclusively for the private network and one for the public network). However, when using only two NICs, lower the priority of one NIC and use the low-priority NIC for public and private communication.

Installing the Veritas Storage Foundation Cluster Option for Microsoft Failover Cluster

Administrative privileges are required on both host and guest operating systems for installing the Veritas Storage Foundation for Windows Cluster Option for Microsoft Failover Cluster.

Before you install SFW, you must install the Microsoft Failover Cluster feature and configure failover cluster nodes on all the systems that are part of the live migration configuration.

Installing SFW requires a reboot, but a reboot on the active cluster node causes it to fail over. Hence, it is advisable to use a "rolling install" procedure to install

SFW first on the inactive cluster node. Then move the cluster resources to the other node and install on the inactive node.

During SFW installation using the product installer, make the following selections:

- Select Storage Foundation for Windows as the product to install.
- When selecting the available options from the server components, ensure that you select the **Cluster Option for Microsoft Failover Cluster** option.
  - Leave the client components selected (the default).

During installation, the installer will display a message box about Quorum Arbitration. The Quorum Arbitration time settings are adjusted to ensure optimal functionality of a dynamic quorum resource on a mirrored dynamic volume.

The quorum arbitration minimum and maximum time settings are used to set the limits of the time period that Microsoft clustering allows for quorum arbitration. Quorum arbitration is the process that occurs when the controlling node of the cluster is no longer active and other nodes of the cluster attempt to gain control of the quorum resource and thus control of the cluster. Refer to the *Veritas Storage Foundation for Windows Administrator's Guide* for information on the settings.

For additional details on using the product installer or command line installation, see the *SFW HA Installation and Upgrade Guide*.

To install SFW/Cluster Option for Microsoft Failover Cluster

1. Insert the software disc containing the installation package into your system's disc drive or download the installation package from the following location:

   https://fileconnect.symantec.com

2. Allow the autorun feature to start the installation or double-click **Setup.exe**.

   The CD browser appears.

Note: If you are installing the software using the product software disc, the CD browser displays the installation options for all the products specified earlier. However, if you are downloading the installation package from the Symantec Web site, the CD browser displays the installation options only for the product to be installed.

---

3 Click to download the required contents.

Note: The client components are installed by default along with the server components. However, on a server core machine, the client components will not be installed.

Veritas Storage Foundation 6.0	Click to install the server components for Storage Foundation for Windows.
Late Breaking News	Click to access the latest information about updates, patches, and software issues regarding this release.
Windows Data Collector	Click to verify that your configuration meets all the software and hardware requirements.
SORT	Click to access the Symantec Operations Readiness Tools (SORT) site. In addition to the product download you can also download the custom reports about your computer and Symantec enterprise products, a checklist providing configuration recommendations, and system and patch requirements to install or upgrade your software.
Browse Contents	Click to view the software disc contents.
Technical Support	Click to contact Symantec Technical Support.

4 On the Welcome panel, review the list of prerequisites and click **Next**.

5 On the License panel, read the license terms, select **I accept the terms of License Agreement**, and then click **Next**.

6 On the System Selection panel, select the systems and the desired Installation and Product options:

You can select the systems in one of the following ways:

- In the System Name or IP text box, manually type the system name or its IP address and click Add.

Note: The wizard does not support the Internet Protocol version 6. To add the systems having Internet Protocol version 6, you must type the system name.

The local host is populated by default.

- Alternatively, browse to select the systems.
  The systems in the domain to which you are logged on are listed in the **Available Systems** list. Select one or more systems and click the right arrow to move them to the **Selected Systems** list.
  Click **OK**.
  The selected systems are validated and details are displayed in **Verification Details**. Select a system to review the details.
  To select the installation and product options, perform the following tasks on each of the selected system.

Note: To apply the selection to multiple systems, select the system for which you have selected the installation and product options and then click **Apply to multiple systems**.

- The product is installed by default at the %ProgramFiles%\Veritas location. To customize the installation directory, click **Browse** and select a location of your choice.
  Click **OK**.

Note: The installation directory is selected by default on systems where the product is being upgraded.

- Select the required license type from the **License key** drop-down list.

Note: The default license type is **Keyless**.

If you select the **Keyless** license type, all the available product options are displayed and are selected by default.
If you select **User entered license key** as your license type, the License Details panel appears by default. On the **License Details** panel, enter the license key and then click **Add**. You can add multiple licenses for the various product options you want to use.
Validation check is done for the entered license keys. If validation fails, an error message is displayed.

After successful validation, click **OK**.

- From the list of product options, select the **Cluster Option for Microsoft Failover Cluster** which provides support for Microsoft Failover Cluster.

7 On the System Selection panel, click **Next**.

All the selected systems must pass the validation check. In case the validation checks have failed on any of the system, review the details and resolve the issue.

Click **Re-verify** to run the validation check on the system again.

8 On the Pre-install Summary panel, review the summary and click **Next**.

9 The **Automatically reboot systems after installer completes operation** check box is selected by default. This option reboots all the selected remote systems immediately after installation completes on selected systems.

However, if you do want to initiate the auto reboot option at this stage, uncheck the checkbox **Automatically reboot systems after installer completes operation** .

10 On the Installation panel, review the progress of installation.

Click **Next** after the installation completes.

If installation is not successful on any of the selected systems, then a failed installation status is shown.

11 On the Post-install Summary panel, review the installation result and click **Next**.

Refer to the log file for details, if installation has failed on any of the selected system. You may need to reinstall the software.

12 On the Summary page, click **Finish**.

If you selected the auto reboot as shown in step 9, a confirmation message to reboot the local system appears.

Click **Yes** to reboot immediately.

Click **No** to reboot later.

However, if the auto reboot option was not selected in step 9, then you must ensure to manually reboot the selected systems.

Configuring ports and firewall settings

Ensure that your firewall settings allow access to ports used by SFW wizards and services. For a detailed list of ports and services used by SFW, refer to the *Veritas*

Storage Foundation and High Availability Solutions for Windows Installation and Upgrade Guide.

Using the SFW Configuration Utility for Hyper-V Live Migration Support through SCC

After a cluster is configured, invoke the SFW Configuration Utility for Hyper-V Live Migration Support from the Solutions Configuration Center (SCC). This step should be completed before creating a Volume Manager Disk Group (VMDg) resource.

See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

The SFW Configuration Utility for Hyper-V Live Migration can be run from any node of the Microsoft failover cluster which has Hyper-V roles added to it. This wizard is made available as an SCC launch point.

SFW Configuration Utility for Hyper-V Live Migration can be used for the following use cases:

- After configuring cluster for the first time and after adding a new node to the cluster
  See "Configuring SFW Configuration Utility for Hyper-V Live Migration Support" on page 28.
- After removing a node from the cluster
  See "Unconfiguring SFW Configuration Utility for Hyper-V Live Migration Support" on page 31.
- Reconfiguring SFW Hyper-V live migration support in case of some network properties (IP\port) changes.
  See "Reconfiguring the SFW Configuration Utility for Hyper-V Live Migration Support" on page 33.

Note: To enable live migration, you must set the VMDg resource **LiveMigrationSupport** attribute to **TRUE** for all VMDg resources in a cluster.

SFW Hyper-V Live Migration is supported on a network within a Microsoft Failover Cluster.

Note: If a cluster node crashes or shuts down abruptly, then it is noticed that on subsequent reboot of the other remaining cluster nodes, the SFW Configuration Utility for Hyper-V Live Migration Support shows the crashed node as **Invalid Configuration**.

In such cases, the SFW messaging for Live Migration support will not work between the remaining nodes and the VMDg **LiveMigrationSupport** attribute cannot be set to **True** for any new VMDg resource. To resolve this issue, it is recommended to first **Unconfigure** and then **Configure** the remaining cluster nodes using the SFW Configuration Utility for Hyper-V Live Migration Support through the Solutions Configuration Center (SCC).

See "Configuring SFW Configuration Utility for Hyper-V Live Migration Support" on page 28.

See "Unconfiguring SFW Configuration Utility for Hyper-V Live Migration Support" on page 31.

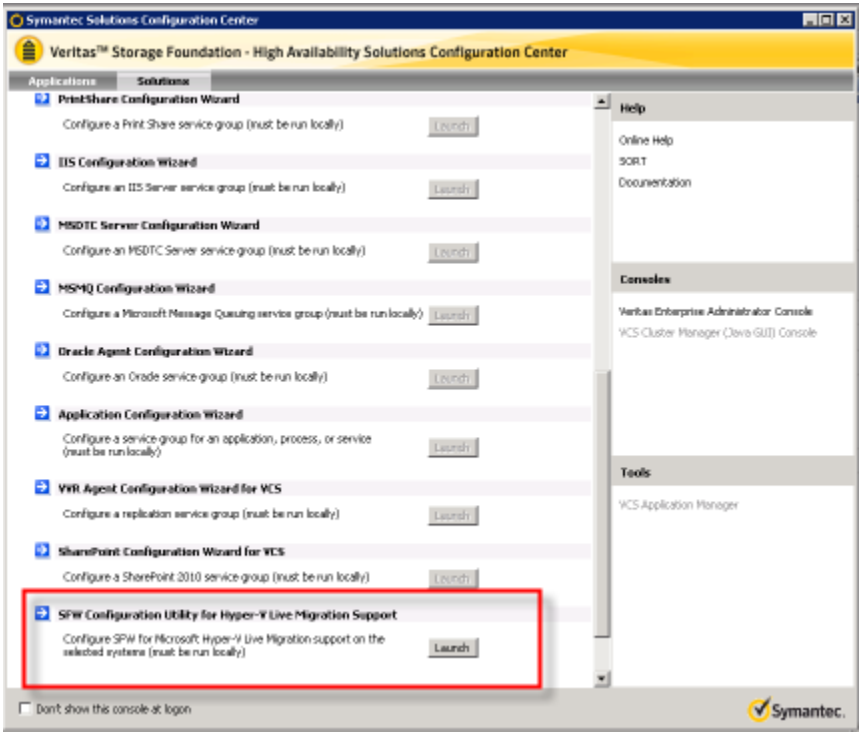
Configuring SFW Configuration Utility for Hyper-V Live Migration Support

Configure live migration support using the SFW Configuration Utility for Hyper-V Live Migration.

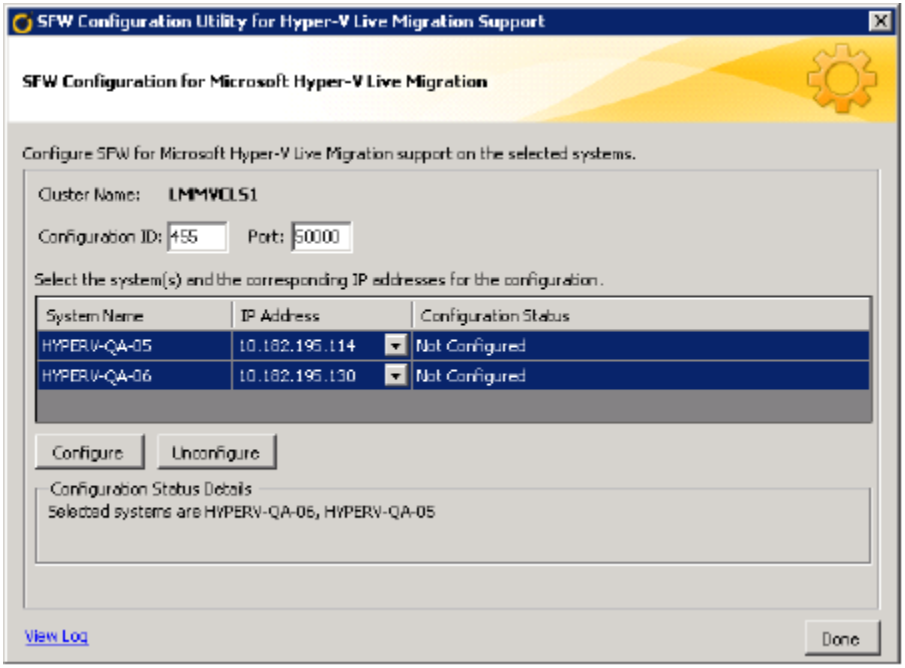
To configure live migration support on failover cluster nodes through SCC

1 Click **Start > Run**, type **scc**, and then click **OK** to launch the Solutions Configuration Center (SCC).

2 From the Solutions view in the SCC, launch the **SFW Configuration Utility for Hyper-V Live Migration Support.**



3 On the SFW Configuration for Hyper-V Live Migration Support page, complete the following:



Field	Description
Configuration ID	Enter a unique cluster configuration ID of your choice. The value can range from 0 to 65535.
Port	Specify a valid port number. The port values can range from 49152 to 65535. Ensure that UDP ports used by you are unblocked if using a firewall.
System Name	This table lists all the hosts in a cluster configuration as well as hosts which are already part of live migration configuration. Select the required cluster nodes from this column. **Note:** Please select at least two systems from the System list to configure live migration support. The SFW Configuration Utility for live migration will configure and unconfigure live migration support for selected systems.

IP Address	Corresponding IP address for the selected host or hosts is displayed. If multiple addresses for a selected host are configured, then a drop-down list is displayed. Select an IP address within the same cluster network.
Configuration Status	The following configuration status is displayed: ■ All the nodes which are already part of Live Migration configuration are shown as **Configured**. ■ For newly added node in a cluster, the status is displayed as **Not Configured**. ■ For invalid configuration, status is displayed as **Invalid Configuration**. ■ **Not Supported** status is displayed when SFW Cluster option for Microsoft Failover Cluster is not installed and if Microsoft Hyper-V role is not added.
Configure	Click on this button to configure SFW Hyper-V live migration support for a selected system that has a **Not Configured** status. Select a system and click on **Configure** to enable Live Migration support on it.
Configuration status details	Displays live migration configuration status for selected systems.

Click **Done** to configure live migration support for the selected systems and exit the SCC console.

Unconfiguring SFW Configuration Utility for Hyper-V Live Migration Support

To remove a node from a cluster when the status is shown as **Configured** or **Invalid Configuration**, use the SFW Configuration Utility for Hyper-V Live Migration Support to unconfigure live migration support.

Perform the following steps to unconfigure SFW Hyper-V live migration support for selected cluster nodes.

Unconfiguring SFW Hyper-V live migration support on failover cluster nodes

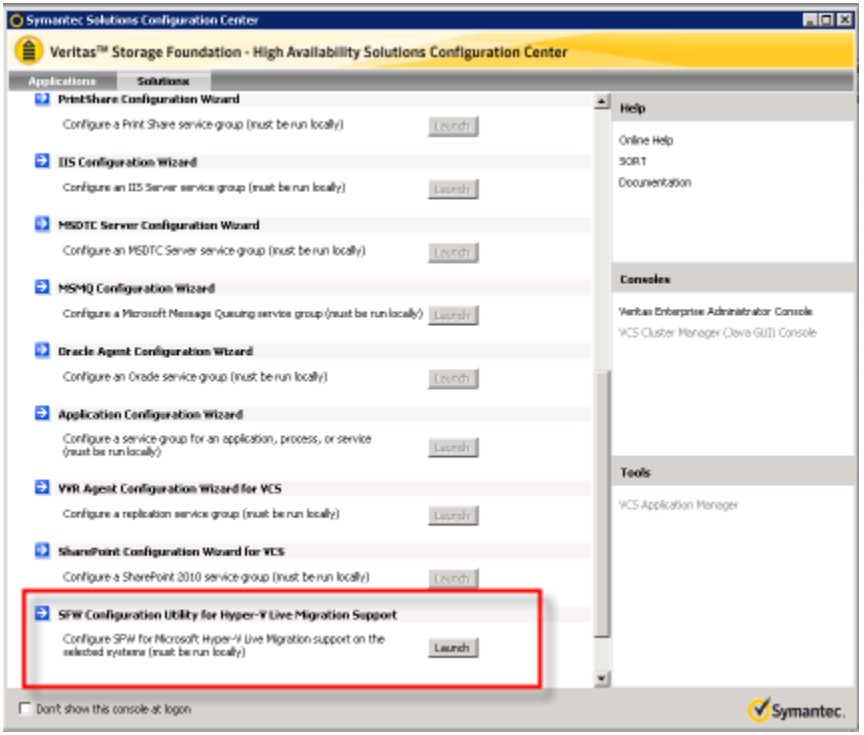
1 Right-click a VMDg resource on which the virtual machine is dependent from the Failover Cluster Manager console. Select **Properties** tab from the context menu.

From the Properties window, select the **Properties** tab and click to edit the VMDg **LiveMigrationSupport** attribute value to **FALSE**.

See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

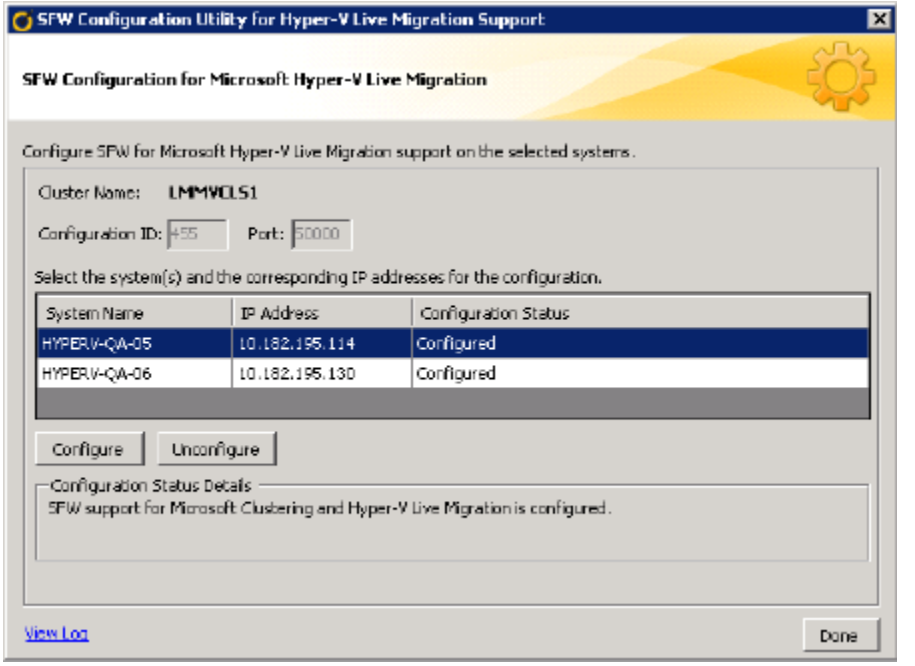
2 Now, using the Solutions Configuration Center (SCC) unconfigure live migration support for cluster nodes that show a status as **Configured** or **Invalid Configuration**.

Click **Start > Run**, type **scc**, and click **OK** to launch the Solutions Configuration Center (SCC).



3 From the **Solutions** tab in the SCC, launch the **SFW Configuration Utility for Hyper-V Live Migration Support**.

4 Select **Configured** or **Invalid Configuration** cluster nodes that you need to remove from live migration configuration.



If total number of cluster nodes is two, you can unconfigure or configure live migration support for these two cluster nodes. However, if total number of cluster nodes displayed is three, then select at least two systems to unconfigure live migration support.

5 Now click the **Unconfigure** button to unconfigure live migration support for the selected cluster nodes.

Additionally, you can also use **Alt+U** shortcut keys to unconfigure live migration support.

6 Validate that unconfiguring live migration support on selected cluster nodes is successful in the **Configuration Status Details** panel.

7 Click **Done** to exit the SCC console.

Reconfiguring the SFW Configuration Utility for Hyper-V Live Migration Support

In case of a change in network configuration (IP or port changes), use the SFW Configuration Utility for Hyper-V Live Migration Support to unconfigure and reconfigure live migration support.

Note: If SFW Hyper-V live migration configuration is not reconfigured, then cluster nodes that display **Invalid Configuration** status fail to receive Read-Only import messages and hence, will not have an up-to-date configuration. In such cases, the eventual SFW-Hyper-V live migration will not be instantaneous and will be slow.

To unconfigure and configure SFW Hyper-V live migration support again on selected cluster nodes, refer to the following sections:

See "Unconfiguring SFW Configuration Utility for Hyper-V Live Migration Support" on page 31.

See "Configuring SFW Configuration Utility for Hyper-V Live Migration Support" on page 28.

Configuring the SFW storage

You use Veritas Storage Foundation for Windows to create dynamic cluster disk groups and volumes for a cluster environment. You then add Volume Manager Disk Group resources to the failover cluster.

See "Creating dynamic cluster disk groups" on page 34.

See "Creating dynamic volumes" on page 36.

See "Managing disk groups and volumes" on page 38.

See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

Creating dynamic cluster disk groups

You create a dynamic cluster disk group with volumes on shared storage so that they can be shared between nodes in the cluster. Part of the process of creating a dynamic disk group is assigning it a name. You must choose a name that is unique to your environment. Make note of this name, as it will be required later.

To create dynamic cluster disk groups, use the Veritas Enterprise Administrator (VEA). The VEA can be invoked on one of the servers and can be used to connect to all the other servers. However, VEA can also be launched on client system and can be used to manage all the servers remotely.

Note: Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. To use these disks when you create your SFW cluster disk groups, you must first remove the physical disk resources from the cluster. Otherwise, a reservation conflict occurs. After creating the SFW cluster disk groups, you will add Volume Manager Disk Group resources to the cluster, instead of physical disk resources.

Note that dynamic disks belonging to a Microsoft Disk Management Disk Group do not support cluster disk groups.

Note: For SFW Hyper-V live migration support, only one virtual machine (VM) per disk group is a mandatory requirement.

To create a dynamic (cluster) disk group

1. Open the VEA console by clicking **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator** (or launch the VEA from the Solutions Configuration Center) and select a profile if prompted.
2. Click **Connect to a Host or Domain**.
3. In the Connect dialog box, select the host name from the pull-down menu and click **Connect**.

   To connect to the local system, select **localhost**.

   Provide the user name, password, and domain if prompted.
4. To start the New Dynamic Disk Group wizard, expand the tree view under the host node, right-click the **Disk Group**s icon, and select **New Dynamic Disk Group** from the context menu.
5. In the Welcome screen of the New Dynamic Disk Group wizard, click **Next**.
6. Provide information about the cluster disk group:
   - Enter the name of the disk group (for example, DG1).
   - Check the **Create cluster group** check box.
   - Select the appropriate disks in the **Available disks list**, and use the **Add** button to move them to the **Selected disks list**.
   - Optionally, check the **Disk names prefix** checkbox and enter a disk name prefix to give the disks in the disk group a specific identifier.
     For example, entering TestGroup as the prefix for a disk group that contains three disks creates TestGroup1, TestGroup2, and TestGroup3 as internal names for the disks in the disk group.

Note: For Windows Server 2008, Windows Disk Management Compatible Dynamic Disk Group creates a type of disk group that is created by Windows Disk Management (LDM).

Click **Next** to accept the confirmation screen with the selected disks.

7 Click **Finish** to create the new disk group.

Creating dynamic volumes

This section will guide you through the process of creating a volume on a dynamic disk group.

Note: When assigning drive letters to volumes, ensure that the drive letters that you assign are available on all nodes.

To create dynamic volumes

1 If the VEA console is not already open, click **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator**and select a profile if prompted.

2 Click **Connect to a Host or Domain**.

3 In the Connect dialog box select the host name from the pull-down menu and click **Connect**.

To connect to the local system, select **localhost**.

Provide the user name, password, and domain if prompted.

4 To start the New Volume wizard, expand the tree view under the host node to display all the disk groups. Right click a disk group and select **New Volume** from the context menu.

You can right-click the disk group you have just created, for example **DG1**.

5 At the New Volume wizard opening screen, click **Next**.

6 Select the disks for the volume.

Make sure the appropriate disk group name appears in the **Group name** drop-down list.

- SFW automatically selects the disks based on the following criteria:
  - Their port assignment (disks with two different ports are selected). Note that in the list of available disks, the entry after each disk name starts with the port number.

For example, the “P3” in the entry P3C0T2L1 refers to port 3.

- Amount of available space on the disks. SFW will pick two disks (one from each array) with the most space.

- To manually select the disks, click the **Manually select disks** radio button and use the **Add** and **Remove** buttons to move the appropriate disks to the “Selected disks” list.
- You may also check **Disable Track Alignment** to disable track alignment for the volume.
  Disabling Track Alignment means that the volume does not store blocks of data in alignment with the boundaries of the physical track of the disk.

Click **Next**.

7 Specify the volume attributes and complete the following.

- Enter a volume name. The name is limited to 18 ASCII characters and cannot contain spaces or forward or backward slashes.
- Provide a size for the volume. If you click the **Max Size** button, a size appears in the Size box that represents the maximum possible volume size for that layout in the dynamic disk group.
- Select a layout type.
- If you are creating a striped volume, the Columns and Stripe unit size boxes need to have entries. Defaults are provided.
- To select mirrored striped, click both the **Mirrored** checkbox and the **Striped** radio button.
- In the Mirror Info area, select the appropriate mirroring options.
- Verify that **Enable logging** is not selected.

Click **Next**.

8 Assign a drive letter or mount point to the volume. You must use the same drive letter or mount point on all systems in the cluster. Make sure to verify the availability of the drive letter before assigning it.

- To assign a drive letter, select **Assign a Drive Letter**, and choose a drive letter.
- To mount the volume as a folder, select **Mount as an empty NTFS folder**, and click **Browse** to locate an empty folder on the shared disk.

Click **Next**.

9 Create an NTFS file system.

- Make sure the **Format this volume** checkbox is checked and click **NTFS**.

- Select an allocation size or accept the default.
- The file system label is optional. SFW makes the volume name the file system label.
- Select Perform a quick format if you want to save time.
- Select **Enable file and folder compression** to save disk space.
  Note that compression consumes system resources and performs encryption and decryption, which may result in reduced system performance.

Click **Next**.

10 Click **Finish** to create the new volume.

11 Repeat these steps to create additional volumes.

Create the cluster disk group and volumes on the first node of the cluster only.

Managing disk groups and volumes

During the process of setting up an SFW environment, refer to these general procedures for managing disk groups and volumes:

- When a disk group is initially created, it is imported on the node where it is created.
- A disk group can be imported on only one node at a time.
- To move a disk group from one node to another, unmount the volumes in the disk group, deport the disk group from its current node, import it to a new node and mount the volumes.

Importing a disk group and mounting a volume

Use the Veritas Enterprise Administrator (VEA) console to import a disk group and mount a volume.

To import a disk group

1 From the VEA Console, right-click a disk name in a disk group or the group name in the Groups tab or tree view.

2 From the menu, click **Import Dynamic Disk Group**.

To mount a volume

1. If the disk group is not imported, import it.
2. To verify if a disk group is imported, from the VEA Console, click the **Disks**tab on the right pane and check if the status is imported.
3. Right-click the volume, click **File System**, and click **Change Drive Letter and Path**.
4. Select one of the following options in the Drive Letter and Paths dialog box depending on whether you want to assign a drive letter to the volume or mount it as a folder.
   - To assign a drive letter
     Select **Assign a Drive Letter**, and select a drive letter.
   - To mount the volume as a folder
     Select **Mount as an empty NTFS folder**, and click **Browse** to locate an empty folder on the shared disk.
     Click **OK**.

Unmounting a volume and deporting a disk group

Use the VEA Console to unmount a volume and deport a disk group.

To unmount a volume and deport the dynamic disk group

1. From the VEA tree view, right-click the volume, click **File System**, and click **Change Drive Letter and Path**.
2. In the Drive Letter and Paths dialog box, click **Remove**.

   Click **OK** to continue.
3. Click **Yes** to confirm.
4. From the VEA tree view, right-click the disk group, and click **Deport Dynamic Disk Group**.
5. Click **Yes**.

Adding the Volume Manager Disk Group (VMDg) resource

Perform the following steps to add a Volume Manager Disk Group (VMDg) resource.

Note: For SFW Hyper-V live migration support, only one virtual machine (VM) per disk group is a mandatory requirement. If multiple virtual machines reside on the same disk group, then before configuring live migration, use the Storage Migration wizard to migrate virtual hard disks and split the disk group using SFW to create separate disks groups.

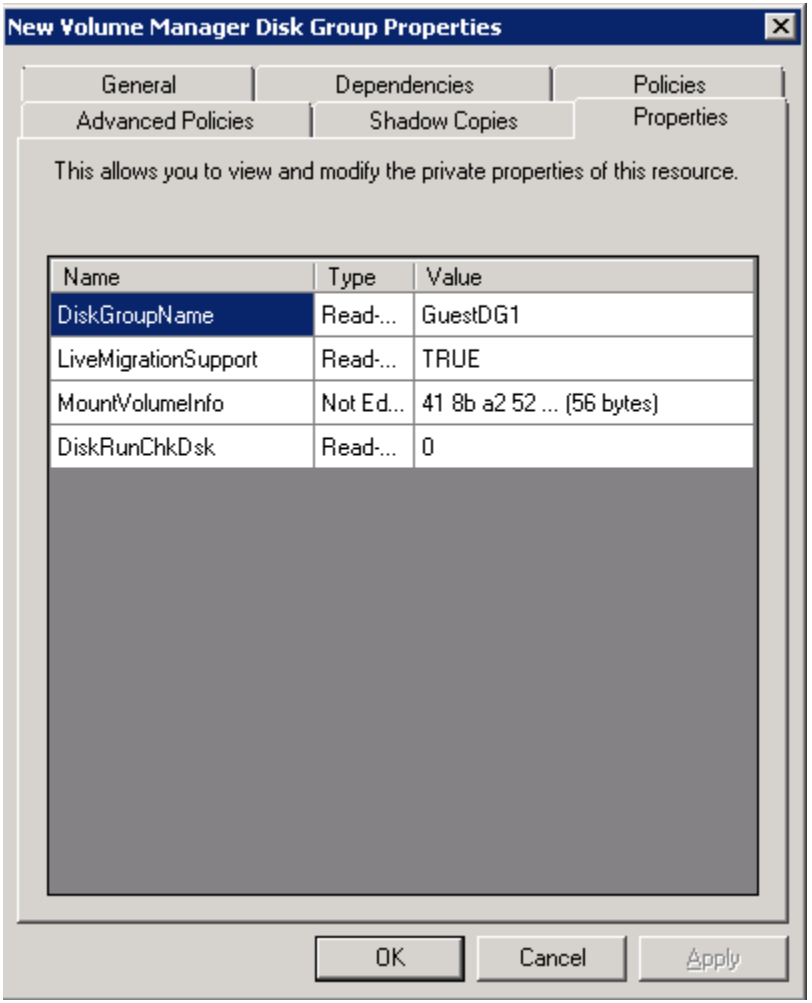
See " Converting your existing Hyper-V configuration to live migration supported configuration" on page 52.

To add a Volume Manager Disk Group (VMDg) resource

1. Click **Start > Administrative Tools > Failover Cluster Manager** to open the failover cluster snap-in.
2. Right-click **Services and Applications**. Select **More Actions > Create Empty Service or Application**. This creates a service group, for example, **SG1**.
3. Right-click the new service group and select **Add a Resource > More Resources > Add a Volume Manager Disk Group** from the context menu.

   A new Volume Manager Disk Group (VMDg) resource is created with a default name
4. Right-click the VMDg resource and select **Properties**.

   Complete the following on the **Properties** window:



- Select the **General** tab to change the default name of the **New Volume Manager Disk Group** to a name of your choice. Say, for example: VMDg1
- Now select the **Properties** tab and perform the following steps:
  - In the **DiskGroupName** box enter the dynamic cluster disk group name created earlier in this document. Say, for example GuestDG1.
    See "Creating dynamic cluster disk groups" on page 34.
  - Edit the **LiveMigrationSupport** attribute value to **TRUE**.
    Displayed default value is **FALSE**.

Note: To enable live migration, you must set the **LiveMigrationSupport** attribute to **TRUE** for all VMDg resources in a cluster.

5 Right-click the VMDg resource and select **Bring this resource online** option from the center pane of the failover cluster snap-in.

Creating a virtual machine service group

After adding a Volume Manager Disk Group (VMDg) resource, proceed with adding a virtual machine on the active failover cluster node.

Note: Virtual machine and virtual hard disk (.vhd) must be stored in the VMDg resource. This is required to make the virtual machine highly available.

To make the shared storage, i.e, the VMDg resource, available to the virtual machine, you must create the virtual machine on a cluster node that owns the storage. You can either create a new virtual hard disk (.vhd), use an existing .vhd as shown in the procedure below, or you can simply create it later.

To create a virtual machine

1 Click **Start > Administrative Tools > Failover Cluster Manager.**

If you are not connected to the cluster node that owns the shared storage connect to it.

2 Click on **Service and Applications > Virtual Machine > New > Virtual Machine** from the left pane of the Failover Cluster Manager console.

3 The New Virtual Machine Wizard is launched. Review the information on the welcome page.

Click **Next**.

4 On the Specify Name and Location page, specify a name for the virtual machine, for example, **VM1**.

5 Enable the checkbox **Store the virtual machine in a different location**, and then type the full path or click **Browse** and copy the virtual hard disk (VHD) file to the Volume Manager Disk Group (VMDg1) resource created in earlier section of this document for storing the virtual machine.

See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

6 On the Memory page, specify the amount of memory required for the operating system that will run on this virtual machine.

7 On configure Networking page, select the network adapter configured to use for Hyper-V.

8 On the Connect Virtual Hard Disk page, three options are shown:

- **Create a new virtual hard disk**
- **Use existing virtual hard drive**
- **Create virtual hard disk later**

Select the required option and give the path to the VHD (.vhd) file on the Volume Manager Disk Group (VMDg) resource.

The VHD (.vhd) file must be stored in a location where the VMDg resource is located.

9 Click **Finish** to close the wizard.

Setting the dependency of the virtual machine on the VMDg resource

As the virtual machine configuration and Virtual Hard Disk (VHD) file lie on the VMDg resource, you need to set a dependency of the virtual machine resource on the VMDg resource to make it highly available and live migrate it.

See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

See "Creating a virtual machine service group" on page 42.

Perform the following steps to set a dependency of the VMDg resource on the virtual machine:

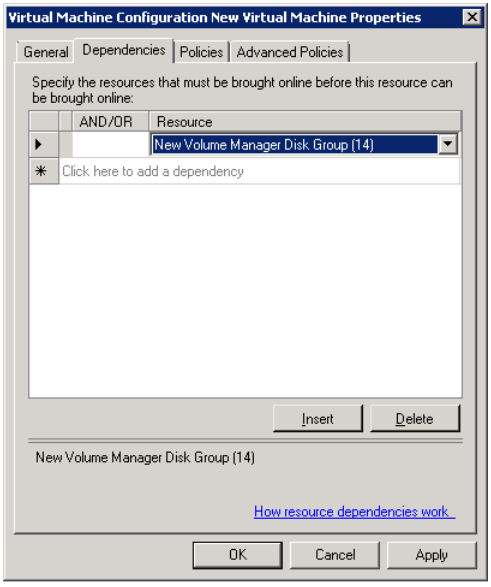
To set the dependency of the VMDg resource on the virtual machine

1. Right click the VMDg resource from the center pane of the Failover Cluster Manager console. Select **Actions > More Actions > Move this resource to another service group or application** from the menu.

   VMDg resource is now moved to the selected virtual machine.

2. From the center pane of console, select and expand the virtual machine resource to display the **Virtual Machine Configuration Resource.**

   Right-click and select **Properties > Dependency** tab to make this Virtual Machine Configuration Resource dependent on the Volume Manager Disk Group resource (VMDg).



   Select the VMDg resource that is displayed and click **Ok** to set the dependency.

   Now the virtual machine is ready to be live migrated to other cluster node.

   Refer to Microsoft documentation for details regarding live migrating a virtual machine.

Chapter 3

Administering storage migration for SFW and Hyper-V Virtual Machines

This chapter includes the following topics:

About storage migration

SFW provides the ability to move volumes to new storage locations via the Storage Migration Wizard. Storage Migration feature facilitates moving multiple volumes to different set of disks while the volumes are still online. Volumes associated with a Hyper-V Virtual Machine (VM) or a SFW disk group can be moved in a single administrative operation while the volumes are online without stopping the applications or Hyper-V VMs.

Storage migration provides administrators great flexibility when deploying new arrays or moving to LUNs that are configured for better performance. It can be used for the following use cases:

- To move data or volumes to disks that have enhanced performance

See "Moving data or volumes to disks with enhanced performance" on page 46.

- To move data or volumes that belong to a particular Hyper-V Virtual Machine to a different set of disks
  See "Moving data or volumes to disks with enhanced performance" on page 46.
- Migrating the volumes of a Hyper-V Virtual Machine from one enclosure or array to another
  See "Migrating the volumes of a Hyper-V Virtual Machine from one enclosure to another" on page 50.
- Converting or changing your existing Hyper-V configuration to a live migration supported configuration (one Hyper-V Virtual Machine per disk group)
  See " Converting your existing Hyper-V configuration to live migration supported configuration" on page 52.

Note: Volume layout and site boundary constraints are preserved during storage migration.

Limitations

Limitations for the storage migration feature are as listed below:

- All source and target disks selected for migrating purposes must belong to the same disk group.
- If the Hyper-V Virtual Machine configuration is spanning across multiple disk groups, then storage migration should be performed on a per disk group basis.

Note: RAID-5 volumes are not supported.

Moving data or volumes to disks with enhanced performance

Volumes belonging to a SFW disk group or Hyper-V Virtual Machine (VM) can be migrated to different disks in the same disk group using the Storage Migration Wizard. This wizard can be launched from the localhost, Disk Group node, and individual disk group node from the Veritas Enterprise Administrator (VEA) GUI.

Note: If you want to migrate to new disks, you must add the new disks to the disk group first.

To migrate SFW or Hyper-V Virtual Machine volumes to disks with enhanced performance, perform the following steps:

To migrate data or volumes

1 Select **localhost > Migrate Storage** from the VEA GUI to launch the Storage Migration Wizard.

Note: While connecting to the VEA console, if IP address is specified instead of **localhost**, then the specified IP Address is displayed.

Additionally, the Storage Migration Wizard can also be launched by selecting the Disk Groups or individual disk group node from the VEA GUI.

The Welcome page appears.

Click **Next**.

2 Select the source volume from the select source volume page and specify your storage preferences.

Note that the options displayed on the Select Source volume page depends on whether the storage migration wizard has been launched from the localhost, Disk Group node, or individual disk group node from the VEA GUI as described below:

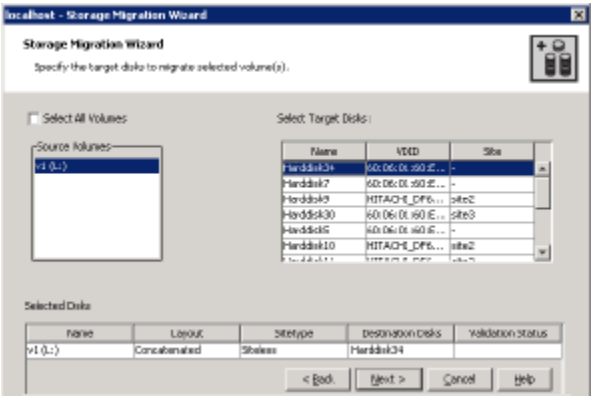
- If the wizard is launched from the VEA **localhost** node, then by default **Hyper-V Virtual Machines** option is selected and all the Hyper-V Virtual Machines are listed.
- If the wizard is launched from the VEA **DiskGroup** node, then by default **Disk Groups** option is selected and all the disk groups are listed.
  Select a particular disk group for storage migration. Note that you can select only one disk group at a time.
  All the volumes that are part of the disk group are listed in the **Select the volume from Disk Group\Virtual Machine** table. You can select either all the volumes or few volumes for migration. At least one volume must be selected.
  If the selected volumes are from different disk group, then an error message is displayed for restricting the selection to a single disk group.
- If the wizard is launched from an individual disk group node, i.e., the **Disks** node from the VEA, then by default **Disk Groups** option is selected and selected disk group is shown in the drop-down list.

Complete the following for source volume selection:

Disk Groups	Enable this option to choose disk group of your choice from the drop-down list. All disks in the selected disk group are displayed with Name, Layout, Sitetype, and other such disk related information in the **Select the volume from Disk Group\Virtual Machine** table.
Hyper-V Virtual Machines	Enable this option to select a Hyper-V virtual machine from the drop-down list for migration. Note that you can select only one Hyper-V VM at a time. Volumes belonging to the selected Hyper-V VM are listed in **Select the volume from Disk Group/Virtual Machine** table. All the VHD files that belong to the selected Hyper-V VM present on each volume are listed in the **Vhd files** column.
Select the volumes from Disk Group/Virtual Machine	Volumes belonging to selected disk group or Hyper-V VM are displayed. Select one or more volumes from the displayed list. Press **Ctrl** key to select multiple volumes for storage migration. **Note:** All the selected volumes must belong to a single disk group.

Click **Next** to continue.

3 On the select target disks page, select the source volumes and destination or target disks to migrate the preselected volume(s).



You can specify target disks per volume or for all the volumes in a single selection. Wizard displays the possible target disks based on source volume(s) selection.

Complete the following for target disk selection:

Source volumes	Destination disks can be selected either for each volume separately or for all the volumes at a time. Use **Select All Volumes** check box to select multiple volumes.
Select Target Disks	The possible target or destination disks are displayed based on your source volume(s) selection. Press **Ctrl** key to select multiple destination disks. Please note that at least one destination disk must be selected for each source volume.
Selected Disks	Selected target disks for each volume are displayed in the **Selected Disks** table. For each selected volume, its Sitetype, layout, and selected target or destination disks are displayed in this table.

Click **Next**.

Wizard validates the current selection. Constraints like disk space, volume layout, and Sitetype are validated.

4 On successful validation, Summary page is displayed with details of source volumes, target disk association, and other selected options like disk group name and virtual machine name.

Validate the information on the summary page and click **Finish** to exit the wizard.

5 To validate the status of storage migration (whether started or failed) for each selected volume, perform the following steps through the VEA console:

- Click the **Console** tab from the bottom panel of the VEA.
  Verify that separate **Subdisk move** tasks are created per subdisk on the bottom panel of the VEA.
- Now select the **Tasks** tab from the bottom panel of the VEA to check the progress of the Subdisk move operation for each subdisk.
  Wait for all Subdisk move tasks to complete.
- Select the **Disks View** tab to verify that all selected volumes are now migrated to the selected target or destination disks.

Migrating the volumes of a Hyper-V Virtual Machine from one enclosure to another

You can use the Storage Migration Wizard to migrate the volumes of a Hyper-V Virtual Machine (VM) from one enclosure or array to another while the VM/guest is in a running state. Before you start migrating the Hyper-V Virtual Machine volumes, it is recommended that you complete the following procedures:

- Creating disk groups and volumes
- Copying Virtual Hard Disks (VHDs) to volumes
- Creating a Hyper-V Virtual Machine and associating more VHDs to the Virtual Machine configuration

To migrate the volumes of Hyper-V Virtual Machine from one enclosure or array to another, perform the following steps:

To migrate volumes of a Hyper-V Virtual Machine

1. Launch the Storage Migration Wizard from the VEA GUI by right clicking the **localhost** node and selecting **Migrate Storage** option from the menu.

   Click **Next**.

2. The **Hyper-V Virtual Machine** radio button is selected by default. Select a Virtual Machine from the drop-down list.

   All the volumes associated with the selected Virtual Machine and related VHDs are displayed in **Select the volumes from Disk Group/Virtual Machine** table.

   Select few or all the volumes for migration.

   Click **Next**.

3. Target disks selection page is displayed.

   Target disks selection is possible for each individual volume or for all volumes. Note that multiple volume selection is not possible.

   Complete the following on this page:

   - To assign target disks for all the selected volumes, select the **Select All Volumes** checkbox.
   - To assign target disks for each individual volume, select individual volume under **Source Volumes**.
     All possible target disks based on volume(s) selection is shown by the wizard.
   - Select target disks belonging to a different enclosure from the **Select Target Disks** pane.
   - Selected destination disks for all source volumes are displayed in the **Selected Disks** table.
     Click **Next**.

4. Validate the information on the summary page and click **Finish** to exit the wizard.

5. To validate the status of storage migration (whether started or failed) for each selected volume, perform the following steps through the VEA console:

   - Click the **Console** tab from the bottom panel of VEA.
     Verify that separate **Subdisk move** tasks are created per subdisk on the bottom panel of the VEA.
   - Now select the **Tasks** tab from the bottom panel of the VEA to check the progress of the Subdisk move operation for each subdisk.
     Wait for all **Subdisk move** tasks to complete.

- Select the **Disks View** tab to verify that all selected volumes are now migrated to the selected target or destination disks.

Converting your existing Hyper-V configuration to live migration supported configuration

Through the Storage Migration Wizard, it is possible to convert your existing Hyper-V Virtual Machine (VM) configuration to a live migration supported configuration (one Hyper-V Virtual Machine per disk group).

Before trying to convert or change your existing Hyper-V Virtual Machine configuration to a Live Migration supported configuration, it is presumed here that you have completed the following procedures already:

- Creating disk groups and dynamic volumes
- Copying Virtual Hard Disks (VHDs) to volumes
- Creating at least two Hyper-V Virtual Machines (VMs)

To convert a Hyper-V Virtual Machine configuration to a live migration supported configuration, you need to perform the following steps:

To convert a Hyper-V configuration to a live migration supported configuration

1. To migrate volumes that belong to a Hyper-V Virtual machine to empty disks, launch the Storage Migration Wizard from the VEA GUI by right clicking on **localhost** node. Select the **Migrate Storage** option from the menu.
2. On the Source Volume page, select a virtual machine from the **Hyper-V Virtual Machines** drop-down list created by you.

   Select all the volumes that belong to the Hyper-V Virtual Machine.

   Click **Next**.
3. On the Target Disks selection page, target disks selection is possible for each individual volume or for all volumes.

   Note that multiple volume selection is not possible.

   Complete the following on this page:

   - To assign target disks for all the selected volumes, select **Select All Volumes** check box.
   - To assign target disks for each individual volume, select individual volume under **Source Volumes**
     Wizard shows all possible target disks based on volume(s) selection.
   - Select all the empty disks as target disks.

- Selected destination disks for all the source volumes are displayed in the **Selected Disks** table.
  Click **Next**.

4 Validate information displayed on the Summary page and click **Finish** to exit the wizard.

5 Now check storage migration status (whether successful or failed) by completing the following on the VEA:

- Click the **Console** tab on the bottom panel of the VEA.
  Verify that separate Subdisk move tasks are created per subdisk.
- Click the **Tasks** tab on the VEA to check the tasks progress in the bottom panel of the console.
  Wait for all Subdisk move tasks to complete.
- From the **Disk View** tab verify that all selected volumes are now migrated to the selected destination disks.

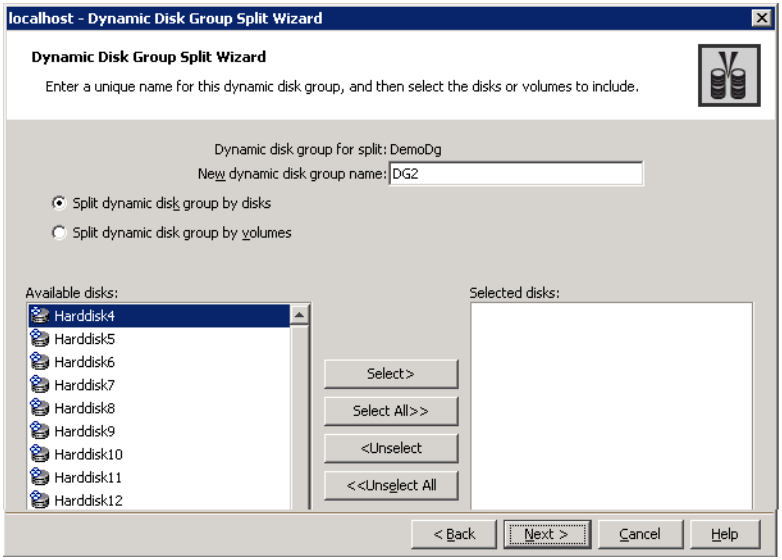
6 After storage migration completes successfully, split the disk group into two disk groups by selecting the dynamic disk group created by you already in the preceding sections. Right-click the disk group to launch the Split Dynamic Disk Group Wizard

OR

On the VEA, right-click a disk group to select the Split Dynamic Disk Group option.

Click **Next**.

7 Specify the **New dynamic disk group name** (Say **DG2**).



Select **Split dynamic disk group by disks** option.

Select the disks to which Hyper-V volumes are migrated as shown in step3.

Click **Next**.

8 The Summary page is displayed. Click **Finish** to exit the Wizard.

Now the configuration is changed to one virtual machine per disk group.

Chapter 4

Optional Storage Foundation for Windows features for Hyper-V environments

This chapter includes the following topics:

About using optional Storage Foundation for Windows features in the Hyper-V parent

Running Storage Foundation for Windows (SFW) in the Hyper-V parent partition offers benefits for virtual machines (VMs) that would otherwise be unavailable at the guest level.

SFW also offers advanced features and functionality, such as multi-pathing, replication, and snapshots, as product options. More information is available on how to use the following features and on the benefits they provide when running SFW in the Hyper-V parent:

- Using Dynamic Multi-pathing (DMP) to provide failover and load-balancing to the LUNs that host the VMs in the child partition (DMP Device Specific Modules option)
  See "Dynamic Multi-Pathing for the virtual environment" on page 56.
- Replicating VMs between sites (Veritas Volume Replicator option)
  See "Replicating virtual machines" on page 57.
- Maintaining Quick Recovery snapshots of the VMs (FlashSnap option)
  See "Virtual machine volume snapshots" on page 58.

In addition, running SFW in the parent partition facilitates implementing campus clusters (stretched clusters) in the Hyper-V environment.

See "Campus clusters" on page 59.

Dynamic Multi-Pathing for the virtual environment

Veritas Storage for Windows (SFW) offers the Dynamic Multi-pathing (DMP) feature. DMP provides an advanced multi-pathing solution for Hyper-V environments.

Multi-pathing software provides the intelligence necessary to manage multiple I/O paths between a server and a storage subsystem. This becomes even more important in virtual environments, where a single physical server hosts multiple operating system instances and applications. Loss of access to storage due to an HBA, cable or controller failure can cause widespread impact, with potential for greater disruption than would be the case with a single physical system.

In virtual environments, a hypervisor separates the VMs from the physical hardware, making it difficult to directly map virtual host bus adapters (HBAs) in the guest to the physical HBAs that service the physical host, and to therefore have a true multi-pathing solution in the guest. Installing DMP in the parent partition allows for true multi-pathing, providing failover and load-balancing to the LUNs that host the VMs in the child partition.

Most multi-pathing solutions are developed by storage vendors for their specific brand of storage and, as such, generally cannot service the many types of storage that can exist in today's heterogeneous SAN environments. In contrast, DMP is a truly heterogeneous solution. DMP fully integrates with the Microsoft Multipath I/O (MPIO) architecture. DMP includes several Device Specific Modules (DSMs) which provide array-specific support for a wide variety of the most popular array families available.

Replicating virtual machines

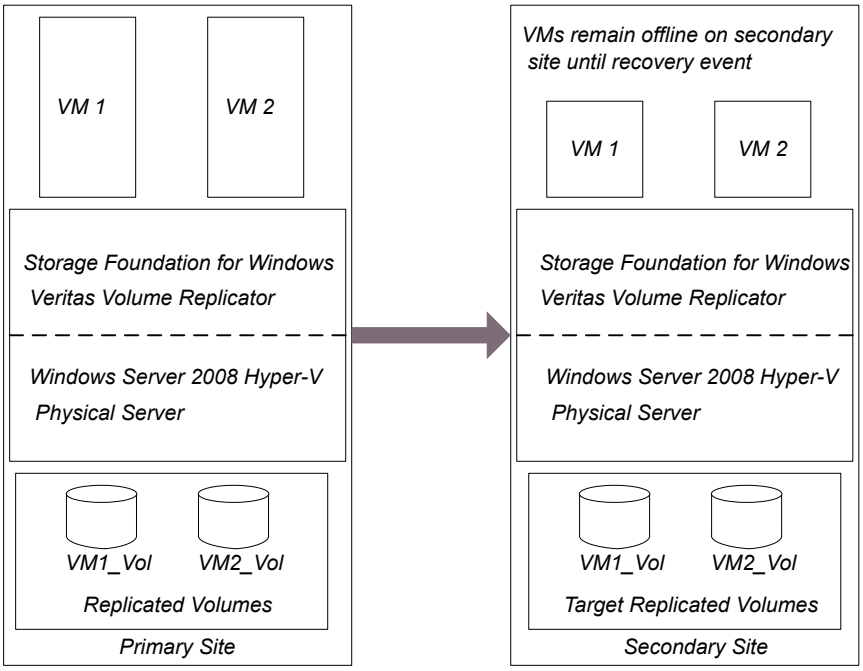
The Veritas Volume Replicator (VVR) option offered by Veritas Storage for Windows (SFW) provides a means to replicate virtual machine (VM) data.

While there are host-based technologies for replicating data across distances, they're usually expensive, requiring not only more storage, but also exactly the same hardware at both ends. They can also be limited in their ability to provide a solution that accounts not only for the data, but also for the applications that access it.

VVR runs at the host level, making it possible to replicate data volumes across distances to provide a means to extended disaster recovery without requiring that the hardware be exactly the same at both ends, and generally requiring less storage. But, while this works fine to protect application data in the guest, allowing recovery at the remote site, running in the guest does nothing to protect the VM.

By installing SFW and VVR in the parent partition, volumes that contain VHD files used for VMs and/or application data can be selectively replicated to remote sites, either synchronously or asynchronously, over an IP network. VVR uses a replicator log to store all writes to the volumes grouped together in what is known as a replicated volume group in the correct order and replicate them to the remote (secondary) site, maintaining write order fidelity, and thereby, consistency. The replicated VMs remain offline at the secondary site until required to be brought online, either due to an intentional migration of services from the primary site, or due to an outage at the primary site, requiring the secondary to take over services.

Figure 4-1 VVR in the parent partition



For planned outages at the primary (active) site, perhaps for a maintenance window, the primary role can be migrated to a secondary site, allowing the VMs that have been replicated to be brought online and applications that run on them to access data that has also been replicated to the secondary.

For unplanned outages at the primary site, operations can be moved to a secondary site via a takeover operation, which turns the secondary into an active primary, allowing VMs to be brought online. Depending on the mode of replication, they can either be completely up to date or behind the previous primary. In either event, consistency will be maintained and applications will be able to successfully attach to their data. The primary can be migrated back to the original site when it becomes available.

Virtual machine volume snapshots

Snapshot technology is available with the Veritas Storage for Windows (SFW) FlashSnap option. Running in the guest, snapshot copies of data volumes can be created, allowing for quickly recovering from a disaster, or for off-host operations, which can occur to another virtual machine (VM) or to a physical server connected

to storage shared with the guest when it uses pass-through disks. SFW also supports Microsoft's VSS framework for creating consistent snapshots.

However, this offers no protection against possible disaster that can occur at the VM level. If the VHD file that holds a VM is corrupted, the volume that hosts the VHD file(s) is lost, or the LUN hosting the volume used by the VHD file fails, snapshots in the guest will be useless until the VM can be rebuilt and the application(s) reinstalled.

By running SFW in the parent partition, you have the advantage of being able to create snapshots of the volumes containing the VHDs. These snapshots can be used to quickly recover the entire VM in the event of a disaster. They can also be moved to another server and brought online to be backed up or used for other operations such as testing.

Campus clusters

As a host-based volume manager, Veritas Storage Foundation for Windows (SFW) provides the ability to mirror volumes across arrays. Clusters which rely on shared storage can be stretched beyond the confines of a single datacenter to a datacenter located at a remote site, as long as the distance between the two datacenters doesn't exceed fiber channel latency limitations. These stretched clusters, also known as campus clusters, provide a level of high availability that can withstand a complete site failure.

SFW running in the parent partition can facilitate stretching of the failover cluster to another site by providing support for dynamic disks through its Volume Manager Disk Group cluster resource. With dynamic disks now available in the cluster, volumes can be mirrored across arrays which are located in different datacenters and are seen and shared by cluster nodes located in those respective datacenters. If the active site should experience a failure, virtual machines that were running at that site can be failed over to the cluster node at the other datacenter, and applications running on them can be brought back online.

Section 2

Veritas Cluster Server for Windows (VCS)

Chapter 5

Overview of the Disaster Recovery for Hyper-V solution

This chapter includes the following topics:

About wide-area disaster recovery for Microsoft Hyper-V

Veritas Cluster Server (VCS) for Windows introduces the Disaster Recovery Manager for Microsoft Hyper-V option to support wide-area disaster recovery for a Microsoft Hyper-V cluster.

Wide-area disaster recovery maintains data and critical services if a disaster affects a local area or metropolitan area. Data and critical services can be failed over to a site that is located hundreds or thousands of miles away.

A Microsoft failover cluster can provide high availability within a local site. This includes live migrating virtual machines (VMs) between local cluster nodes if a node fails. However, current disaster recovery solutions for VMs have limitations that reduce their effectiveness.

Wide-area disaster recovery with the Disaster Recovery Manager for Microsoft Hyper-V option provides new capabilities for a robust disaster recovery solution. A separate Disaster Recovery Manager VM is set up on the local and remote site to implement, monitor, and manage disaster recovery and replication.

Advantages of Disaster Recovery Manager for Microsoft Hyper-V

Wide-area disaster recovery with the Veritas Cluster Server (VCS) Disaster Recovery Manager for Microsoft Hyper-V option provides the following advantages:

- This easy-to-deploy solution embraces your existing Hyper-V environment and extends its capabilities with a true disaster recovery solution. High availability for the application virtual machines (VMs) is provided by Windows Failover Cluster, while disaster recovery is provided by the Disaster Recovery Manager for Hyper-V solution.
- Disaster recovery communication between sites is easily configured with the Hyper-V DR Manager Virtual Machine (VM) Configuration Wizard and monitored by a separate DR Manager VM at each site.
- The local and remote site can be on different subnets. The DR Manager VM enables automated configuration of network settings at both sites. The remote site's network settings are implemented automatically, upon failover, by the Symantec Network Updater Service.
- The DR Manager VMs monitor heartbeat communications between the local and remote cluster.
- The DR Manager VMs monitor the state of the application VMs and replication. No heartbeat is required between the DR Manager VM and the application VMs.
- If the local site fails, the DR Manager VMs handle the failover between sites, providing options for quickly bringing all application VMs online.

About the Disaster Recovery Manager for Microsoft Hyper-V configuration

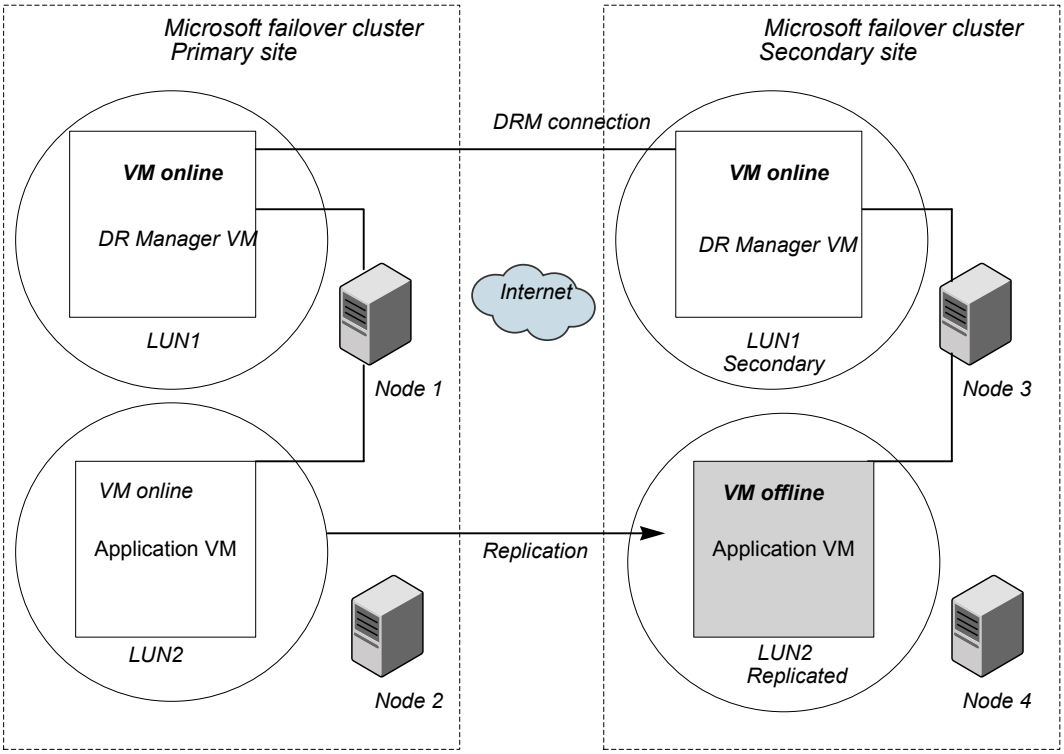
Wide-area disaster recovery for VMs with Disaster Recovery Manager uses the following configuration components:

- Separate Microsoft clusters are set up on the local (primary) and remote (secondary) site.

- The application VMs are configured for high availability within the Microsoft cluster on the local site.
  Disaster Recovery Manager includes support for configuring application VMs on storage managed as Storage Foundation for Windows (SFW) dynamic disk groups and volumes. SFW has added support for live migration and storage migration for Hyper-V VMs.
  See "Advantages of running Storage Foundation for Windows in the Hyper-V parent" on page 13.
- Hardware replication is set up to replicate the application VMs and data LUNs from the local to the remote site.
  Disaster Recovery Manager supports Hitachi TrueCopy or EMC SRDF replication.
- A separate VM for the Disaster Recovery Manager is set up on the local and remote sites on separate non-replicated storage. The Disaster Recovery Manager is installed on both VMs.
- Using the wizard provided, a connection is configured between the DR Manager VMs on the local and remote site, and other settings are configured for disaster recovery support.

As shown in the illustration, the application VMs and the DR Manager VM are online on node 1 of the Microsoft cluster on the primary site. On the secondary site the DR Manager VM is online on node 3 but the application VMs remain offline. If node 1 becomes unavailable, the VMs can fail over to node 2 on the primary site. If both node 1 and node 2 go down on the primary site, the DR Manager VM on the secondary site enables you to quickly bring the application VMs online on node 3.

Figure 5-1 VCS Hyper-V disaster recovery



How disaster recovery with Disaster Recovery Manager works

The Disaster Recovery Manager monitors the application virtual machines (VMs) in the Microsoft failover cluster. All the VMs that are being monitored by the Disaster Recovery Manager must fail to trigger the DR failover. Failover occurs at the site level, not at the individual VM level.

Optionally, the Disaster Recovery Manager can automate updating of network settings when the application VMs are failed over between sites. The local and remote DR site can be on different subnets. The application VMs at each site can therefore have different network settings.To implement automatic updating of network settings, you configure a network settings file for each site. The network settings are implemented automatically, upon failover, by the Symantec Network Updater Service, which is copied to the application VMs during disaster recovery configuration.

As part of the disaster recovery configuration process, you export the application VM configurations. Bringing the VMs online on the remote DR site imports the application VM configurations on the remote site and updates their network settings.

If the primary site fails, you use the Disaster Recovery Manager to bring the VMs online at the disaster recovery site. You can also manually initiate a failover at any time to test the disaster recovery solution.

See "Bringing the DR (secondary) site up if the primary site fails" on page 93.

Chapter 6

Deploying Hyper-V disaster recovery

This chapter includes the following topics:

Requirements for Disaster Recovery Manager

Disaster Recovery Manager has the following requirements:

Table 6-1 Requirements for Disaster Recovery Manager

Requirement	Description
Hardware	Hardware must meet the requirements specified in the Veritas Cluster Server for Windows 6.0 hardware compatibility list: http://www.symantec.com/docs/TECH152806
Operating system in Hyper-V parent	Windows Server 2008 R2 must be installed on the Hyper-V parents in the Microsoft cluster on the local (primary) and remote DR (secondary) sites.

Table 6-1 Requirements for Disaster Recovery Manager *(continued)*

Requirement	Description
Application virtual machines (VMs)	Application VMs can run the following Windows operating systems: ■ Windows Server 2008 ■ Windows Server 2008 R2 ■ Windows Vista ■ Windows 7 For details on supported versions, see the Veritas Cluster Server for Windows 6.0 software compatibility list: http://www.symantec.com/docs/TECH153742 Application VMs can be configured on shared storage LUNS as a CSV (cluster shared volume) or physical disk resource in the Microsoft failover cluster. If Storage Foundation for Windows (SFW) is installed in the parent, application VMs can be configured on shared storage as SFW dynamic disk groups and volumes and added to the cluster as Volume Manager Disk Group (VMDg) resources. See "Advantages of running Storage Foundation for Windows in the Hyper-V parent" on page 13. See "Tasks for deploying SFW Hyper-V virtual machine live migration support" on page 19. The application VMs are configured on the local (primary) site only. **Note:** Disaster Recovery Manager provides an optional feature to automate updating of network settings. To ensure that the automatic update works consistently, install a Microsoft hotfix as follows. For VMs running Vista or Windows Server 2008, see Microsoft KB 950134: http://support.microsoft.com/kb/950134/ For VMs running Windows 7 or Windows Server 2008 R2, see Microsoft KB 2530185: http://support.microsoft.com/kb/2530185

Table 6-1 Requirements for Disaster Recovery Manager *(continued)*

Requirement	Description
MAC address range	If the application VMs use dynamically generated MAC addresses, ensure that all Hyper-V hosts in the primary and secondary clusters use the same MAC address range. You can verify or configure the MAC address range setting with the Virtual Network Manager, available from the Microsoft Hyper-V Manager. In the **Virtual Network Manager** window, in the **Global Network Settings** section, select the **MAC Address Range** setting. Note that changing this setting does not affect network adapters that have already been created. To apply to existing adapters, recreate the adapter.
VMs for Disaster Recovery Manager	A separate VM, running Windows Server 2008 R2 x64 RTM or SP2, must be configured for the Disaster Recovery Manager on both the local (primary) and remote DR (secondary) site. The Disaster Recovery Manager software is installed within this VM. There are additional requirements for setting up the DR Manager VM. See "Preparing a VM for Hyper-V DR installation" on page 80.
Hardware replication	The sites must support Hitachi TrueCopy or EMC SRDF array-based replication for the application VMs. See "Setting up the hardware replication for disaster recovery" on page 77.
Disk space required	Approximately 824 MB of disk space is required for the Disaster Recovery Manager installation. If you implement the feature to update network settings automatically, the Symantec Network Updater Service is copied to the application VMs by the Disaster Recovery Manager during disaster recovery configuration. It requires a small amount of disk space.

Table 6-1 Requirements for Disaster Recovery Manager *(continued)*

Requirement	Description
Permissions and rights	Installing and configuring Disaster Recovery Manager requires local administrator permission for the Microsoft cluster systems, the DR Manager VM, and the application VMs. If configuring the feature to update network settings automatically, the application VMs must allow a connection to the administrative share to allow copying the Symantec Network Updater Service binaries to the application VMs.
Required services	The following services must be running inside the application VMs to support disaster recovery using Disaster Recovery Manager: ■ Hyper-V Integration Services (typically installed during Hyper-V installation) ■ Symantec Network Updater Service (optional) Installed on the application VMs during configuration of disaster recovery only if you want to implement the feature to update network settings automatically.
Required static IPv4 address	Each DR Manager VM must be configured with at least one static IPv4 address.
Firewall settings and ports	Ensure that the firewall settings allow access to the ports used by Disaster Recovery Manager. See "Ports used by Disaster Recovery Manager" on page 73.

Ports used by Disaster Recovery Manager

Ensure that the firewall settings allow access to the following ports that may be used by Disaster Recovery Manager.

Table 6-2 Ports used by Disaster Recovery Manager

Port number	Protocol	Description	Process
14150	TCP	Veritas Command Server	CmdServer.exe

Table 6-2 Ports used by Disaster Recovery Manager *(continued)*

Port number	Protocol	Description	Process
14141	TCP	Veritas High Availability Engine Veritas Cluster Manager (Java Console) (ClusterManager.exe) VCS Agent driver (VCSAgDriver.exe)	had.exe
7419	TCP	Symantec Plugin Host Service	pluginHost.exe
1556	TCP/UDP	Symantec Private Branch Exchange	pbx_exchange.exe
14149	TCP/UDP	VCS Authentication Service	vcsauthserver.exe
14144	TCP/UDP	VCS Notification	Notifier.exe
14155	TCP/UDP	VCS Global Cluster Option (GCO)	wac.exe

Workflow for deploying Hyper-V disaster recovery

To deploy Hyper-V disaster recovery for application virtual machines (VMs) in a Microsoft cluster using Disaster Recovery Manager, perform the following tasks in the sequence shown.

Table 6-3 Process for deploying Hyper-V disaster recovery

Action	Description
Review the requirements	Make sure that you understand the planned configuration and that your environment meets the hardware and software requirements. See "About the Disaster Recovery Manager for Microsoft Hyper-V configuration" on page 64. See "Requirements for Disaster Recovery Manager" on page 69.

Table 6-3 Process for deploying Hyper-V disaster recovery *(continued)*

Action	Description
On the local (primary) site, set up the application VMs for high availability in a Microsoft cluster	See the Microsoft documentation. Information is also available on configuring VMs on Storage Foundation for Windows (SFW) for live migration. See "Tasks for deploying SFW Hyper-V virtual machine live migration support" on page 19.
On a remote site, set up a Microsoft cluster for Hyper-V	On a remote (secondary) site, set up the desired number of nodes as part of a separate Microsoft cluster. More information is available on the requirements for the remote DR cluster. See "Configuration requirements for the remote disaster recovery cluster" on page 77.
Set up hardware replication between both sites	Disaster Recovery Manager supports EMC SRDF or Hitachi TrueCopy replication. See "Setting up the hardware replication for disaster recovery" on page 77.
On both sites, configure the VM to be used for the Disaster Recovery Manager	See "Preparing a VM for Hyper-V DR installation" on page 80.
On both sites, install the Disaster Recovery Manager	See "Installing the Disaster Recovery Manager for Hyper-V" on page 80.
On the local site, configure the disaster recovery connection between sites	On the local site DR Manager VM, run the Hyper-V DR Manager Virtual Machine (VM) Configuration Wizard. This wizard sets up the connection between the local and remote Disaster Recovery Managers. See "Configuring the disaster recovery connection to the remote site" on page 82.

Table 6-3 Process for deploying Hyper-V disaster recovery *(continued)*

Action	Description
On both sites, configure a network settings file	To implement automatic updating of the application VM network settings when the VMs are failed over between sites, configure two network settings files. One file contains the network settings for the application VMs on the local site. The other contains the network settings for the application VMs on the remote site. See "Configuring automatic update of network settingss" on page 83.
On the local site, export the application VM configurations	See "Exporting application VM configurations" on page 84.
On the local site, run the script to finish configuring DR for the VMs	See "Running the script to set up the disaster recovery configuration for the application VMs" on page 85.
Verify that the DR configuration is successful using the VCS Java Console	Use the VCS Java Console to connect to the Disaster Recovery Manager and to verify that configuration was successful See "Connecting to the Disaster Recovery Manager with the Java Console" on page 88.
(Optional) Manually switch the application VMs between sites	Optionally, manually switch the application VMs between sites using the VCS Java Console. See "Manually failing over the VMs between sites" on page 90.
If the primary site goes down, bring the secondary site up	Use the VCS Java Console to bring the secondary site up if the primary site fails. **Note:** In addition, only for VMs configured on Storage Foundation for Windows storage, configure a dependency in the Microsoft failover cluster on the DR site between the VM resources and the VMDg resources. See "Bringing the DR (secondary) site up if the primary site fails" on page 93.
If application VMs are added or removed, update the configuration	See "Adding or removing application VMs" on page 96.

Configuration requirements for the remote disaster recovery cluster

Disaster recovery for Hyper-V VMs using Disaster Recovery Manager requires setting up a separate Microsoft failover cluster on a remote site. Note the following requirements for the remote (secondary) disaster recovery (DR) cluster:

- Ensure that the remote DR cluster is in the same domain as the local (primary) cluster.
- Ensure that the systems that form the cluster nodes of the remote DR cluster meet the same hardware and software requirements as the local cluster.
- When configuring Hyper-V on the remote DR cluster, set up the same virtual network switches as on the local (primary) site.
- If the application VMs use dynamically generated MAC addresses, ensure that all Hyper-V hosts use the same MAC address range as on the local cluster. To verify or configure the MAC address range setting, use Virtual Network Manager, available from the Hyper-V Manager. In the **Virtual Network Manager** window, in the **Global Network Settings** section, select the **MAC Address Range** setting.
- Create cluster shared volumes (CSVs) or physical disk resources on the secondary cluster to match what was set up for the application VMs on the primary cluster.
  If the application VMs are configured on SFW storage, create the appropriate Volume Manager Disk Group (VMDg) resources on the secondary cluster to match what was set up for the application VMs on the primary cluster.
  See "Adding the Volume Manager Disk Group (VMDg) resource" on page 39.

Note: CSV or SFW (VMDg) resources created on the secondary cluster will remain in a FAILED state until a failover occurs and replication roles reverse.

Setting up the hardware replication for disaster recovery

As part of the workflow for setting up disaster recovery for Hyper-V VMs using Disaster Recovery Manager, configure hardware replication for the application VMs and their associated storage.

Note: Configure replication only for the application VMs and their associated storage. Do not configure replication for the DR Manager VM and its associated storage.

The hardware replication must be set up before you can configure disaster recovery with the Disaster Recovery Manager.

The Disaster Recovery Manager supports EMC SRDF replication and Hitachi TrueCopy replication. It uses agents to monitor the replication.

The replication agents do not support specialized software solutions that the array vendor may have developed for cluster shared volumes (CSV).

The following topics cover the requirements for configuring replication to work with the Disaster Recovery Manager.

See "Prerequisites for EMC SRDF replication with Disaster Recovery Manager" on page 78.

See "Prerequisites for Hitachi TrueCopy replication with Disaster Recovery Manager" on page 79.

Prerequisites for EMC SRDF replication with Disaster Recovery Manager

The Disaster Recovery Manager supports EMC SRDF replication. Before you configure the Disaster Recovery Manager, you must configure the replication for the application VMs and their associated storage.

Note: Do not configure replication for the DR Manager VM and its associated storage.

The Disaster Recovery Manager includes agent software that supports SYMCLI versions that EMC recommends for the firmware on the array. The agent supports SRDF on all microcode levels on all Symmetrix arrays, provided that the host/HBA/array combination is in EMC's hardware compatibility list.

To enable the Disaster Recovery Manager to configure the required agent settings for EMC SRDF, ensure that the following software requirements are met:

- The EMC Solutions Enabler is installed on all cluster nodes.
- The SYMCLI version that is installed supports the generation of XML output.
- The SYMCLI version and the microcode level support dynamic swapping.

The agent has the following requirements for EMC SRDF replication:

- The device group must not span more than one array (no composite device groups).
- Dynamic swap must be enabled on both sites.
- On the local site:
  - All devices must be RDF1 and part of an RDF1 device group.
  - Devices must have write access.
- On the remote DR (secondary) site:
  - All devices must be RDF2 and part of an RDF2 device group.
  - Write access must be disabled.
- Device group configuration must be the same on all nodes of the cluster.

Prerequisites for Hitachi TrueCopy replication with Disaster Recovery Manager

The Disaster Recovery Manager supports Hitachi TrueCopy replication. Before you configure the Disaster Recovery Manager, you must configure the replication for the application VMs and their associated storage.

Note: Do not configure replication for the DR Manager VM and its associated storage.

Disaster Recovery Manager includes an agent that supports all versions of Hitachi RAID Manager.

Ensure that the following requirements are met before configuring the Disaster Recovery Manager:

- RAID Manager is installed on the DR Manager VMs.
- The horcm files are named horcmnn.conf (where nn is a positive number without a leading zero, for example, horcm1.conf but not horcm01.conf).
- All configured instances are running.
- The device group does not span more than one array.
- At the local (primary) site, all devices are of the type P-VOL.
- At the remote DR (secondary) site, all devices are of the type S-VOL.
- All device groups at the local (primary) site are paired to an IP address which must be online on the remote DR (secondary)node.

- Device group and device names include only alphanumeric characters or the underscore character.

Preparing a VM for Hyper-V DR installation

Prepare a Hyper-V virtual machine (VM) for the Disaster Recovery Manager as follows:

- Set up a separate DR Manager VM in the Microsoft Hyper-V cluster on both the local (primary) and remote DR (secondary) site.
- The DR Manager VMs must be in the same Active Directory domain as the Microsoft failover clusters.
- For the DR Manager VM operating system, install Windows Server 2008 R2 x64 RTM or SP2.
- Install the Microsoft failover cluster management tools on the DR Manager VMs.
- Configure at least one static IPv4 address on each DR Manager VM.
- Enable PowerShell Remoting on the DR Manager VMs.
- Configure the storage for the DR Manager VM on a separate (non-replicated) LUN from the application VMs.
- Install and configure the array replication management software on the DR Manager VMs.
- Configure the arrays to give the DR Manager VMs access to the array hardware gateway (command) devices. This is required during Disaster Recovery Manager configuration.
- On the local (primary) site, set up the DR Manager VM for failover within the local Microsoft failover cluster.

Installing the Disaster Recovery Manager for Hyper-V

Install the Veritas Cluster Server for Windows (VCS) Disaster Recovery Manager for Hyper-V on the DR Manager virtual machines (VMs). Before installing, ensure that you have met the requirements.

See "Requirements for Disaster Recovery Manager" on page 69.

See "Preparing a VM for Hyper-V DR installation" on page 80.

To install the Disaster Recovery Manager for Hyper-V

1. From any system that can connect to the DR Manager VMs, insert the disc containing the installation software into the system's disk drive or download the VCS 6.0 for Windows package from the Symantec Web site.

   https://fileconnect.symantec.com

2. Allow the autorun feature to start the installation or double-click **Setup.exe**. The CD browser appears.
3. Select **Veritas Cluster Server 6.0**.
4. On the Welcome panel, review the list of prerequisites and click **Next**.
5. On the License panel, read the license terms, select **I accept the terms of License Agreement,** and then click **Next**.
6. On the System Selection panel, make the following selections:
   - Select both DR Manager VM(s) for installation. You can install on multiple systems.
   - By default the wizard uses `%ProgramFiles%\Veritas` as the installation directory. To customize the installation directory, click **Browse** and select the desired location, then click **OK**.
   - Select the required license type from the **License key** drop-down list.
     The default license type is "Keyless".
     If you select the "Keyless," all the available product options are displayed and are selected by default.
     If you select "User entered license key," the License Details panel appears by default. On the License Details panel, enter the license key and then click **Add**.
     The wizard validates the entered license keys. After the validation is complete, click **OK**.
   - From the product options list, select the **Disaster Recovery Manager for Microsoft Hyper-V** option to install on both VMs.
7. When you have completed all selections on the System Selection panel, click **Next**.

   If the validation checks have failed, review the details and rectify the issue. Then select the system and click **Re-verify** to re-initiate the validation checks for this system.

8 On the Pre-install Summary panel, review the summary and click **Next**.

Note that **Automatically reboot systems after installer completes operation** is selected by default. If you do not want the wizard to initiate this auto reboot, clear the selection.

9 When installation is complete, click **Next**.

10 On the Post-install Summary panel, review the installation result and click **Next**.

If the installation has failed, refer to the log file for details. You may have to reinstall the software.

11 On the Finish panel, click **Finish**.

If you chose the auto reboot, a confirmation message appears. Click **Yes** to reboot immediately or **No** to reboot later.

If you did not choose the auto reboot, ensure that you manually restart.

Configuring the disaster recovery connection to the remote site

After installing Disaster Recovery Manager on both DR Manager VMs, configure the connection between the DR Manager VMs on the local site and remote DR site.

To perform this configuration, use the Hyper-V DR Manager Virtual Machine (VM) Configuration Wizard. The wizard is launched when you log on to the DR Manager VM after product installation. You can also launch it from the **Start** menu.

To run the wizard you must be a domain user with administrator rights on both DR Manager VMs.

To configure the disaster recovery connection to the remote site

1 Launch the Hyper-V DR Manager VM Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Launch Hyper-V DR Manager VM Configuration Wizard**

2 Specify the following information using the wizard:

- The host name of the DR Manager VM on the remote DR (secondary) site.
- Administrator account credentials for the local Microsoft cluster.
- Administrator account credentials for the remote (secondary) Microsoft cluster (if different from the local cluster).

Configuring the disaster recovery settings for the application VMs

The VM Monitoring script configures the Disaster Recovery Manager with the settings needed to perform disaster recovery for the application virtual machines (VMs).

Complete the following tasks before you run the script:

See "Configuring automatic update of network settingss" on page 83.

See "Exporting application VM configurations" on page 84.

Configuring automatic update of network settingss

The DR Manager VM enables automated configuration of network settings when the application virtual machines (VMs) are failed over between sites. The local and remote DR site can be on different subnets. The application VMs at each site can therefore have different network settings.

To implement automatic updating of the application VM network settings, you must configure two network settings files, one for each site. The file on the local site contains the network settings used on the local site for each application VM. The file on the remote site contains the network settings to be used on the remote site for each application VM. The network settings in the file are implemented automatically, upon failover, by the Symantec Network Updater Service, which is copied to the application VMs during disaster recovery configuration.

Configure the network settings file as a comma separated values (.csv) file. The file must list the following network settings, separated by commas, for each VM in the cluster, in the order shown:

- Application VM name
- Mac address
- IP address
- Subnet mask
- Gateway address
- DNS server address

The following would be an example of a .csv file containing settings for two VMs, IISVM and SQLVM:

```
#VMName,MAC,IP,Subnet,Gateway,DNSServer
IISVM,00:15:5D:6D:5B:03,10.182.105.210,255.255.240.0,10.182.96.1,10.182.144.50
SQLVM,00:15:5D:6D:5B:11,10.182.105.212,255.255.240.0,10.182.96.1,10.182.144.50
```

Note: Application VMs can use multiple IP addresses or network interfaces.

When you run the VM Monitoring PowerShell script, supply the file name and full path of the network settings files on each site. A separate menu selection of the script deploys the Network Updater Service to the application VMs.

Note: Application VMs require installing a Microsoft hotfix to ensure that the automatic update works consistently. For more information, see the requirements for application VMs.

See "Requirements for Disaster Recovery Manager" on page 69.

Warning: If you add or remove VMs, ensure that you update the contents of the network settings files on both sites.

Exporting application VM configurations

The export-VM PowerShell script is supplied with the Disaster Recovery Manager. This script exports the configuration for the specified application virtual machine (VM). Only application VMs with exported configurations are failed over to the disaster recovery site.

Complete the export step before running the VM Monitoring PowerShell script to set up disaster recovery for the application VMs.

See "Running the script to set up the disaster recovery configuration for the application VMs" on page 85.

The export script requires the exact VmStoreRootPath (the path to the VM configuration location). You can retrieve this from the Virtual Machine Configuration resource in the Microsoft failover cluster.

The default path of the script is `%vcs_home%\bin`, where `%vcs_home%` is the installation path of the product. For example: `%ProgramFiles%\Veritas\Cluster Server\bin`

To export the application VM configuration

1. Shut down the VM.
2. From the command prompt on the local DR Manager VM, type:

   `export-VM.ps1 <ClusterName> <VMName> <RemoteExportPath>`

   Use quotes around any text strings that contain spaces.

   For example:

   ```
   export-vm.ps1 "PRI Cluster" VM1
   C:\ClusterStorage\Volume1\VM1\export
   ```

   Where the values for the variable parameters are as follows:

ClusterName	The name of the local Microsoft failover cluster Example: `"PRI Cluster"`
VMName	The name of the VM for which you are exporting the configuration Example: `VM1`
RemoteExportPath	The path to use for the export on the remote cluster.This must use the VMStoreRootPath, as follows:*VMStoreRootPath*`\export` Example: `C:\ClusterStorage\Volume1\VM1\export`

Running the script to set up the disaster recovery configuration for the application VMs

The VM Monitoring PowerShell script is supplied with the Disaster Recovery Manager. Run this script to set up the initial DR configuration for the application virtual machines (VMs). Run it again whenever you add or remove VMs.

The script will change the **Cluster-Controlled Offline Action** setting on the VM cluster resources in the Microsoft cluster from the default of **Save** to **Shutdown (Forced)**. This setting change is required for the VMs to properly fail over to the recovery site.

The default path of the script is `%vcs_home%\bin`, where `%vcs_home%` is the installation path of the product. For example: `%ProgramFiles%\Veritas\Cluster Server\bin`

Before running the script, complete the following steps:

- Export the configurations for all application VMs to be configured for disaster recovery.
  The script lists the export status for each VM so that you can verify whether you omitted any required exports.
  See "Exporting application VM configurations" on page 84.
- Ensure that hardware replication is configured.
  The script requires some hardware replication information, as described below. Ensure that you complete the hardware replication setup before running the script.
  See "Setting up the hardware replication for disaster recovery" on page 77.
- To enable the optional feature for automatic update of network settings, the script requires the local and remote file name and path of the network settings files. In addition, the script provides a menu option to deploy the Symantec Network Updater Service. Before selecting that option, make sure that application VMs allow a connection to the administrative share.
  See "Configuring automatic update of network settingss" on page 83.

To run the script to set up the disaster recovery configuration for the application VMs

1. From the command prompt on the local DR Manager VM, type:

   ```
   configure-HyperV-VM-monitoring.ps1
   ```

   The script discovers and lists the following information; if discovery fails, it will prompt for the information:

   - The names of the local and remote DR Manager VM
   - The names of the local and remote Microsoft failover cluster

2. The script displays the main menu. Type **1** and press **Enter** to select option 1, **Configure Disaster Recovery Monitoring of the application VMs**.

   The script discovers the VMs on the local Microsoft failover cluster. It lists the VM name, the path where the VM is stored, whether the configuration is exported, the VM state, and the name of the physical host on which the VM resides.

   The script notifies you of the required change to the Cluster-Controlled Offline Action setting.

3. Review the list of VMs to ensure that all the application VMs that you want to configure for disaster recovery have exported configurations. Either export any missing configurations after running the script, or type **n** to exit the script and do the export.

4 To continue with the script, type **y** and press **Enter**.

5 To enable updating of network settings, specify the following information when prompted by the script; otherwise, press **Enter** to skip these steps:

Local cluster's network settings file path	The local path and file name of the file that contains the network settings for the application VMs. Example: `C:\primary-nw-settings.csv` See "Configuring automatic update of network settingss" on page 83.
Remote cluster's network settings file path	The remote path and file name of the file that contains the network settings for the application VMs. Example: `C:\dr-nw-settings.csv`

6 Choose the type of replication by typing **H** for HTC or **E** for EMC SRDF and press **Enter**.

7 Type the requested replication information as follows and press **Enter**:

- If configuring Hitachi TrueCopy replication, respond as follows:

`Enter a TrueCopy Device Group Name`	Enter the name of the Hitachi TrueCopy device group that contains the LUNs for the selected instance. The same device group name is used on both sites.
`Enter the instance number of the TrueCopy Device Group`	Enter the instance number of the device group. Multiple device groups may have the same instance number. The same instance number is used on both sites.

- If configuring EMC SRDF replication, enter the name of the Symmetrix device group.

8 The replication prompt is displayed again to allow for entering information for multiple device groups.Once you have entered all the information, press **Enter** again to continue with the script.

A summary of the configuration information is displayed.

9 If satisfied with the configuration, type **y** and press **Enter**.

The script configures the disaster recovery settings according to the information provided.

10 Choose one of the following:

- If you do not want to enable the automatic update feature for network settings, you have completed the script. Type **quit** and press **Enter** to exit.
- To enable the automatic update feature for network settings, you must deploy the Network Updater Service. The deployment can take some time. If you want to deploy now, type **2** and press **Enter**.
  The script connects to each VM to copy and register the Symantec Network Updater Service.

Use the VCS Java Console to verify that the DR configuration was successful.

See "Connecting to the Disaster Recovery Manager with the Java Console" on page 88.

Connecting to the Disaster Recovery Manager with the Java Console

Use the Veritas Cluster Server (VCS) Cluster Manager Java Console to connect to the Disaster Recovery Manager. You can use the Java Console to do the following:

- Verify that the DR Manager configuration was successful
- Switch application VMs between sites
- Bring the secondary site online because of a primary site failure

For a complete description of all Java Console features, see the *Veritas Cluster Server Administrator's Guide*.

To connect to the Disaster Recovery Manager with the Java Console

1 If using a firewall, ensure that you have added ports 14141 and 14150 for firewall exceptions.

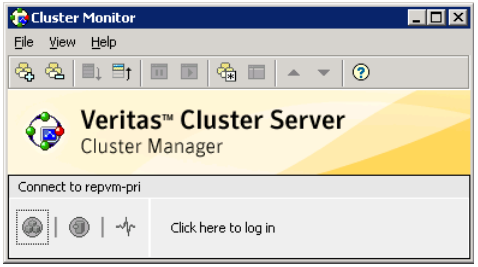
2 Start the Java Console: Click **Start > All Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console**

The first window that appears is Cluster Monitor. The local and remote DR Manager VMs are each a separate VCS cluster. You will add cluster panels for the DR Manager clusters and then logon to complete the connection.

3 Add a cluster panel for the local DR Manager VM cluster, as follows:

- In Cluster Monitor, click **File > New cluster**.

- In the **Host Name** field, enter the host name or IP address of the local DR Manager VM.
- Click **OK**.
  The local DR Manager cluster panel is added, as shown in the illustration. The panel is inactive (not connected to the cluster) until you log on.

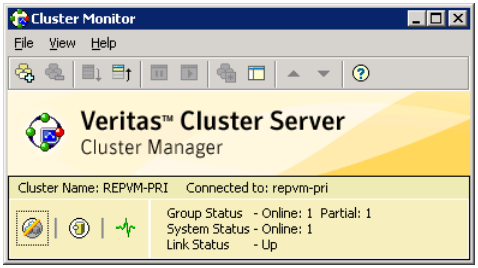


4 To add a cluster panel for the remote DR Manager VM cluster, repeat the previous step, but this time specify the host name or IP address of the remote DR Manager VM in the **Host Name** field.

5 To log on to a cluster panel:

- Click on the inactive cluster panel. The logon dialog box is displayed.
- Enter the credentials of a native user. You can use nis or nis+ accounts or accounts set up on the local system. If you do not enter the name of the domain, VCS assumes the domain is the local system.
- Click **OK**.

The cluster panel changes color and displays connection status.

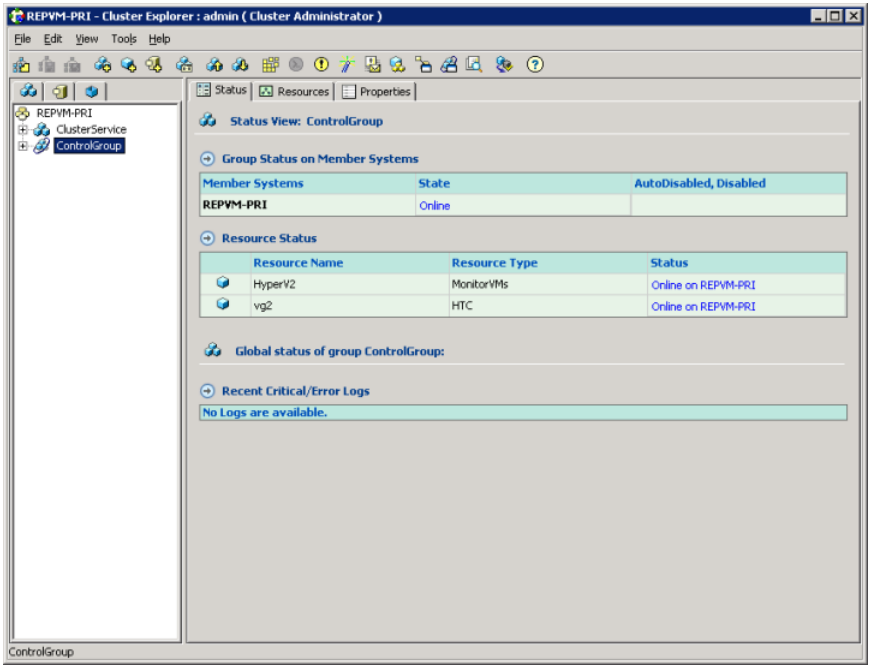


The Cluster Explorer is launched automatically upon initial logon.

6 To verify that the DR configuration was successful, continue with the following step. Otherwise, see one of the following topics for additional tasks that you can perform from the Java Console:

- See "Manually failing over the VMs between sites" on page 90.
- See "Bringing the DR (secondary) site up if the primary site fails" on page 93.

7 To verify that the DR configuration was successful, logon to the primary site cluster panel and do the following steps from the Cluster Explorer for the primary site:



- By default the Service Groups tab is selected in the left pane configuration tree, and the tree displays the **ControlGroup** node. Select **ControlGroup**.
- In the right pane, check that in the **Status** view, the **Group Status on Member Systems** shows the state of the primary DR Manager VM as **Online**, as shown in the illustration.
- If the state is not **Online**, in the configuration tree, right-click **ControlGroup** and click **Online**.

Manually failing over the VMs between sites

You can use the Veritas Cluster Server (VCS) Cluster Manager Java Console to test the DR failover manually when the primary site is still online. The failover brings

the application VMs offline on the primary (local) site cluster and online on the secondary (remote) cluster.

If the primary site has failed, use the procedure in the following topic instead of the procedure below:

See "Bringing the DR (secondary) site up if the primary site fails" on page 93.

You can test the failover from either the primary or secondary site. The instructions in the following procedure demonstrate logging on to the Java Console and DR Manager VM cluster on the secondary site.

Before doing this procedure, complete the steps to connect to the Java Console and verify the configuration.

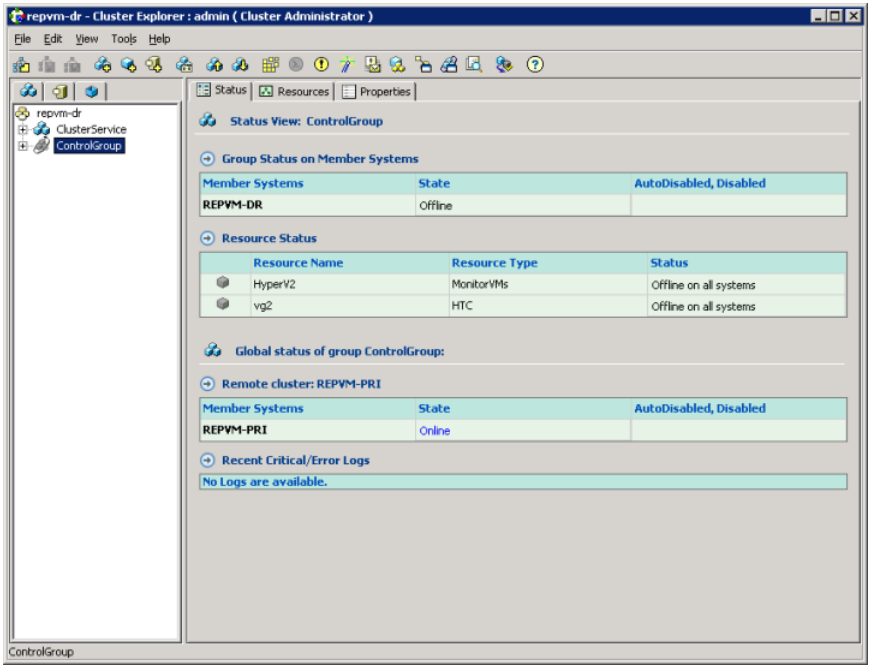
See "Connecting to the Disaster Recovery Manager with the Java Console" on page 88.

To manually fail over the VMs between sites

1. On the secondary site, launch the Java Console from the DR Manager VM. From the Start menu, click **Start > All Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console**
2. If you have not yet done so, use the Java Console Cluster Monitor to log on to the cluster panel for the secondary DR Manager VM.

   See "Connecting to the Disaster Recovery Manager with the Java Console" on page 88.

3 Cluster Explorer for the secondary DR Manager VM is launched upon logon. In the configuration tree, select **ControlGroup**.

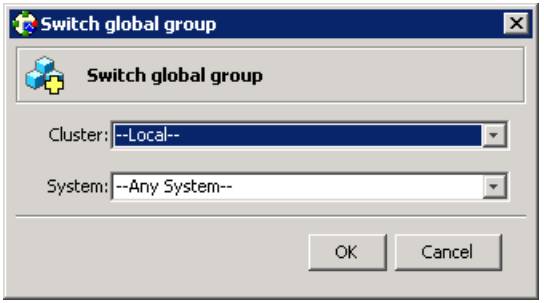


If you are logged on to the secondary site (DR) cluster, the **Status** view shows the group status for the secondary DR Manager VM as **Offline**, as shown in the illustration. The status for the primary site cluster is listed under **Remote cluster** and shown as **Online**.

4 In the configuration tree, right-click **ControlGroup**.

5 Click **Switch To**, and click **Remote switch**.

The **Switch global group** dialog box is displayed.



6 In the **Switch global group** dialog, the default shown in the **Cluster** field is **Local** (for the DR Manager cluster you are logged onto). If you are logged onto the secondary site DR Manager cluster, leave the selection as **Local** and click **OK**. (Since there is only one DR Manager VM on each site, no selection is needed in the **System** field.)

   If you are logged onto the primary site cluster instead, select the name of the secondary DR Manager in the **Cluster** list.

7 When prompted, confirm the switch. In the Cluster Explorer **Status** view, verify that the state of the secondar DR Manager VM changes from **Offline** to **Online**.

8 Confirm that the application VMs are online on the secondary site using the Windows failover cluster management console.

9 If you configured automatic update of network settings, verify that the settings are updated. In some cases, upon the very first failover, Windows detects configuration changes in the application VM and displays a message prompting you to restart the computer to apply the changes. If settings are not updated, check for this message and restart the VM.

10 If VMs are configured on SFW storage, then the first time the VMs are failed over, you must configure the resource dependency between the application VM resource and the VMDg resource.

   See "Setting the dependency of the virtual machine on the VMDg resource" on page 43.

To switch the application VMs back to the primary site

1 In the Cluster Explorer configuration tree, right-click **ControlGroup**.

2 Click **Switch To**, and click **Remote switch**.

3 In the **Switch global group** dialog box, if you are logged onto the secondary site DR Manager VM cluster, ensure that the **Cluster** field displays the name of the DR Manager VM for the primary site. Click **OK**.

4 In the Cluster Explorer **Status** view, verify that the state of the primary site DR Manager VM cluster changes to **Online**.

Bringing the DR (secondary) site up if the primary site fails

If the primary site fails, use the Veritas Cluster Server (VCS) Cluster Manager Java Console to connect to the Disaster Recovery Manager and bring the secondary site online.

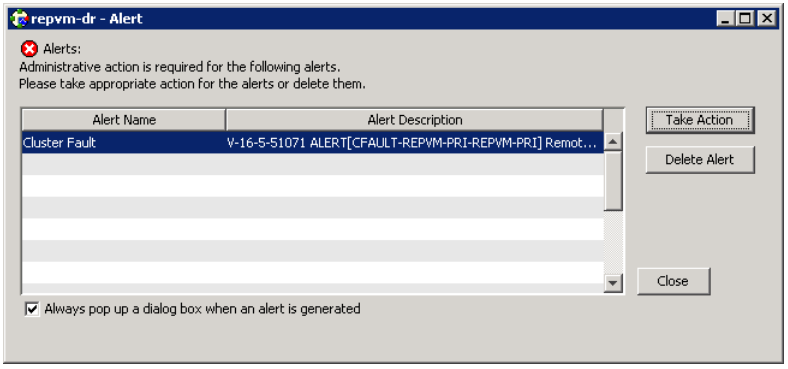
For a complete description of all Java Console features, see the *Veritas Cluster Server Administrator's Guide*.

The following procedure assumes that in a disaster recovery scenario, you are running the VCS Java Console from the DR Manager VM on the secondary site, since the primary site is down.

To bring the DR (secondary) site up if the primary site fails

1. On the secondary site, launch the Java Console from the DR Manager VM. From the Start menu, click **Start > All Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console**
2. If you have not yet done so, in the Java Console, log on to the secondary site DR Manager VM cluster panel.

   See "Connecting to the Disaster Recovery Manager with the Java Console" on page 88.
3. If the primary site cluster has failed in a disaster recovery scenario, the **Alert** dialog box is displayed by default when you logon to the secondary site cluster:



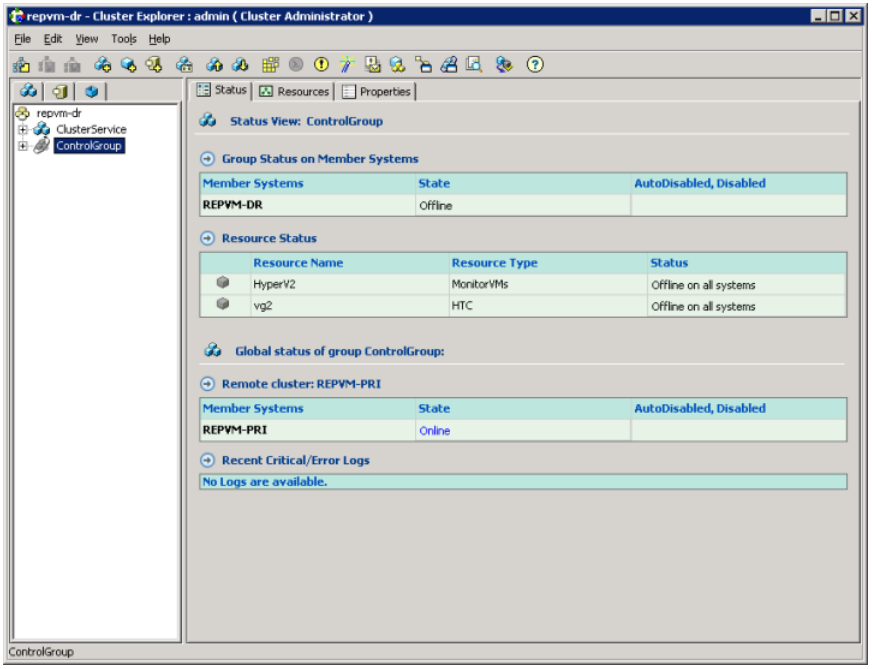
   If the Alert dialog box is displayed, continue with the following steps. Otherwise, skip to step 7.
4. On the **Alert** dialog box, click **Take Action**.

   The **Declare Cluster** dialog box is displayed.
5. On the **Declare Cluster** dialog box, in the **Declare** field, select **Disaster**, and then select the name of the secondary DR Manager VM cluster and click **OK**.

   In Cluster Explorer, verify that the **Status** view shows the secondary DR Manager VM cluster as **Online**.
6. Confirm that the application VMs are online on the secondary site using the Windows failover cluster management console

7 If the Alert message is not displayed, but the primary site is down, you can use Cluster Explorer to bring the DR Manager cluster online on the secondary site, as follows:

- In the Cluster Explorer configuration tree, select **ControlGroup**
  The **Status** view shows the secondary DR Manager VM as **Offline**, as shown in the illustration.



8 In the configuration tree, right-click **ControlGroup**, click **Online**, and select the name of the secondary DR Manager VM.

9 In Cluster Explorer, verify that the **Status** view shows the secondary DR Manager VM cluster as **Online**.

10 Confirm that the application VMs are online on the secondary site using the Windows failover cluster management console.

11 If you configured automatic update of network settings, verify that the settings are updated. In some cases, upon the very first failover, Windows detects configuration changes in the application VM and displays a message prompting you to restart the computer to apply the changes. If settings are not updated, check for this message and restart the VM.

12 If VMs are configured on SFW storage and have not previously been failed over to the DR site, you must configure the resource dependency between the application VM resource and the VMDg resource.

See "Setting the dependency of the virtual machine on the VMDg resource" on page 43.

Adding or removing application VMs

If you add or remove application VMs after you have configured disaster recovery with the Disaster Recovery Manager, ensure that you do the following steps:

- If using the feature to enable automatic update of the network configuration upon failover, ensure that you update the network settings files on both sites.
  See "Configuring automatic update of network settingss" on page 83.
- If you added a VM, export the configuration.
  See "Exporting application VM configurations" on page 84.
- Run the VM Monitoring PowerShell script to ensure that the correct VMs are monitored for disaster recovery.
  See "Running the script to set up the disaster recovery configuration for the application VMs" on page 85.

Chapter 7

Hyper-V DR agent

This chapter includes the following topics:

About the Hyper-V DR agents

Disaster Recovery Manager is a special feature of Veritas Cluster Server (VCS) for Windows. The installation includes the following Veritas Cluster Server (VCS) agents:

- Hardware replication agents
- The Monitor VMs agent (MonitorVMs) for Disaster Recovery Manager

The MonitorVMs agent monitors the health of application VMs that are configured for disaster recovery failover. The configuration wizard for the Disaster Recovery Manager creates a VCS global service group on the local (primary) and remote DR (secondary) sites. The configuration scripts then create the following resources and dependencies in the VCS global service group:

- A MonitorVM resource is created for each application VM that you configure for Hyper-V disaster recovery.
- A replication resource is created for each storage resource associated with the application VMs.
- The MonitorVM resource depends on the storage replication resource.

The following information is provided for troubleshooting purposes. For more information on VCS agents and agent configuration, refer to the VCS documentation.

- See "MonitorVMs agent functions" on page 98.
- See "MonitorVMs agent attribute definitions" on page 99.
- See "MonitorVMs agent resource type definition" on page 99.

MonitorVMs agent functions

The MonitorVMs agent can monitor, start, and stop the application VMs and their associated storage by monitoring these resources and bringing them online or offline.

Table 7-1 MonitorVMs agent functions

Function	Description
Monitor	If all VM resources in the Microsoft failover cluster are not in a FAILED state, report the resources as ONLINE. If the Microsoft failover cluster group containing the VM resources is in a failed state, report the resources as FAULTED.
Online	Bring the CSVs or physical disk resources online. If VMs are configured on SFW storage, bring SFW Volume Manager Disk Group (VMDg) resources online. If application VMs are not configured in the Microsoft cluster, then perform the steps necessary to import the VM configuration and create VM resources in the Microsoft cluster. Import the VM configuration using the documented API. Create the required resources in the Microsoft cluster on the remote DR (secondary) site, using the add-ClusterVirtualMachineRole cmdlet. Bring online all VMs being monitored.
Offline	Bring offline all VMs and VM configurations that depend on the same CSV volume or physical disk resources. Bring offline the CSV volume or physical disk resources

MonitorVMs agent state definitions

The following are the MonitorVMs agent state definitions:

ONLINE	All virtual machines (VMs) being monitored are running
OFFLINE	All VMs being monitored are not running
UNKNOWN	Some of the VMs are not running or in a failed state

MonitorVMs agent attribute definitions

The following table describes the MonitorVMs agent attribute definitions.

Table 7-2 MonitorVMs agent required attributes

Required attributes	Type and dimension	Definition
FOCClusterName	string-scalar	The name of the Microsoft failover cluster
ClusterNodes	string-vector	The name of the physical nodes in the Microsoft cluster
VMNames	string-association	The names of the application virtual machines
VMNetworkSettingsFile	string-scalar	The full path including file name of the network settings file

MonitorVMs agent resource type definition

The following is the MonitorVMs agent resource type definition:

```
type MonitorVMs (
  static boolean IntentionalOffline = 1
  static i18nstr ArgList[] = { ClusterName, ClusterNodes, VMNames, VMNetworkSettingsFile }
  i18nstr FOCClusterName
  i18nstr ClusterNodes[]
  i18nstr VMNames{}
  i18nstr VMNetworkSettingsFile
```