Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Enterprise Vault

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

6.0

October 2011

Symantec

Veritas Storage Foundation and HA Solutions HA and Disaster Recovery Solutions Guide for Enterprise Vault

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

Product version: 6.0

Document version: 6.0.0

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 automatic software upgrades protection
- 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 3 Requirements and Planning

Chapter 4 Requirements and planning for your HA and DR configurations

Section 4 Deployment

Chapter 5 Installing and configuring SFW HA

Section 1

Introduction and Concepts

This section contains the following chapters:

Chapter 1

Introducing Veritas Storage Foundation and High Availability Solutions for Enterprise Vault

This chapter contains the following topics:

About clustering solutions with SFW HA

Veritas Storage Foundation HA for Windows (SFW HA) provides the following clustering solutions for high availability and disaster recovery with Enterprise Vault:

- High availability failover cluster in an active/passive configuration on the same site
- Wide area disaster recovery, with a separate cluster on a secondary site, with replication support using Veritas Volume Replicator or hardware replication

About high availability

The term high availability refers to a state where data and applications are highly available because software or hardware is in place to maintain the continued functioning in the event of computer failure. High availability can refer to any software or hardware that provides fault tolerance, but generally the term has become associated with clustering.

A cluster is a group of independent computers working together to ensure that mission-critical applications and resources are as highly available as possible. The group is managed as a single system, shares a common namespace, and is specifically designed to tolerate component failures and to support the addition or removal of components in a way that is transparent to users.

Local clustering provides high availability through database and application failover. This solution provides local recovery in the event of application, operating system, or hardware failure, and minimizes planned and unplanned application downtime.

The high availability solution includes procedures for installing and configuring clustered environments using Veritas Storage Foundation HA for Windows (SFW HA). SFW HA includes Veritas Storage Foundation for Windows and Veritas Cluster Server.

Setting up the clustered environment is also the first step in creating a wide-area disaster recovery solution using a secondary site.

How a high availability solution works

Keeping data and applications functioning 24 hours a day and seven days a week is the desired norm for critical applications today. Clustered systems have several advantages over standalone servers, including fault tolerance, high availability, scalability, simplified management, and support for rolling upgrades.

Using Veritas Storage Foundation HA for Windows as a local high availability solution paves the way for a wide-area disaster recovery solution in the future.

A high availability solution is built on top of a backup strategy and provides the following benefits:

- Reduces planned and unplanned downtime.
- Serves as a local and wide-area failover (rather than load-balancing) solution. Enables failover between sites or between clusters.
- Manages applications and provides an orderly way to bring processes online and take them offline.
- Consolidates hardware in larger clusters. The HA environment accommodates flexible fail over policies, active-active configurations, and shared standby servers.

About replication

The term replication refers to the use of a tool or service to automate the process of maintaining a consistent copy of data from a designated source (primary site) on one or more remote locations (secondary sites).

In the event that the primary site data center is destroyed, the application data is readily available at the remote site, and the application can be restarted at the remote site.

SFW HA provides Veritas Volume Replicator (VVR) for use in replication. VVR can be used for replication in either a replicated data cluster (RDC) or a wide area disaster recovery solution.

For more information on VVR refer to the *Veritas Volume Replicator, Administrator's Guide*.

About disaster recovery

Wide area disaster recovery (DR) provides the ultimate protection for data and applications in the event of a disaster. If a disaster affects a local or metropolitan area, data and critical services are failed over to a site hundreds or thousands of miles away. Veritas Storage Foundation HA for Windows (SFW HA) provides the capability for implementing disaster recovery.

A disaster recovery (DR) solution is a series of procedures which you can use to safely and efficiently restore application user data and services in the event of a catastrophic failure. A typical DR solution requires that you have a source or *primary site* and a destination or *secondary site*. The user application data on the primary site is replicated to the secondary site. The cluster on the primary site

provides data and services during normal operations. In the event of a disaster at the primary site and failure of the cluster, the secondary site provides the data and services.

What you can do with a disaster recovery solution

A DR solution is vital for businesses that rely on the availability of data.

A well-designed DR solution prepares a business for unexpected disasters and provides the following benefits in a DR situation:

- Minimizes economic loss due to the unavailability or loss of data.
- Provides a plan for the safe and orderly recovery of data in the event of a disaster.
- Ensures safe and efficient recovery of data and services.
- Minimizes any decision making during DR.
- Reduces the reliance on key individuals.

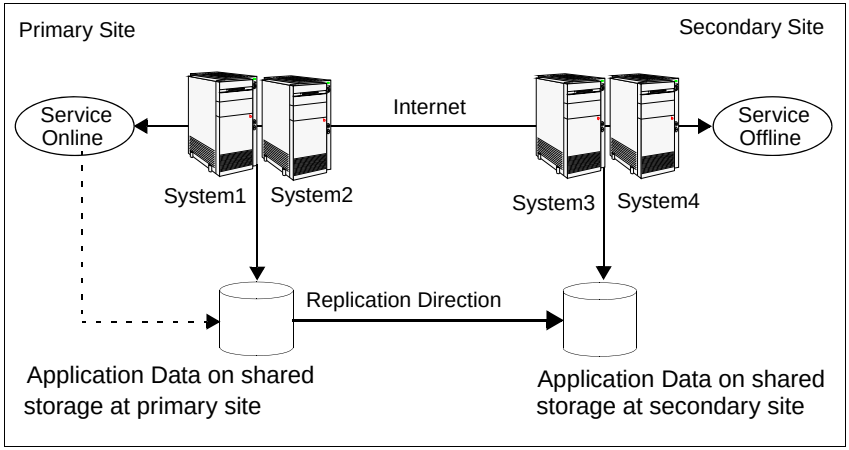
Strategically planning a DR solution provides businesses with affordable ways to meet their service level agreements, comply with government regulations, and minimize their business risks.

Typical disaster recovery configuration

A disaster recovery (DR) configuration enables you to restore application data and services in the event of a catastrophic failure. A typical DR solution requires primary and secondary sites, and clusters within those sites. The cluster at the primary site provides data and services during normal operation, and the cluster at the secondary site provides data and services if the primary site fails.

Figure 1-1 illustrates a typical DR configuration.

Figure 1-1 Typical DR configuration in a VCS cluster



The illustration displays an environment with a DR solution that is prepared for a disaster. In this case, the primary site consists of two nodes, System1 and System2. Similarly the secondary setup consists of two nodes, System3 and System4. Each site has a clustered setup with the nodes set up appropriately for failover within the site.

Data is replicated from the primary site to the secondary site. Replication between the storage is set up using a replication software. If the application on System1 fails, the application comes online on node System2 and begins servicing requests. From the user's perspective there might be a small delay as the backup node comes online, but the interruption in effective service is minimal.

When a failure occurs, such as an earthquake that destroys the data center in which the primary site resides, the DR solution is activated. System3 at the secondary site takes over, and the data that was replicated to the secondary site is used to restore the application services to clients.

Where to get more information

Table 1-2 shows the additional Veritas Storage Foundation and High Availability Solutions guides for Enterprise Vault.

Table 1-1 Additional SFW HA solutions guides for Enterprise Vault

Title	Description
Veritas Storage Foundation and High Availability Solutions Quick Recovery Solutions Guide for Enterprise Vault	Quick Recovery solutions for Enterprise Vault using either Veritas Storage Foundation for Windows or Veritas Storage Foundation HA for Windows.

Symantec recommends as a best practice to configure SQL Server for high availability before configuring Enterprise Vault. Configuring SQL Server for high availability is covered in the SQL Server solutions guides.

Table 1-2 shows the available Veritas Storage Foundation and High Availability Solutions guides for SQL Server.

Table 1-2 SFW HA solutions guides for SQL Server

Title	Description
Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2005	Solutions for SQL Server 2005 and Veritas Cluster Server clustering with Veritas Storage Foundation HA for Windows ■ High availability (HA) ■ Campus clusters ■ Replicated data clusters ■ Disaster recovery (DR) with Veritas Volume Replicator or hardware array replication
Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008 and 2008 R2	Solutions for SQL Server 2008, SQL Server 2008 R2, and Veritas Cluster Server clustering with Veritas Storage Foundation HA for Windows ■ High availability (HA) ■ Campus clusters ■ Replicated data clusters ■ Disaster recovery (DR) with Veritas Volume Replicator or hardware array replication

Table 1-2 SFW HA solutions guides for SQL Server (Continued)

Title	Description
Veritas Storage Foundation and High Availability Solutions Microsoft Clustering Solutions Guide for Microsoft SQL 2005, 2008 and 2008 R2	Solutions for SQL Server and Microsoft clustering with Veritas Storage Foundation for Windows: ■ High availability (HA) ■ Campus clusters ■ Disaster recovery (DR) with Veritas Volume Replicator
Veritas Storage Foundation and High Availability Solutions Quick Recovery Solutions Guide for Microsoft SQL 2005, 2008, and 2008 R2	Quick Recovery solutions for SQL Server 2005, 2008, and 2008 R2 using either Veritas Storage Foundation for Windows or Veritas Storage Foundation HA for Windows.

Section 2

Configuration Workflows

This section contains the following chapters:

Chapter 2

Configuration workflows for Enterprise Vault

This chapter contains the following topics:

About using the workflow tables

Configuring a high availability or a disaster recovery environment involves a series of tasks such as evaluating the requirements, configuring the storage, installing and configuring VCS, installing and configuring the application, and so on. A configuration workflow table provides high level description of all the required tasks, with links to the topics that describe these tasks in detail.

Separate workflow tables are provided for HA and DR configurations. Use the appropriate workflow table as a guideline to perform the installation and configuration.

Symantec recommends using the Solutions Configuration Center as a guide for installing and configuring SFW HA for Enterprise Vault.

See "About the Solutions Configuration Center" on page 35.

The workflow tables are organized to follow the workflows in the Solutions Configuration Center.

For example, in using the Solutions Configuration Center to set up a site for disaster recovery, you first follow the steps under High Availability (HA) Configuration and then continue with the steps under Disaster Recovery Configuration. Likewise, in this guide, you first refer to the High Availability

workflow to set up high availability. You then continue with the disaster recovery workflow.

High availability (HA) configuration (New Server)

Table 2-1 outlines the high-level objectives and the tasks to complete each objective for an Active-Passive configuration.

Note: Symantec recommends as a best practice to configure SQL Server for high availability before configuring Enterprise Vault for high availability. Configuring SQL Server for high availability is covered in the SQL Server solutions guides. See "Where to get more information" on page 18.

Table 2-1 Enterprise Vault Server: Active-Passive configuration tasks

Action	Description
Verify hardware and software requirements	See "Reviewing the requirements" on page 46.
Review the HA configuration	■ Understand active-passive configuration See "Reviewing the HA configuration" on page 52.
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment ■ Verify the DNS entries for the systems on which Enterprise Vault Server will be installed See "Configuring the storage hardware and network" on page 62.
Install SFW HA	■ Install Veritas Storage Foundation HA for Windows ■ If you plan on configuring fast failover, select the VCS Fast Failover option. See "Installing Veritas Storage Foundation HA for Windows" on page 64. See "Considerations for a fast failover configuration" on page 75.

Table 2-1 Enterprise Vault Server: Active-Passive configuration tasks

Action	Description
Configure disk groups and volumes for Enterprise Vault Server	■ Create a dynamic cluster disk group using the Veritas Enterprise Administrator (VEA) ■ Create dynamic volumes for the MSMQ data, registry replication data, and EV services data See "Configuring cluster disk groups and volumes for Enterprise Vault" on page 74.
Configure VCS cluster	If the cluster has not already been configured for SQL Server: ■ Verify static IP addresses and name resolution configured for each node ■ Run the VCS Cluster Configuration Wizard (VCW) to configure cluster components and set up secure communication for the cluster See "Configuring the cluster" on page 85.
Install Enterprise Vault on the cluster nodes	■ Ensure that the appropriate amount of local storage space is available on the node. This is required for storing temporary files during Enterprise Vault installation. Refer to the Enterprise Vault documentation for installation instructions
Create an Enterprise Vault service group	■ Ensure that you have met the prerequisites ■ Ensure that the disk group and volumes for the various Enterprise Vault components are mounted on the first node ■ Create a EV service group using the Enterprise Vault Cluster Setup Wizard ■ Bring the EV service group online on the first node See "Configuring the Enterprise Vault service group" on page 106
Configure fast failover for disk groups (optional)	■ Ensure that you have installed the Fast Failover option and met the prerequisites for storage ■ Use the Java Console to enable the FastFailover attribute for VMDg resources See "Enabling fast failover for disk groups (optional)" on page 110.

Table 2-1 Enterprise Vault Server: Active-Passive configuration tasks

Action	Description
Configure Enterprise Vault for the cluster environment on the first node	■ Launch the Enterprise Vault Configuration Wizard on the first node ■ Choose the option to create a new Enterprise Vault server with cluster support ■ Complete running the wizard on the first node See "Configuring Enterprise Vault Server in a cluster environment" on page 112. Refer to the Enterprise Vault documentation for more information.
Configure Enterprise Vault for the cluster environment on any additional nodes	■ Bring the EV service group online on the first node ■ Launch the Enterprise Vault Configuration Wizard on the second node ■ Choose the option to add the node as a failover node for an existing clustered server ■ Complete running the wizard on the second node ■ Repeat these steps for any additional nodes in the EV cluster See "Configuring Enterprise Vault Server in a cluster environment" on page 112. Refer to the Enterprise Vault documentation for more information.
Perform additional configuration steps for Enterprise Vault	See "Setting up Enterprise Vault" on page 115. Refer to the Enterprise Vault documentation for more information.
(Optional) Configure the appropriate service group dependencies	Configure the appropriate service group dependencies See "Verifying the Enterprise Vault cluster configuration" on page 113.
Verify the HA configuration	Test failover between nodes See "Verifying the Enterprise Vault cluster configuration" on page 113

Disaster recovery configuration

For configuring disaster recovery, you first begin by configuring the primary site for high availability. After setting up an SFW HA high availability environment for Enterprise Vault (EV) on a primary site, you can create a secondary or "failover" site for disaster recovery.

Note: Symantec recommends as a best practice to configure SQL Server for disaster recovery before configuring Enterprise Vault for disaster recovery. Configuring SQL Server for disaster recovery is covered in the SQL Server solutions guides. See "Where to get more information" on page 18.

The Disaster Recovery (DR) wizard helps you to configure the storage, VVR replication, and the global cluster on the secondary site.

The DR wizard is available from the Solutions Configuration Center. Symantec recommends using the Solutions Configuration Center as a guide for installing and configuring disaster recovery.

See "About the Solutions Configuration Center" on page 35.

To follow the workflow in the Solutions Configuration Center, the disaster recovery workflow has been split into two tables, one covering the steps for configuring high availability at the primary site, and the other covering the steps for completing the disaster recovery configuration at the secondary site.

DR configuration tasks: Primary site

Table 2-2 outlines the high-level objectives and the tasks to complete each objective for a DR configuration at the primary site.

Table 2-2 Configuring the primary site for disaster recovery

Action	Description
Verify hardware and software prerequisites	See "Reviewing the requirements" on page 46. **Note:** If the DR site is on a different network segment, ensure that you allocate two IP addresses for the virtual server, one for the primary site and one for the DR site.
Understand the configuration	Understand the DR configuration See "Reviewing the disaster recovery configuration" on page 54.

Table 2-2 Configuring the primary site for disaster recovery (Continued)

Action	Description
Configure the storage hardware and network	For all nodes in the cluster: ■ Set up the storage hardware for a cluster environment ■ Verify the DNS entries for the systems on which EV will be installed See "Configuring the storage hardware and network" on page 62.
Install SFW HA	■ Install Veritas Storage Foundation for Windows HA on all nodes that will become part of the cluster ■ Select the option to install the Global Cluster Option (GCO) ■ Select the option to install VVR See "Installing Veritas Storage Foundation HA for Windows" on page 64.
Configure the cluster	If the cluster has not already been configured for SQL Server: ■ Verify static IP addresses and name resolution configured for each node ■ Configure cluster components using the Veritas Cluster Server Configuration Wizard (VCW) ■ Set up secure communication for the cluster See "Configuring the cluster" on page 85.
Configure cluster disk groups and volumes for Enterprise Vault	■ Create a dynamic cluster disk group using the Veritas Enterprise Administrator (VEA) ■ Create dynamic volumes for the MSMQ data, registry replication data, and EV services data See "Configuring cluster disk groups and volumes for Enterprise Vault" on page 74.
Install Enterprise Vault on the cluster nodes	■ Ensure that the appropriate amount of local storage space is available on the first cluster node. This is required for storing temporary files during Enterprise Vault installation. Refer to the Enterprise Vault documentation for installation instructions

Table 2-2 Configuring the primary site for disaster recovery (Continued)

Action	Description
Create an Enterprise Vault service group	■ Ensure that you have met the prerequisites ■ Ensure that the disk group and volumes for the various Enterprise Vault components are mounted on the first node ■ Create a EV service group using the Enterprise Vault Cluster Setup Wizard ■ Bring the EV service group online on the first node See "Configuring the Enterprise Vault service group" on page 106.
Configure Enterprise Vault for the cluster environment on the first node	■ Launch the Enterprise Vault Configuration Wizard on the first node ■ Choose the option to create a new Enterprise Vault server with cluster support ■ Complete running the wizard on the first node See "Configuring Enterprise Vault Server in a cluster environment" on page 112. Refer to the Enterprise Vault documentation for more information.
Configure Enterprise Vault for the cluster environment on any additional nodes	■ Bring the EV service group online on the first node ■ Launch the Enterprise Vault Configuration Wizard on the second node ■ Choose the option to add the node as a failover node for an existing clustered server ■ Complete running the wizard on the second node ■ Repeat these steps for any additional nodes in the EV cluster See "Configuring Enterprise Vault Server in a cluster environment" on page 112. Refer to the Enterprise Vault documentation for more information.
Perform additional configuration steps for Enterprise Vault	See "Setting up Enterprise Vault" on page 115. Refer to the Enterprise Vault documentation for more information.
(Optional) Configure the appropriate service group dependencies	Configure the appropriate service group dependencies See "Verifying the Enterprise Vault cluster configuration" on page 113.

Table 2-2 Configuring the primary site for disaster recovery (Continued)

Action	Description
Verify the primary site configuration	Test failover between nodes on the primary site See "Verifying the Enterprise Vault cluster configuration" on page 113.

DR configuration tasks: Secondary site

Table 2-3 outlines the high-level objectives and the tasks to complete each objective for a DR configuration at the secondary site.

Table 2-3 Configuring the secondary site for disaster recovery

Action	Description
Install SFW HA and configure the cluster on the secondary site	**Caution:** Ensure that the name you assign to the secondary site cluster is different from the name assigned to the primary site cluster. See "Guidelines for installing SFW HA and configuring the cluster on the secondary site" on page 122.
Verify that Enterprise Vault has been configured for high availability at the primary site	Verify that Enterprise Vault has been configured for high availability at the primary site and that the service group is online See "Verifying your primary site configuration" on page 121.
Set up security for VVR	Ensure that you have completed setting up VVR security before running the DR wizard See "Setting up security for VVR" on page 122.
(Secure cluster only) Assign user privileges	For a secure cluster only, assign user privileges See "Assigning user privileges (secure clusters only)" on page 126.
Start running the DR wizard	■ Review prerequisites for the DR wizard ■ Start the DR wizard and make the initial selections required for each task: selecting a primary site system, the service group, the secondary site system, and the replication method See "Configuring disaster recovery with the DR wizard" on page 127.

Table 2-3 Configuring the secondary site for disaster recovery (Continued)

Action	Description
Clone the storage configuration	Clone the storage configuration on the secondary site using the DR wizard See "Cloning the storage on the secondary site using the DR wizard" on page 130.
Install Enterprise Vault on the cluster nodes	■ Ensure that the appropriate amount of local storage space is available on the first cluster node. This is required for storing temporary files during Enterprise Vault installation. Refer to the Enterprise Vault documentation for installation instructions
Create an Enterprise Vault service group	■ Ensure that you have met the prerequisites ■ Ensure that the disk group and volumes for the various Enterprise Vault components are mounted on the first node ■ Create a EV service group for the secondary site using the same service group name, virtual server name, and configuration as on the primary site See "Installing and configuring Enterprise Vault on the secondary site" on page 133.
Configure Enterprise Vault for the cluster environment on the first node	■ Launch the Enterprise Vault Configuration Wizard on the first node ■ Choose the option to create a new Enterprise Vault server with cluster support ■ Complete running the wizard on the first node See "Installing and configuring Enterprise Vault on the secondary site" on page 133. Refer to the Enterprise Vault documentation for more information.

Table 2-3 Configuring the secondary site for disaster recovery (Continued)

Action	Description
Configure Enterprise Vault for the cluster environment on any additional nodes	■ Bring the EV service group online on the first node ■ Launch the Enterprise Vault Configuration Wizard on the second node ■ Choose the option to add the node as a failover node for an existing clustered server ■ Complete running the wizard on the second node ■ Repeat these steps for any additional nodes in the EV cluster See "Installing and configuring Enterprise Vault on the secondary site" on page 133. Refer to the Enterprise Vault documentation for more information.
Perform additional configuration steps for Enterprise Vault	See "Setting up Enterprise Vault" on page 115. Refer to the Enterprise Vault documentation for more information.
Configure replication and global clustering	Use the DR wizard to configure VVR replication and global clustering See "Configuring VVR replication and global clustering" on page 136.
(Optional) Configure the appropriate service group dependencies	Configure the appropriate service group dependencies See "Setting service group dependencies for disaster recovery" on page 143.
Verify the disaster recover configuration	Verify that the secondary site has been fully configured for disaster recovery See "Verifying the disaster recovery configuration" on page 144.
(Optional) Add secure communication	Add secure communication between local clusters within the global cluster (optional task) See "Establishing secure communication within the global cluster (optional)" on page 145.
(Optional) Add additional DR sites	Optionally, add additional DR sites to a VVR environment See "Adding multiple DR sites (optional)" on page 147.

Table 2-3 Configuring the secondary site for disaster recovery (Continued)

Action	Description
Handling service group dependencies after failover	If your environment includes dependent service groups, review the considerations for bringing the service groups online after failover to the secondary site See "Recovery procedures for service group dependencies" on page 148.

Chapter 3

Using the Solutions Configuration Center

This chapter covers the following topics:

About the Solutions Configuration Center

The Storage Foundation and High Availability Solutions Configuration Center guides you through setting up your Veritas Storage Foundation for Windows (SFW) or SFW High Availability (HA) environment. The Configuration Center provides solutions for the following applications:

- Microsoft Exchange Server 2007 and 2010
- Microsoft SQL Server 2005, 2008, and 2008 R2
- Enterprise Vault Server (high availability and disaster recovery solutions)
- Microsoft SharePoint Server 2010 (high availability, disaster recovery, and Quick Recovery solutions)
- Additional applications

Depending on the application, the following solutions may be available:

- High availability at a single site for a new installation

- High availability at a single site for an existing server
- Campus cluster disaster recovery, including the following:
  - Campus cluster using Veritas Cluster Server (SFW HA)
  - Campus cluster using Microsoft clustering
- Wide area disaster recovery involving multiple sites
- Quick Recovery for on-host recovery from logical errors in application data
- Fire drill to test the fault readiness of a disaster recovery environment

Starting the Solutions Configuration Center

You can start the Solutions Configuration Center in the following ways:

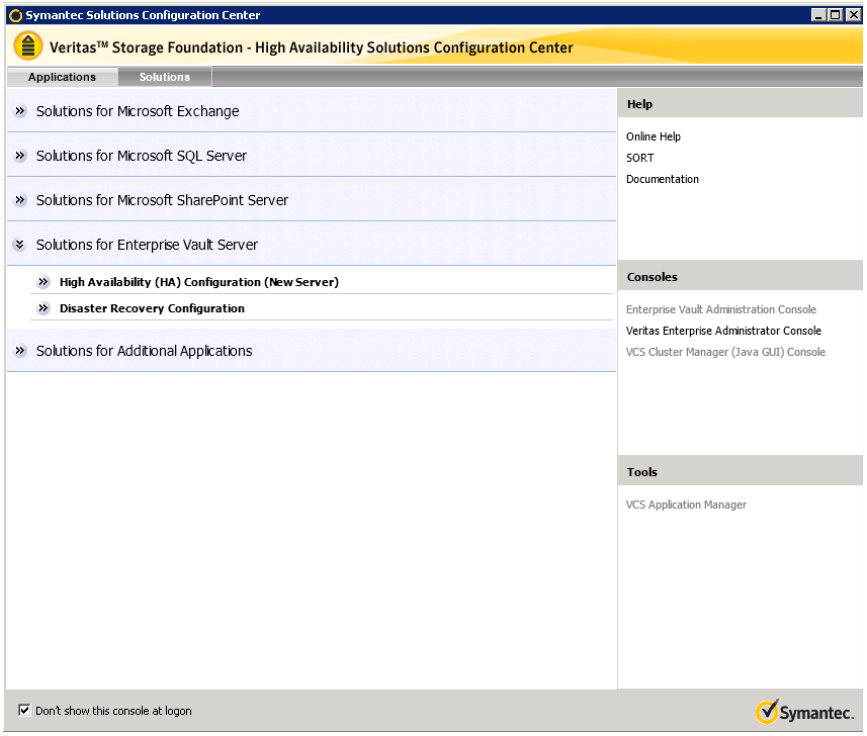
- Click **Start > All Programs > Symantec > Veritas Storage Foundation > Solutions Configuration Center**.
- Click **Start > All Programs > Symantec > Veritas Cluster Server > Solutions Configuration Center**.
- Click **Start > Run** and type **scc**.

Available options from the Configuration Center

On the Applications tab, the Solutions Configuration Center is context-sensitive to the application. For example, the solutions displayed when you click the application name are those available for that application. The steps that are shown when you click on a solution are customized for that application.

Figure 3-1 shows the solutions available when you click Solutions for Enterprise Vault Server.

Figure 3-1 Solutions Configuration Center for Enterprise Vault Server



How to launch the Configuration Center wizards

The Solutions Configuration Center provides two ways to access wizards:

Applications tab	Lists solutions by application Provides step-by-step configuration instructions that include buttons to launch the appropriate wizard for each step
Solutions tab	For advanced users Lists wizards by solution, without additional instructions, so that you can go directly to a particular wizard. The following categories of solution are listed: High Availability Configuration Wizards Disaster Recovery Configuration Wizards Quick Recovery Configuration Wizards Fire Drill Configuration Wizards

Using the Configuration Center from remote systems

The Solutions Configuration Center and some wizards can be run from a remote system. Wizards that you can run remotely include the following:

Disaster Recovery Configuration Wizard	Configures wide area disaster recovery, including cloning storage, cloning service groups, and configuring the global cluster Also can configure Veritas Volume Replicator (VVR) replication or configure the VCS resource for EMC SRDF and Hitachi TrueCopy array-based hardware replication Requires first configuring high availability on the primary site To configure IPv6 settings, the wizard must be launched from a system on which the IPv6 stack is installed
Fire Drill Wizard	Sets up a fire drill to test disaster recovery Requires configuring disaster recovery first To configure IPv6 settings, the wizard must be launched from a system on which the IPv6 stack is installed

Quick Recovery Configuration Wizard	Schedules preparation of snapshot mirrors and schedules the Quick Recovery snapshots
VCS Configuration Wizard	Sets up the VCS cluster
VVR Security Service Configuration Wizard	Configures the VVR security service

Wizards related to storage configuration and application installation must be run locally on the system where the process is occurring. Wizards that you must run locally include the following:

New Dynamic Disk Group Wizard	Launched from the Veritas Enterprise Administrator console
New Volume Wizard	Launched from the Veritas Enterprise Administrator console
Enterprise Vault Cluster Setup Wizard	Configures the service group for Enterprise Vault Server high availability
Enterprise Vault Cluster Wizard	Configures Enterprise Vault Server in a cluster environment
MSMQ Configuration Wizard	Configures a Microsoft Message Queuing (MSMQ) service group
SFW Configuration Utility for Hyper-V Live Migration Support	Configure SFW for Microsoft Hyper-V Live Migration support on the selected systems.

Solutions wizard logs

The Solutions Configuration Center provides access to many wizards. However, three wizards are built in to the Solutions Configuration Center:

- Disaster Recovery Wizard
- Fire Drill Wizard
- Quick Recovery Configuration Wizard

These three Solutions wizards are launched only from the Solutions Configuration Center, whereas other wizards can be launched from product consoles or the Start menu.

Logs created by these three Solutions wizards are located in the following path:

`C:\ProgramData\Veritas\winsolutions\log`

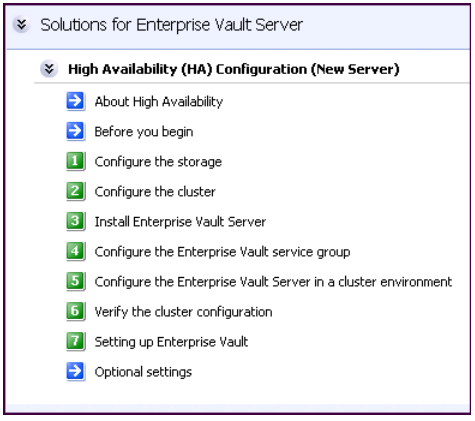
Following the workflow in the Configuration Center

During the multi-step High Availability Configuration workflow, you may find it helpful to run an SFW HA client on another system and leave the Solutions Configuration Center open on that system. In this way, you can see what step comes next, drill down to the information about that step, and access the online help if needed. You can also print the online help topics and the documentation in PDF format.

When setting up a site for disaster recovery, you first follow the steps under High Availability (HA) Configuration and then continue with the steps under Disaster Recovery Configuration.

Figure 3-2 shows the high-level overview of the workflow steps for configuring high availability for Enterprise Vault Server from the Solutions Configuration Center.

Figure 3-2 Workflow for configuring high availability for Enterprise Vault Server



Section 3

Requirements and Planning

This section contains the following chapter:

- Requirements and planning for your HA and DR configurations

Chapter 4

Requirements and planning for your HA and DR configurations

This chapter contains the following topics:

Reviewing the requirements

Verify that the requirements for your configuration are met before starting the Veritas Storage Foundation HA for Windows installation.

Disk space requirements

The following table estimates disk space requirements for SFW HA.

Table 4-1 Disk space requirements

Installation options	Required disk space
SFW HA + all options	1589 MB
Client components	916 MB

Requirements for Veritas Storage Foundation High Availability for Windows (SFW HA)

Before installing Veritas Storage Foundation High Availability for Windows (SFW HA), ensure that you review the following:

- Review the general installation requirements for SFW HA in the *Veritas Storage Foundation and High Availability Solutions for Windows Installation and Upgrade Guide*.
- Review the SFW HA 6.0 Hardware Compatibility List to confirm supported hardware:
  http://www.symantec.com/docs/TECH152806
- Review the SFW HA 6.0 Software Compatibility List to confirm supported software:
  http://www.symantec.com/docs/TECH153742
- Review the Enterprise Vault Server versions supported with Veritas Storage Foundation High Availability for Windows (SFW HA).
- When installing SFW HA for a Disaster Recovery configuration, ensure that you select the VCS Global Clustering Option and if required for your replication solution, select the SFW Veritas Volume Replicator option.
- When installing SFW HA for a Replicated Data Cluster configuration, ensure that you select the VCS option to install Veritas Volume Replicator.

Supported Enterprise Vault versions

The following versions of Enterprise Vault are tested and supported with this release of SFW HA:

- Enterprise Vault 8.0 SP1, SP2, and SP3
- Enterprise Vault 9.0

System requirements for SFW HA

Systems must meet the following requirements for SFW HA:

- Memory must be a minimum 4 GB of RAM per server for SFW HA.
- Shared disks to support applications that migrate between nodes in the cluster. Campus clusters require more than one array for mirroring. Disaster recovery configurations require one array for each site. Replicated data clusters with no shared storage are also supported.
  If your storage devices are SCSI-3 compliant, and you wish to use SCSI-3 Persistent Group Reservations (PGR), you must enable SCSI-3 support using the Veritas Enterprise Administrator (VEA). See the *Veritas Storage Foundation Administrator's Guide* for more information.
- SCSI, Fibre Channel, iSCSI host bus adapters (HBAs), or iSCSI Initiator supported NICs to access shared storage.
- 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.
  See "Best practices for SFW HA" on page 51.
- NIC teaming is not supported for the VCS private network.

Network requirements for SFW HA

SFW HA has the following network requirements:

- Do not install SFW HA on servers that are assigned the role of a Domain Controller. Configuring a cluster on a domain controller is not supported.
- Ensure that your firewall settings allow access to ports used by SFW HA wizards and services. For a detailed list of services and ports used by SFW HA, refer to the *Veritas Storage Foundation and High Availability Solutions for Windows Installation and Upgrade Guide*.
- Static IP addresses are required for certain purposes when configuring high availability or disaster recovery solutions. For IPv4 networks, ensure that you have the addresses available to enter. For IPv6 networks, ensure that the network advertises the prefix so that addresses are autogenerated. Static IP addresses are required for the following purposes:
  - One static IP address per site for each Enterprise Vault virtual server.
  - A minimum of one static IP address for each physical node in the cluster.

- One static IP address per cluster used when configuring Notification or the Global Cluster Option. The same IP address may be used for all options.
- For VVR replication in a disaster recovery configuration, a minimum of one static IP address per site for each application instance running in the cluster.
- For VVR replication in a Replicated Data Cluster configuration, a minimum of one static IP address per zone for each application instance running in the cluster.

- Configure name resolution for each node.
- Verify the availability of DNS Services. AD-integrated DNS or BIND 8.2 or higher are supported.
  Make sure a reverse lookup zone exists in the DNS. Refer to the application documentation for instructions on creating a reverse lookup zone.
- DNS scavenging affects virtual servers configured in SFWHA because the Lanman agent uses Dynamic DNS (DDNS) to map virtual names with IP addresses. If you use scavenging, then you must set the DNSRefreshInterval attribute for the Lanman agent. This enables the Lanman agent to refresh the resource records on the DNS servers.
  See the *Veritas Cluster Server Bundled Agents Reference Guide*.
- In an IPv6 environment, the Lanman agent relies on the DNS records to validate the virtual server name on the network. If the virtual servers configured in the cluster use IPv6 addresses, you must specify the DNS server IP, either in the network adapter settings or in the Lanman agent's AdditionalDNSServers attribute.
- If Network Basic Input/Output System (NetBIOS) is disabled over the TCP/IP, then you must set the Lanman agent's DNSUpdateRequired attribute to 1 (True).

IPv6 support

For IPv6 networks, the following is supported:

Types of addresses	The following types of IPv6 addresses are supported: ■ Unicast addresses Only Global Unicast and Unique Local Unicast addresses are supported. ■ Automatic configuration Only Stateless IPv6 address configuration is supported. In stateless mode, the IP address is configured automatically based on router advertisements. The prefix must be advertised.
LLT over UDP	LLT over UDP is supported on both IPv4 and IPv6. You can use the Cluster Configuration Wizard (VCW) to configure LLT over UDP over IPv6.
VCS agents, wizards, and other components	VCS agents that require an IP address attribute and wizards that configure or discover IP addresses now support IPv6 addresses (of the type described above). The VCS High Availability Engine (HAD) and the Global Cluster resource (WAC) also support IPv6 addresses.

Note: Support is limited to mixed mode (IPv4 and IPv6) network configurations only; a pure IPv6 environment is currently not supported.

Permission requirements for SFW HA

The following permissions are required:

- You must be a domain user.
- You must be a member of the local Administrators group on all nodes where you are installing.
- You must have write permissions for the Active Directory objects corresponding to all the nodes.
- If you plan to create a new user account for the VCS Helper service, you must have Domain Administrator privileges or belong to the Account Operators group. If you plan to use an existing user account context for the VCS Helper service, you must know the password for the user account.

Additional requirements for SFW HA

Please review the following additional requirements:

- Installation media for all products and third-party applications.
- Licenses for all products and third-party applications.
- For a Replicated Data Cluster, install only in a single domain.

Best practices for SFW HA

Symantec recommends that you perform the following tasks:

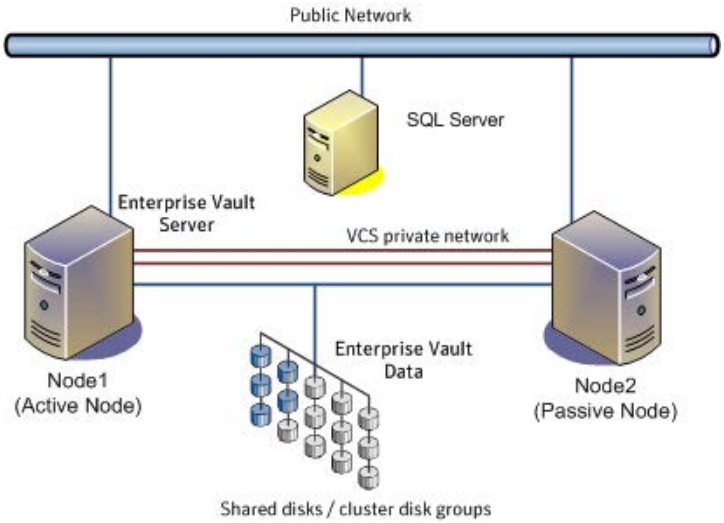
- Verify that you have three network adapters (two NICs exclusively for the private network and one for the public network).
  When using only two NICs, lower the priority of one NIC and use the low-priority NIC for public and private communication.
- Route each private NIC through a separate hub or switch to avoid single points of failure.
- NIC teaming is not supported for the VCS private network.
- Verify that your DNS server is configured for secure dynamic updates. For the Forward and Reverse Lookup Zones, set the Dynamic updates option to "Secure only". (DNS > Zone Properties > General tab)
- Although you can use a single node cluster as the primary and secondary zones, you must create the disk groups as clustered disk groups. If you cannot create a clustered disk group due to the unavailability of disks on a shared bus, use the vxclus UseSystemBus ON command. This is applicable for a Replicated Data Cluster configuration.

Reviewing the HA configuration

In a typical example of a high availability cluster, you create a virtual Enterprise Vault server in an Active-Passive configuration. The active node of the cluster hosts the virtual server. The second node is a dedicated redundant server able to take over and host the virtual server in the event of a failure on the active node.

Figure 4-1 illustrates a typical Active-Passive configuration.

Figure 4-1 Active-Passive configuration



Enterprise Vault Server is installed on both Node1 and Node2 and configured as a virtual server with a virtual IP address.

Shared volumes are configured on shared storage for the following:

- MSMQ data
- Registry replication data
- Various EV services data (Indexing service, Shopping service, Vault store partitions, PST holding folders, etc.)

Symantec recommends as a best practice to configure SQL Server for high availability before configuring Enterprise Vault. You will specify the SQL virtual server name during EV configuration.

Configuring SQL Server for high availability is covered in the SQL Server solutions guides. See “Where to get more information” on page 18.

Sample Active-Passive configuration

A sample setup is used to illustrate the installation and configuration tasks for an Active-Passive configuration.

Table 4-2 describes the objects created and used during the installation and configuration using sample names.

Table 4-2 Active-Passive configuration objects

Object Name	Description
SYSTEM1 & SYSTEM2	servers
EVDG	cluster disk group
EV_MSMQ_DATA	volume for MSMQ data
EV_MSMQ_LOG	volume for MSMQ log
EV_DATASTORE1	additional volume(s) for storing EV data, as appropriate for your needs
MSMQ_REGREP_VOL	volume that contains the list of registry keys that must be replicated among cluster systems for the EV Server
CLUS1	EV cluster (if the cluster is not already created for SQL Server)
EV-VS	EV virtual server
EV_SG	EV service group

IP addresses for sample Active-Passive configuration

In addition to preparing the names you want to assign the Active-Passive configuration objects, for an IPv4 network, you should obtain all required IP addresses before beginning configuration. For an IPv6 network, IP addresses are generated during configuration.

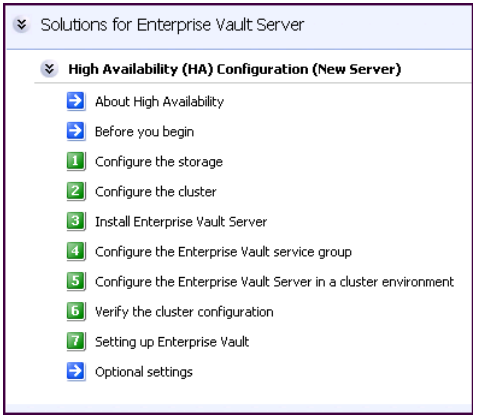
Each EV virtual server requires its own virtual IP address. In the sample configuration there is one EV virtual server. Therefore you would need one virtual server IP address. If you want to use the VCS notification service, you require a cluster IP address. The cluster IP address is also used by the Global Cluster Option for disaster recovery.

Following the HA workflow in the Solutions Configuration Center

The Solutions Configuration Center helps you through the process of installing and configuring a new Veritas Storage Foundation HA environment for Enterprise Vault.

Figure 4-2 shows the workflow under the High Availability (HA) Configuration in the Solutions Configuration Center.

Figure 4-2 Configuration steps in the Solutions Configuration Center



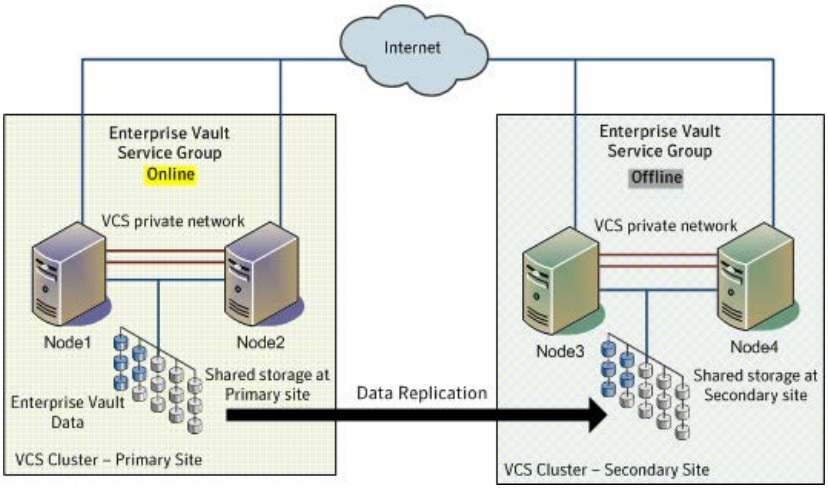
See "Following the workflow in the Configuration Center" on page 41.

Reviewing the disaster recovery configuration

You may be preparing to configure both a primary site and a secondary site for disaster recovery.

Figure 4-3 illustrates a typical Active-Passive disaster recovery configuration.

Figure 4-3 Typical DR configuration



In the example, the primary site consists of two nodes, Node1 and Node2. Similarly the secondary setup consists of two nodes, Node3 and Node4. Each site has a clustered setup with the nodes set up appropriately for failover within the site.

If the Enterprise Vault server on Node1 fails, Enterprise Vault comes online on node Node2 and begins servicing requests. From the user's perspective there might be a small delay as the backup node comes online, but the interruption in effective service is minimal. If there is a disaster at the primary site, Node3 at the secondary site takes over.

The cluster on the primary site has a shared disk group that is used to create the volumes required by VVR for setting up the Replicated Volume Group (RVG). The application data is stored on the volumes that are under the control of the RVG.

The sample setup has four servers, two for the primary site and two for the secondary site. The nodes will form two separate clusters, one at the primary site and one at the secondary site.

Table 4-3 describes the objects created and used during the installation and configuration.

Table 4-3 Sample Disaster Recovery configuration objects

Object Name	Description
Primary site	
SYSTEM1 & SYSTEM2	first and second nodes of the primary site
EVDG	cluster disk group
EV_MSMQ_DATA	volume for MSMQ data
EV_MSMQ_LOG	volume for MSMQ log
EV_DATASTORE1	additional volume(s) for storing EV data, as appropriate for your needs
MSMQ_REGREP_VOL	volume that contains the list of registry keys that must be replicated among cluster systems for the EV Server
CLUS1	EV cluster (if the cluster is not already created for SQL Server)
EV-VS	EV virtual server
EV_SG	EV service group
Secondary site	
SYSTEM3 & SYSTEM4	First and second nodes of the secondary site
	All the other parameters are the same as on the primary site.
DR Components (VVR only)	
EV_RDS	RDS Name
EV_RVG	RVG Name
EV_RVG_SG	Replication service group

IP addresses for disaster recovery configuration

In addition to preparing the names you want to assign configuration objects, for an IPv4 network, you should obtain all required IP addresses before beginning configuration. For an IPv6 network, IP addresses are generated during configuration.

You specify the following addresses during the replication process:

virtual server IP address	For a disaster recovery configuration, the virtual IP address for the virtual server at the primary and disaster recovery site can be the same if both sites can exist on the same network segment. Otherwise, you need to allocate one IP address for the virtual server at the primary site and a different IP address for the virtual server at the disaster recovery site.
Cluster IP address	You need one for the primary site cluster and one for the secondary site cluster.
Replication IP address	You need two IP addresses per application instance, one for the primary site and one for the secondary site.

Supported disaster recovery configurations for service group dependencies

Service group dependencies have special requirements and limitations for disaster recovery configuration and for actions to be taken in a disaster recovery scenario.

Service group dependency configurations are described in detail in the VCS documentation.

See *Veritas Cluster Server Administrator's Guide*.

For disaster recovery only certain dependent service group configurations are supported:

- Online local soft
- Online local firm
- Online local hard

If the service group has an unsupported type of dependency and you select it in the DR wizard, you receive an error notification when you attempt to move to the next wizard page.

In a hardware replication environment, the Disaster Recovery wizard supports one level of dependency (one child). If you need to configure more levels, you will need to add the service group and the dependency link manually on the secondary site after you finish running the DR wizard.

In a VVR environment, the wizard cannot configure DR for a service group that has a child and you will need to configure the secondary site manually. For more information on configuring VVR, see the *Volume Replicator Administrator's*

Guide. For more information on configuring GCO, see the *Veritas Cluster Server Administrator's Guide*.

Section 4

Deployment

This section contains the following chapters:

- Installing and configuring SFW HA
- Installing and configuring Enterprise Vault for failover
- Configuring disaster recovery for Enterprise Vault

Chapter 5

Installing and configuring SFW HA

This chapter contains the following topics:

Configuring the storage hardware and network

To configure the hardware

1. Install the required network adapters, and SCSI controllers or Fibre Channel HBA.
2. Connect the network adapters on each system.
   - To prevent lost heartbeats on the private networks, and to prevent VCS from mistakenly declaring a system down, Symantec recommends disabling the Ethernet autonegotiation options on the private network adapters. Contact the NIC manufacturer for details on this process.
   - Symantec recommends removing TCP/IP from private NICs to lower system overhead.
3. Use independent hubs or switches for each VCS communication network (GAB and LLT). You can use cross-over Ethernet cables for two-node clusters. LLT supports hub-based or switch network paths, or two-system clusters with direct network links.
4. Verify that each system can access the storage devices. Verify that each system recognizes the attached shared disk and that the attached shared disks are visible.

To verify the DNS settings and binding order for Windows Server 2008 systems

1. Open the Control Panel (**Start > Control Panel**).
2. Click **Network and Internet**, and then click **Network and Sharing Center**.
3. In the Network and Sharing Center window, on the left side of the screen under Tasks, double-click **Manage network connections**.
4. Ensure the public network adapter is the first bound adapter:
   - From the Advanced menu in the Network Connections window, click **Advanced Settings**.
   - In the Adapters and Bindings tab, verify the public adapter is the first adapter in the Connections list. If necessary, use the arrow button to move the adapter to the top of the list.
   - Click **OK**.
5. Open the Public status dialog box by doing one of the following in the Network Connections window:
   - Double-click the adapter for the public network.
   - Right-click the adapter for the public network and click **Status**.

- Select the adapter for the public network and click **View status of this connection** in the toolbar.

When enabling DNS name resolution, make sure that you use the public network adapters, and not those configured for the VCS private network.

6 In the Public Status dialog box, on the General tab, click **Properties**.

7 In the Public Properties dialog box, on the **General** tab:

- Select the **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)** check box, depending on which protocol your network is using.
- Click **Properties**.

8 Select the **Use the following DNS server addresses** option.

9 Verify the correct value for the IP address of the DNS server.

10 Click **Advanced**.

11 In the **DNS** tab, make sure the **Register this connection's address in DNS** check box is selected.

12 Make sure the correct domain suffix is entered in the **DNS suffix for this connection** field.

13 Click **OK**.

Installing Veritas Storage Foundation HA for Windows

You can install SFW HA using either the product installer wizard or the command line interface (CLI). Before you begin to install the product, ensure that you have reviewed and performed the required preinstallation and planning tasks.

Note: The Windows MPIO feature must be enabled for Windows Server 2008 before you proceed with SFW HA 6.0 installation.

During the installation you can choose to separately install the server components or the client components. If you choose to install the server components, the following components are installed by default.

Table 5-1 List of options installed by default

Client components	Installs the VCS Java Console on the same node where the server components are installed.
High Availability Hardware Replication Agents	■ Veritas Cluster Server Hardware Replication Agent for EMC MirrorView Enables VCS to manage MirrorView replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDF Enables VCS to manage SRDF replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for EMC SRDFSTAR Enables VCS to manage SRDFSTAR replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for Hitachi TrueCopy Enables VCS to manage TrueCopy replicated devices. ■ Veritas Cluster Server Hardware Replication Agent for MetroMirror Enables VCS to manage MetroMirror replicated devices.

Table 5-1 List of options installed by default

High Availability Application Agents	■ Veritas Cluster Server Application Agent for Exchange 2007 ■ Veritas Cluster Server Database Agent for Exchange 2010 ■ Veritas Cluster Server Application Agent for SharePoint Server 2010
High Availability Database Agents	■ Veritas Cluster Server Database Agent for SQL. Installs the VCS agent for both SQL Server 2005 and SQL Server 2008. ■ Veritas Cluster Server Database Agent for Oracle

Note: The high availability agents that get installed with the product software are also available in the form of an agent pack. The agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing SFW HA installation. Refer to the Symantec Operations Readiness Tools (SORT) website for information on the latest agent pack availability.
https://sort.symantec.com
Refer to the agent-specific configuration guide for more details about the application agents.

To install the server components,

See "Installing SFW HA server components using the product installer" on page 65.

To install the client components,

See "Installing the client components using the product installer" on page 71.

Installing SFW HA server components using the product installer

Use the following procedure to install SFW HA server components using the product installer.

Ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

During installation, some product features are installed by default and others must be selected, as follows:

- For a disaster recovery configuration, select the VCS global cluster (GCO) option.
- If you plan to use Veritas Volume Replicator (VVR) for replication, select the SFW VVR option.

- If you plan to use the Fast Failover feature, select the VCS Fast Failover option.

To install SFW HA server components using the product installer

1. Insert the disc containing the installation software into your system's disk drive or download the installation software from the Symantec website.
   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 website, 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.

Storage Foundation HA 6.0 for Windows	Click to install the server and client components for SFW HA.
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 pertinent software and hardware requirements.
SORT	Click to access the Symantec Operations Readiness Tools 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 Content	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 that belong to the domain in which you have logged in 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**.

Once you add or select a system, the wizard performs certain validation checks and notes the details in the Verification Details box. To review the details, select the desired system.

To select the installation and product options, perform the following tasks on each of the selected systems.

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**.

See Applying the selected installation and product options to 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. Click **OK**.

- 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.

The wizard validates the entered license keys and displays the relevant error if the validation fails. After the validation is complete, click **OK**.

- From the list of product options, select the appropriate options to be installed. The options differ depending on your product and environment.

Storage Foundation Options	■ Veritas Volume Replicator (VVR) Veritas Volume Replicator (VVR) replicates data across multiple sites for disaster recovery. ■ FlashSnap FlashSnap allows you to create and maintain split-mirror, persistent snapshots of volumes and application components. FlashSnap supports VSS based snapshots to provide application data in a consistent state after the application is restored. ■ Replace Disk Management Snap-in with SFW VEA GUI Replaces the Disk Management Snap-in in the Windows Computer Management console and the Server Manager console with the Veritas Enterprise Administrator GUI for Windows Server 2008.

DMP Device Specific Modules

- 3PARDATA (V3PARAA)
- Compellent array (VCOMPLNT)
- Dell EqualLogic array (VEQLOGIC)
- EMC Clarion (VEMCCLAR)
- EMC Symmetrix/DMX (VEMCSYMM)
- EMC VPLEX array (VEMCVPLX)
- FUJITSU ETERNUS 2000 array (VFUJITSUAA)
- Hitachi 95xx-AMS-WM (VHDSAP)
- Hitachi TagmaStore/HP XP (VHDSAA)
- HP 2000 array (VHPMSA2)
- HP EVA-MSA (VHPEVA)
- HUAWEI S5300/S2300 array (VHUAWEIAP)
- IBM DS AP (VIBMAPDS)
- IBM DS4000/SUN 6000 (VENGAP)
- IBM DS6000 (VIBMAP)
- IBM DS8000/ESS (VIBMAADS)
- IBM XiV Storage System (VXIV)
- NETAPP (VNETAPP)
- NEXSAN SATA/SAS Beast, E60/E18 array (VNEXSAN)
- PILLAR (VPILLAR)
- Sun array (VSUN)
- XioTech array (VXIOTECH)

Symantec maintains a Hardware Compatibility List (HCL) that lists supported hardware. The HCL provides information on HBAs and firmware that have been tested with each supported array. Check the HCL for details about your hardware before installing or using DMP DSMs.

The HCL is located at:

http://www.symantec.com/docs/TECH152806

Note: Do not use a DMP DSM together with a third-party DSM for the same array. Only one DSM at a time can claim the LUNs in an array. According to Microsoft Multipath I/O (MPIO) documentation, if multiple DSMs are installed, the Microsoft MPIO framework contacts each DSM to determine which is appropriate to handle a device. There is no particular order in which the MPIO framework contacts the DSMs. The first DSM to claim ownership of the device is associated with that device. Other DSMs cannot claim an already claimed device. Therefore, to ensure that the DMP DSM claims the LUNs of an array, no other DSM should be installed for that same array.

Veritas Cluster Server Options	■ Global Cluster Option Global Cluster Option (GCO) enables you to link the clusters located in different geographies. This provides wide-area failover and disaster recovery. ■ Fast Failover Fast failover improves the failover time taken by storage resources during the service group failovers, in a clustered environment. Fast failover is particularly noticeable in clusters having multiple storage stacks configured, typically over 20 disk groups and over 150 volumes.

7 On the System Selection panel, click **Next**.
Note that the wizard fails to proceed with the installation unless all the selected systems have passed the validation checks and are ready for installation. If the validation checks have failed on any of the systems, review the details and rectify the issue. Before you choose to proceed with the installation, 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 the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot all the selected remote systems immediately after the installation is complete on the respective system. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

9 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.
If an installation is not successful on any of the systems, the status screen shows a failed installation.

10 On the Post-install Summary panel, review the installation result and click **Next**.
If the installation has failed on any of the systems, refer to the log file for details. You may have to re-install the software.

11 On the Finish panel, click **Finish**.
If you chose to initiate the auto reboot, a confirmation message to reboot the local system appears. Click **Yes** to reboot immediately or **No** to reboot later.
If you did not choose to initiate the auto reboot, ensure that you manually reboot these systems.
This completes the product installation.

Applying the selected installation and product options to multiple systems

The following procedure gives details on applying options to multiple systems.

To apply the selected installation and product options to multiple systems

1. Click on any one of the selected systems and select the desired installation and product options.
2. Click **Apply to multiple systems**.
3. On the Apply Installation Options panel, select the installation options to be applied and then select the desired systems. Click **OK**.

Installing the client components using the product installer

Use the following procedure to install SFW HA client components using the product installer.

Note: Client components cannot be installed on server core systems.

Before you begin the installation, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress on the system where you want to install the client components.

To install SFW HA client components using the product installer

1. Insert the software disk containing the installation package into your system's disc drive or download the installation package from the following 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. Click to download the required contents.

Veritas Storage Foundation HA 6.0 for Windows	Click to install the server or client components for SFW HA.
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 pertinent software and hardware requirements.

SORT	Click to access the Symantec Operations Readiness Tools 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 Content	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 Agreement 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 installation directory.

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.

  Local host is populated by default.

- Alternatively, browse to select the systems.
  The systems that belong to the domain in which you have logged in 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**.

Once you add or select a system, the wizard performs certain validation checks and notes the details in the Verification Details box. To review the details, select the desired system.

By default the wizard uses %ProgramFiles%\Veritas as the installation directory. To customize the installation directory, click **Browse** and select the desired location. Click **OK**.

To apply the customized directory to multiple systems, click **Apply to multiple systems**. On the Apply Installation Options panel, select the systems to apply the customized directory. Click **OK**.

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

Note that the wizard fails to proceed with the installation unless all the selected systems have passed the validation checks and are ready for installation. If the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation 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**.

9 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.
If an installation is not successful on any of the systems, the status screen shows a failed installation.

10 On the Post-install Summary panel, review the installation result and click **Next**.
If the installation has failed on any of the system, refer to the log file for details. You may have to re-install the software.

11 On the Finish panel, click **Finish**.
This completes the installation of the client components.

Configuring cluster disk groups and volumes for Enterprise Vault

Before configuring Enterprise Vault for high availability, you must create cluster disk groups and volumes using the Veritas Enterprise Administrator (VEA) console installed with SFW.

Planning cluster disk groups and volumes is covered in the following topics:

Configuring cluster disk groups and volumes is covered in the following topics:

About cluster disk groups and volumes

SFW uses disk groups to organize disks or LUNs for management purposes. A dynamic disk group is a collection of disks that is imported or deported as a single unit. A cluster disk group is a special type of dynamic disk group that is created on shared storage and is designed to be moved or to failover between hosts. In order to prevent data corruption a cluster disk group uses SCSI reservations to protect the shared disks and limits access to a single host at a time.

Volumes are logical entities that are comprised of portions of one or more physical disks and are accessed by a drive letter or mount point. Volumes can be configured for performance and high availability.

Note: You create a cluster disk group and volumes on only one node of a cluster. The volumes can be accessed by other nodes in a high-availability cluster by first deporting the cluster disk group from the current node and then importing it on the desired node. In a campus cluster, the volumes are mirrored across the storage arrays.

Note: If your storage devices are SCSI-3 compliant, and you wish to use SCSI-3 Persistent Group Reservations (PGR), you must enable SCSI-3 support using the Veritas Enterprise Administrator (*VEA - Control Panel - System Settings*). See the *Veritas Storage Foundation Administrator's Guide* for more information.

Prerequisites for configuring cluster disk groups and volumes

Before you create a disk group, consider the following items:

- The type of volume configurations that are required
- The number of volumes or LUNs required for the disk group
- The implications of backup and restore operations on the disk group setup
- The size of databases and logs that depend on the traffic load

Complete the following tasks before you create the cluster disk group and volumes:

- Determine the layout or configuration for each volume and the total number of disks needed.
- Determine the initial size necessary for the volumes. You may increase the volume size at a later time using the Expand Volume command but you can not decrease the size.
- Verify that the disks you plan to include in the cluster disk group are shared and are available from all nodes. If new disks are installed, you must rescan, and if necessary, use the Write Signature command in order to identify the disks to the operating system.
- Verify that the drive letters that will be assigned to the volumes are available on all nodes so that the volumes can be accessed from any node.

For a fast failover configuration, read the following topic:

- Considerations for a fast failover configuration

For a disaster recovery configuration using Veritas Volume Replicator, read the following topic:

- Considerations for volumes for a VVR configuration

Considerations for a fast failover configuration

For VCS service groups that contain many disk groups, you can greatly reduce failover time by implementing fast failover. Fast failover is a licensable feature of SFW HA. Fast failover speeds up the failover of storage resources in several ways:

- Fast failover provides a “read-only deported” mode for disk groups on inactive nodes. This mode speeds up the process of importing a disk group.
- Fast failover maintains the current disk group configuration in memory on the inactive nodes. Any changes are automatically synchronized so that all nodes maintain an identical disk group configuration.

For more details about fast failover, refer to the *Veritas Storage Foundation Administrator’s Guide*.

To use fast failover, install the VCS Fast Failover option during SFW HA installation. Additional steps are required after you complete the service group configuration.

Take the following storage-related requirements into account if you are planning to implement fast failover.

Fast failover is currently not supported for the following:

- RAID-5 volumes
- SCSI-2
- Active/Passive (A/P) arrays for DMP

The disk group version must be 60 or later for fast failover to work. To verify the disk group version, from the VEA console, right-click the disk group and click **Properties**. Disk group version upgrade is required after upgrading SFW HA on the cluster nodes. Refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for more information.

Considerations for volumes for a VVR configuration

For a configuration using Veritas Volume Replicator, either a disaster recovery configuration on a secondary site or a Replicated Data Cluster, note the following:

- VVR does not support the following types of volumes:
  - SFW (software) RAID 5 volumes
  - Volumes with the Dirty Region Log (DRL)
  - Data Change Object (DCO)
  - Volumes with commas in the names
- A configuration with VVR requires a Storage Replicator Log (SRL) volume for each disk group that contains volumes that are replicated. You can create the SRL volume when configuring the other volumes for the application or you can create it later when you set up replication. If you create it later, ensure that you allow sufficient disk space for this volume. For more about VVR planning, see the *Veritas Volume Replicator, Administrator’s Guide*.

- Do not assign a drive letter to the Storage Replicator Log volume. This will limit access to that volume and avoid potential data corruption.

Sample disk group and volume configuration

For an SFW HA solution, you first create a cluster disk group (EVDG) on shared disks and then create volumes for the following:

- MSMQ data
- Registry replication data
- Various EV services data (Indexing service, Shopping service, Vault store partitions, PST holding folders, etc.)

Viewing the available disk storage

Before creating disk groups and volumes you may want to view available disk storage.

To view the available disk storage

1. Open the VEA console (launch from the Solutions Configuration Center, or by clicking **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator**). 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. In the VEA configuration tree, expand **hostname > StorageAgent** and then click **Disks**.
   The internal names for the disks that the current system can access for available storage are displayed, with names Harddisk1, Harddisk2, etc. The list includes both disks internal to the local system and any external storage that is available.

Creating a cluster disk group

Use the Veritas Enterprise Administrator (VEA) to create a cluster disk group on the first node where Enterprise Vault is being installed and configured. Repeat the procedure if you want to create additional disk groups.

To create a dynamic (cluster) disk group

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

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 Groups** 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:
   - In the **Group Name** field, enter the name of the disk group, for example, EVDG.
   - 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**.
7. Click **Next** to accept the confirmation screen with the selected disks.
8. Click **Finish** to create the new disk group.

Creating volumes

This procedure will guide you through the process of creating a volume on a cluster disk group. Repeat the procedure to create additional volumes.

Before you begin, review the following topic if applicable to your environment:

- Considerations for volumes for a VVR configuration

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

To create dynamic volumes

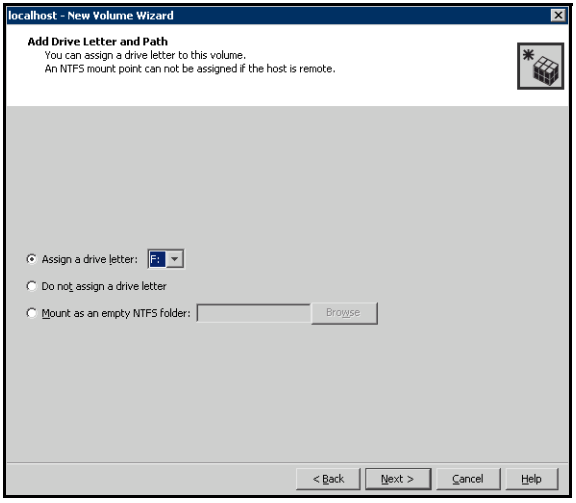
1. If the VEA console is not already open, click **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator** and select a profile if prompted.
2. Click **Connect to a Host or Domain**.
3. In the Connect dialog box select the host name from the pull-down menu and 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.
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.
   - For Site Preference, leave the setting as **Siteless** (the default).
   - Automatic disk selection is the default setting. To manually select the disks, click **Manually select disks** and use the **Add** and **Remove** buttons to move the appropriate disks to the **Selected disks** list. Manual selection of disks is recommended.
   - 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.

- 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 volume layout type. To select mirrored striped, click both the **Mirrored** checkbox and the **Striped** radio button.
- If you are creating a striped volume, the **Columns** and **Stripe unit size** boxes need to have entries. Defaults are provided.
- 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.
- If creating a Replicator Log volume for Veritas Volume Replicator, select **Do not assign a drive letter**.



9 Click **Next**.

10 Create an NTFS file system.
   - Make sure the **Format this volume** checkbox is checked and click **NTFS**.
   - For a VVR configuration, for the Replicator Log volume only, clear the **Format this volume** check box.
   - 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**.
11 Click **Finish** to create the new volume.
12 Repeat these steps to create additional volumes.
   Create the cluster disk group and volumes on the first node of the cluster only.

About managing disk groups and volumes

Importing a disk group and mounting a volume

Use the 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 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.
5. 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**.

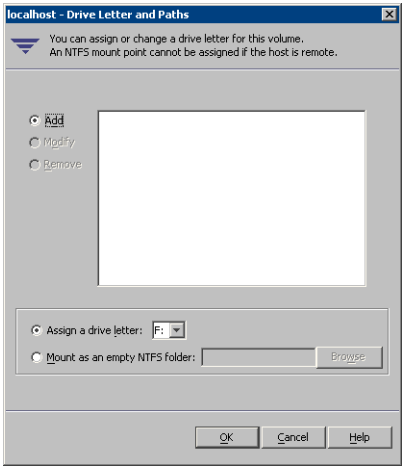
Adding drive letters to mount the volumes

Occasionally, when a disk group is imported a drive letter may not be associated with an existing volume. If this occurs, use the VEA console to add a drive letter and mount the volume so that it can be seen by the operating system. You can also mount the volume as a folder. Verify that all volumes are mounted.

To add a drive letter or path to a volume

1 Navigate to the **Volumes** folder.

2 Right-click the volume, click **File System** and click **Change Drive Letter and Path**.



3 In the Drive Letter and Paths dialog box, click **Add**.

4 Select one of the following options 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 the **Assign a Drive Letter** option and select a drive letter from the drop-down list.
- *To mount the volume as a folder*
  Select the **Mount as an empty NTFS folder** option and click **Browse** to locate an empty folder on the shared disk.

Note: Assign the same drive letter or mount path that was assigned when the volume was created.

5 Click **OK**.

Deporting the cluster disk group

To move ownership of the cluster disk group to another node, you use the Veritas Enterprise Administrator (VEA) to deport the clustered cluster disk group from the current node and then import it to the desired node.

To deport the cluster disk group

1 Stop all processes accessing the volumes in the cluster disk group.

2 Click **Start > All Programs > Symantec > Veritas Enterprise Administrator** and if prompted, select a profile.

3 Click **Connect to a Host or Domain** and in the Connect dialog box, specify the host name and click **Connect**.

4 In the tree view, expand the system name where the disk group is current imported, expand **Storage Agent**, and expand **Disk Groups**.

5 In the tree view, right-click the cluster disk group to be deported and select **Deport Dynamic Disk Group**.

6 Click **Yes** to deport the dynamic cluster disk group.

Configuring the cluster

The VCS Cluster Configuration Wizard (VCW) sets up the cluster infrastructure, including LLT and GAB, and configures Symantec Product Authentication Service in the cluster. The wizard also provides the option to configure the ClusterService group, which can contain resources for notification and global clusters.

Complete the following tasks before creating a cluster:

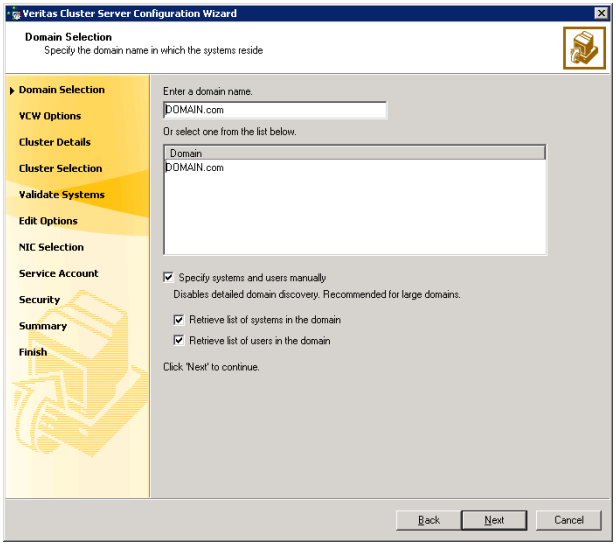
- Verify that each node uses static IP addresses and that name resolution is configured for each node.
- Verify that you have the required privileges.
  See "Reviewing the requirements" on page 46.

Refer to the *Veritas Cluster Server Administrator's Guide* for complete details on VCS, including instructions on adding cluster nodes or removing or modifying cluster configurations.

To configure a VCS cluster

1. Start the VCS Cluster Configuration Wizard.
   Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Cluster Configuration Wizard**.
2. Read the information on the Welcome panel and click **Next**.
3. On the Configuration Options panel, click **Cluster Operations** and click **Next**.

4 On the Domain Selection panel, select or type the name of the domain in which the cluster resides and select the discovery options.



Do one of the following:

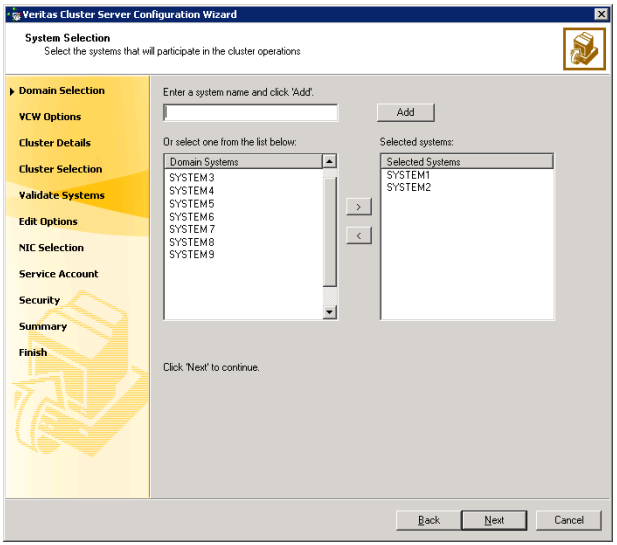
- To discover information about all systems and users in the domain:
  - Clear the **Specify systems and users manually** check box.
  - Click **Next**.
  - Proceed to step 8 on page 87.
- To specify systems and user names manually (recommended for large domains):
  - Check the **Specify systems and users manually** check box. Additionally, you may instruct the wizard to retrieve a list of systems and users in the domain by selecting appropriate check boxes.
  - Click **Next**.
  - If you chose to retrieve the list of systems, proceed to step 6 on page 87. Otherwise, proceed to the next step.

5 On the System Selection panel, type the name of each system to be added, click **Add**, and then click **Next**.

Do not specify systems that are part of another cluster.

Proceed to step 8 on page 87.

6 On the System Selection panel, specify the systems for the cluster and then click **Next**. Do not select systems that are part of another cluster.



Enter the name of the system and click **Add** to add the system to the Selected Systems list, or click to select the system in the Domain Systems list and then click the **>** (right-arrow) button.

7 The System Report panel displays the validation status, whether *Accepted* or *Rejected*, of all the systems you specified earlier. Review the status and then click **Next**.

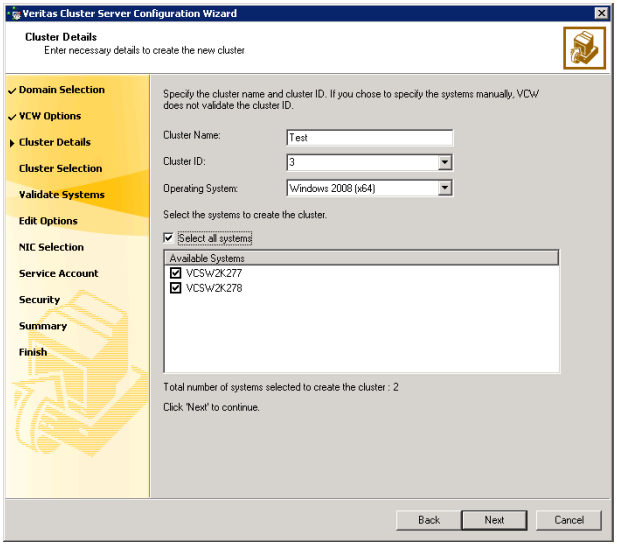
Click on a system name to see the validation details. If you wish to include a rejected system, rectify the error based on the reason for rejection and then run the wizard again.

A system can be rejected for any of the following reasons:

- System is not pingable.
- WMI access is disabled on the system.
- Wizard is unable to retrieve the system architecture or operating system.
- VCS is either not installed on the system or the version of VCS is different from what is installed on the system on which you are running the wizard.

8 On the Cluster Configuration Options panel, click **Create New Cluster** and click **Next**.

9 On the Cluster Details panel, specify the details for the cluster and then click **Next**.



Cluster Name — Type a name for the new cluster. Symantec recommends a maximum length of 32 characters for the cluster name.

Cluster ID — Select a cluster ID from the suggested cluster IDs in the drop-down list or type a unique ID for the cluster. The cluster ID can be any number from 0 to 65535.

Caution: If you chose to specify systems and users manually in step 4 or if you share a private network between more than one domain, make sure that the cluster ID is unique.

Operating System — From the drop-down list select the operating system.
The Available Systems box then displays all the systems that are running the specified operating system.
All the systems in the cluster must have the same operating system and architecture. You cannot configure a Windows Server 2008 and a Windows Server 2008 R2 system in the same cluster.

Available Systems	Select the systems that you wish to configure in the cluster. Check the **Select all systems** check box to select all the systems simultaneously. The wizard discovers the network interface cards (NICs) on the selected systems. For single-node clusters with the required number of NICs, the wizard prompts you to configure a private link heartbeat. In the dialog box, click **Yes** to configure a private link heartbeat.

10 The wizard validates the selected systems for cluster membership. After the systems are validated, click **Next**.

If a system is not validated, review the message associated with the failure and restart the wizard after rectifying the problem.

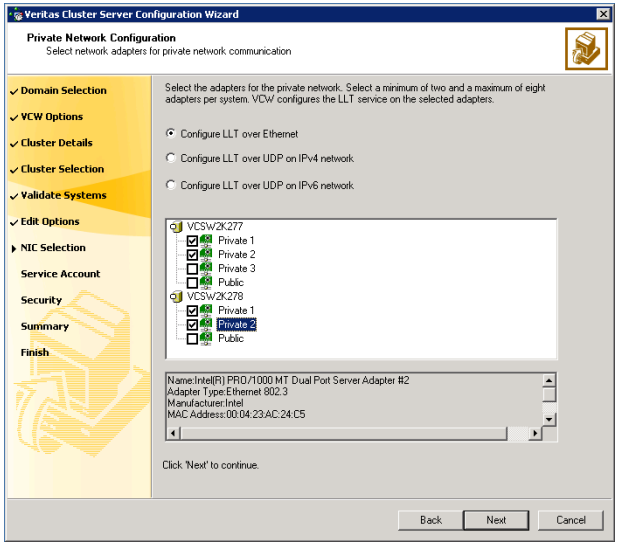
If you chose to configure a private link heartbeat in the earlier step, proceed to the next step. Otherwise, proceed to step 12 on page 91.

11 On the Private Network Configuration panel, configure the VCS private network and then click **Next**.

You can configure the VCS private network either over ethernet or over the User Datagram Protocol (UDP) layer using IPv4 or IPv6 network.

Do one of the following:

- To configure the VCS private network over the ethernet, complete the following steps:



- Select **Configure LLT over Ethernet**.

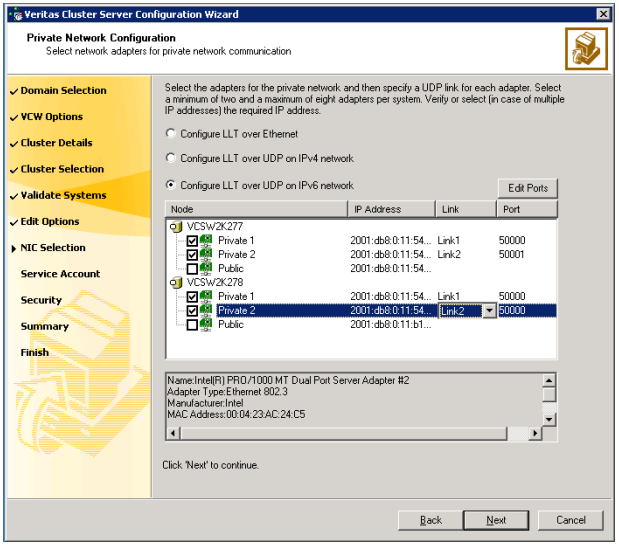
- Select the check boxes next to the two NICs to be assigned to the private network. You can assign a maximum of eight network links.

  Symantec recommends reserving two NICs exclusively for the private network. However, you could lower the priority of one of the NICs and use the low-priority NIC for both public and private communication.
- If you have only two NICs on a selected system, it is recommended that you lower the priority of at least one NIC that will be used for private as well as public network communication.

  To lower the priority of a NIC, right-click the NIC and select **Low Priority** from the pop-up menu.
- If your configuration contains teamed NICs, the wizard groups them as "NIC Group #N" where "N" is a number assigned to the teamed NIC. A teamed NIC is a logical NIC, formed by grouping several physical NICs together. All NICs in a team have an identical MAC address. Symantec recommends that you do not select teamed NICs for the private network.

The wizard configures the LLT service (over ethernet) on the selected network adapters.

- To configure the VCS private network over the User Datagram Protocol (UDP) layer, complete the following steps:



- Select **Configure LLT over UDP on IPv4 network** or **Configure LLT over UDP on IPv6 network** depending on the IP protocol that you wish to use.

  The IPv6 option is disabled if the network does not support IPv6.
- Select the check boxes next to the two NICs to be assigned to the private network. You can assign a maximum of eight network links.

  Symantec recommends reserving at least two adapters exclusively for the VCS private network.
- For each selected NIC, verify the displayed IP address. If a selected NIC has multiple IP addresses assigned, double-click the field and choose the desired IP address from the drop-down list. In case of IPv4, each IP address can be in a different subnet.

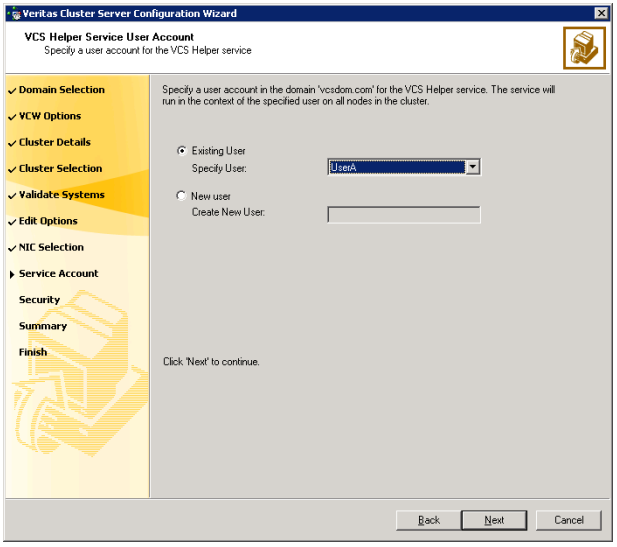
  The IP address is used for the VCS private communication over the specified UDP port.
- Specify a unique UDP port for each of the link. Click **Edit Ports** if you wish to edit the UDP ports for the links. You can use ports in the range 49152 to 65535. The default ports numbers are 50000 and 50001 respectively. Click **OK**.

  For each selected NIC, double-click the respective field in the Link column and choose a link from the drop-down list. Specify a different link (Link1 or Link2) for each adapter. Each link is associated with a UDP port that you specified earlier.

The wizard configures the LLT service (over UDP) on the selected network adapters. The specified UDP ports will be used for the private network communication.

12 On the VCS Helper Service User Account panel, specify a domain user account for the VCS Helper service. The VCS high availability engine (HAD), which runs in the context of the local system built-in account, uses the VCS Helper service user context to access the network.

This account does not require Domain Administrator privileges.



Specify a domain user as follows:

- To specify an existing user, do one of the following:
  - Click **Existing user** and select a user name from the drop-down list
  - If you chose not to retrieve the list of users in step 4 on page 86, type the user name in the **Specify User** field, and then click **Next**.
- To specify a new user, click **New user** and type a valid user name in the Create New User field, and then click **Next**.

  Do not append the domain name to the user name; do not type the user name as Domain\user or user@domain.
- In the Password dialog box, type the password for the specified user and click **OK**, and then click **Next**.

13 On the Configure Security Service Option panel, specify the security options for the cluster communications and then click **Next**.

Do one of the following:

- To use VCS cluster user privileges, click **Use VCS User Privileges** and then type a user name and password.

  The wizard configures this user as a VCS Cluster Administrator. In this mode, communication between cluster nodes and clients, including the Cluster Manager (Java Console), occurs using the encrypted VCS cluster administrator credentials. The wizard uses the VCSEncrypt utility to encrypt the user password.

The default user name for the VCS administrator is *admin* and the password is *password*. Both are case-sensitive. You can accept the default user name and password for the VCS administrator account or type a new name and password.

Symantec recommends that you specify a new user name and password.

- To configure a secure cluster using the single sign-on feature, click **Use Single Sign-on**.

  In this mode, the VCS Authentication Service is used to secure communication between cluster nodes and clients by using digital certificates for authentication and SSL to encrypt communication over the public network. VCS uses SSL encryption and platform-based authentication. The VCS high availability engine (HAD) and Veritas Command Server run in secure mode.

  The wizard configures all the cluster nodes as root brokers (RB) and authentication brokers (AB). Authentication brokers serve as intermediate registration and certification authorities. Authentication brokers have certificates signed by the root. These brokers can authenticate clients such as users and services. The wizard creates a copy of the certificates on all the cluster nodes.

14 Review the summary information on the Summary panel, and click **Configure**.

   The wizard configures the VCS private network. If the selected systems have LLT or GAB configuration files, the wizard displays an informational dialog box before overwriting the files. In the dialog box, click **OK** to overwrite the files. Otherwise, click **Cancel**, exit the wizard, move the existing files to a different location, and rerun the wizard.

   The wizard starts running commands to configure VCS services. If an operation fails, click **View configuration log file** to see the log.

15 On the Completing Cluster Configuration panel, click **Next** to configure the ClusterService group; this group is required to set up components for notification and for global clusters.

   To configure the ClusterService group later, click **Finish**.

   At this stage, the wizard has collected the information required to set up the cluster configuration. After the wizard completes its operations, with or without the ClusterService group components, the cluster is ready to host application service groups. The wizard also starts the VCS engine (HAD) and the Veritas Command Server at this stage.

Note: After configuring the cluster you must not change the names of the nodes that are part of the cluster. If you wish to change a node name, run this wizard to remove the node from the cluster, rename the system, and then run this wizard again to add that system to the cluster.

16 On the Cluster Service Components panel, select the components to be configured in the ClusterService service group and click **Next**.

- Check the **Notifier Option** check box to configure notification of important events to designated recipients.
  See "Configuring notification" on page 94.
- Check the **GCO Option** check box to configure the wide-area connector (WAC) process for global clusters. The WAC process is required for inter-cluster communication.
  Configure the GCO Option using this wizard only if you are configuring a Disaster Recovery (DR) environment and are not using the Disaster Recovery wizard.
  Refer to the *Veritas Cluster Server Administrator's Guide* for details on configuring GCO using the cluster configuration wizard.

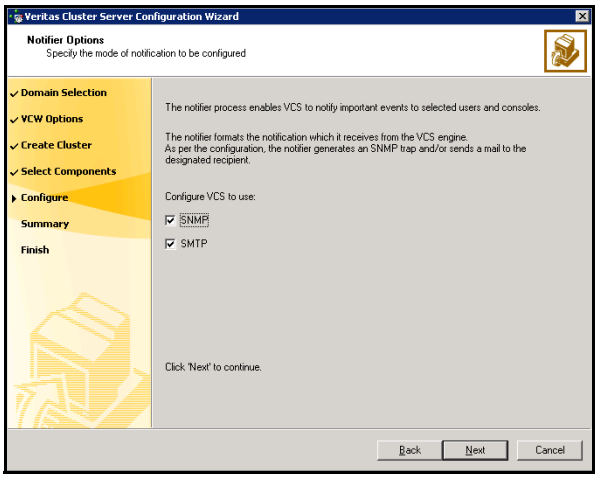
  You can configure the GCO Option using the DR wizard. The Disaster Recovery chapters discuss how to use the Disaster Recovery wizard to configure the GCO option.

Configuring notification

This section describes steps to configure notification.

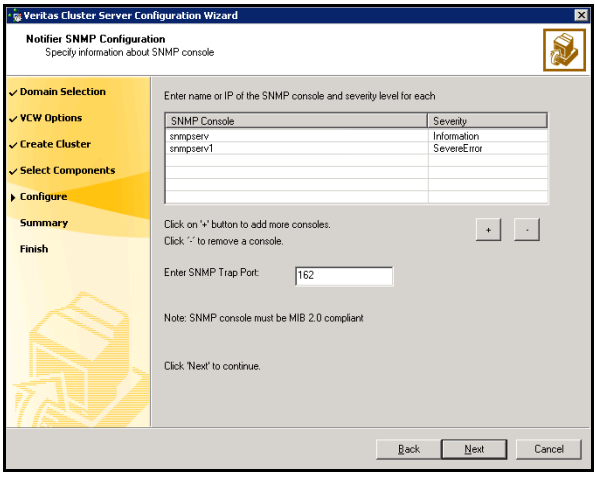
To configure notification

1 On the Notifier Options panel, specify the mode of notification to be configured and click **Next**.



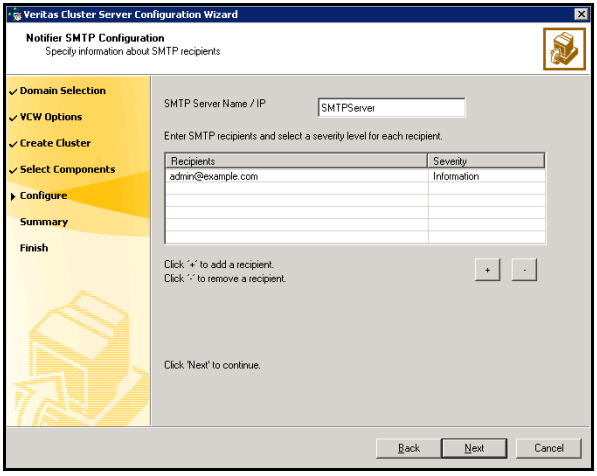
You can configure VCS to generate SNMP (V2) traps on a designated server and send emails to designated recipients in response to certain events.

2 If you chose to configure SNMP, specify information about the SNMP console and click **Next**.



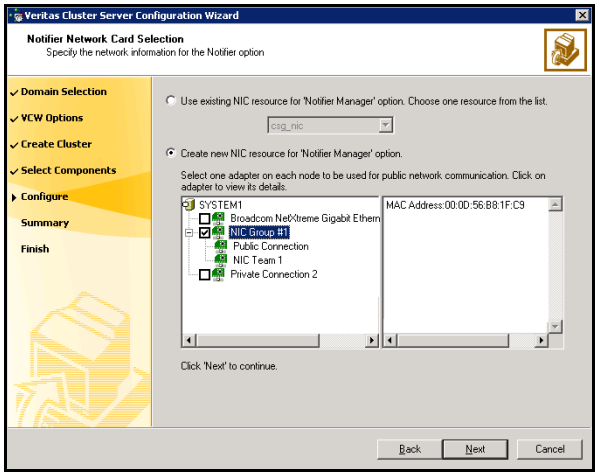
- Click a field in the SNMP Console column and type the name or IP address of the console. The specified SNMP console must be MIB 2.0 compliant.
- Click the corresponding field in the Severity column and select a severity level for the console.
- Click '**+**' to add a field; click '**-**' to remove a field.
- Enter an SNMP trap port. The default value is "162".

3 If you chose to configure SMTP, specify information about SMTP recipients and click **Next**.



- Type the name of the SMTP server.
- Click a field in the Recipients column and enter a recipient for notification. Enter recipients as admin@example.com.
- Click the corresponding field in the Severity column and select a severity level for the recipient. VCS sends messages of an equal or higher severity to the recipient.
- Click **+** to add fields; click **-** to remove a field.

4 On the Notifier Network Card Selection panel, specify the network information and click **Next**.



- If the cluster has a ClusterService service group configured, you can use the NIC resource configured in the service group or configure a new NIC resource for notification.
- If you choose to configure a new NIC resource, select a network adapter for each node in the cluster. The wizard lists the public network adapters along with the adapters that were assigned a low priority.

5 Review the summary information and choose whether you want to bring the notification resources online when VCS is started.

6 Click **Configure**.

7 Click **Finish** to exit the wizard.

Adding a node to an existing VCS cluster

You use the VCS Cluster Configuration Wizard (VCW) to add one or more nodes to an existing VCS cluster.

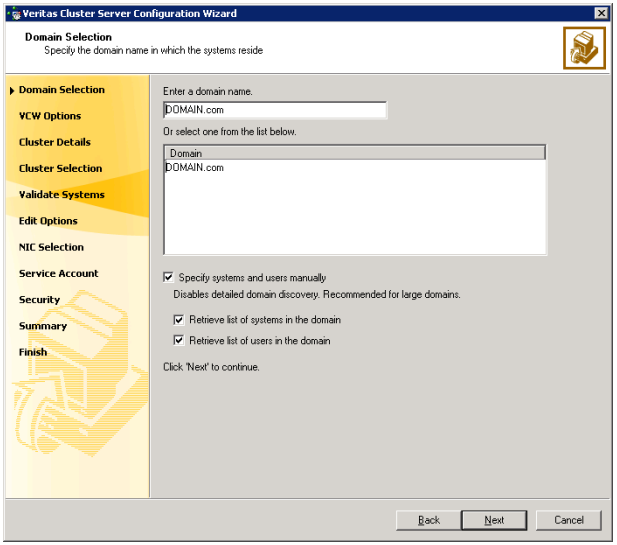
Prerequisites for adding a node to an existing cluster are as follows:

- Verify that the logged-on user has VCS Cluster Administrator privileges.
- The logged-on user must be a local Administrator on the system where you run the wizard.

- Verify that Command Server is running on all nodes in the cluster. Select Services on the Administrative Tools menu and verify that the Veritas Command Server shows that it is started.
- Verify that the Veritas High Availability Daemon (HAD) is running on the node on which you run the wizard. Select Services on the Administrative Tools menu and verify that the Veritas High Availability Daemon is running.

To add a node to a VCS cluster

1. Start the VCS Cluster Configuration wizard.
   Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Cluster Configuration Wizard**.
   Run the wizard from the node to be added or from a node in the cluster. The node that is being added should be part of the domain to which the cluster belongs.
2. Read the information on the Welcome panel and click **Next**.
3. On the Configuration Options panel, click **Cluster Operations** and click **Next**.
4. In the Domain Selection panel, select or type the name of the domain in which the cluster resides and select the discovery options.



Do one of the following:

- To discover information about all the systems and users in the domain:
  - Clear the **Specify systems and users manually** check box.

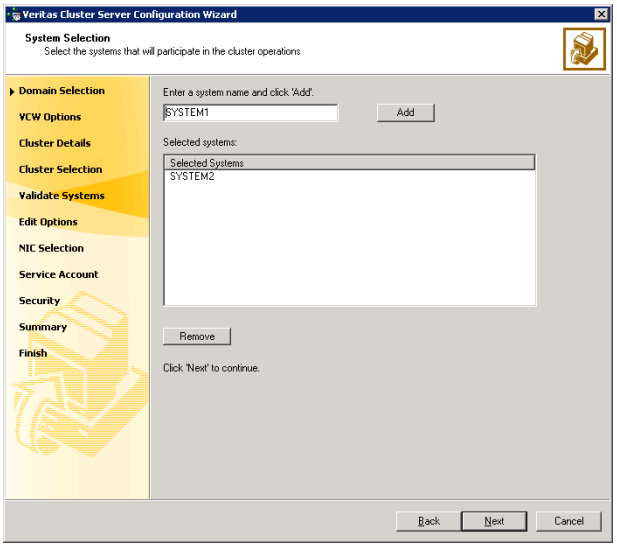
- Click **Next**.

Proceed to step 8 on page 101.

- To specify systems and user names manually (recommended for large domains):
  - Check the **Specify systems and users manually** check box. Additionally, you may instruct the wizard to retrieve a list of systems and users in the domain by selecting appropriate check boxes.
  - Click **Next**.

If you chose to retrieve the list of systems, proceed to step 6 on page 100. Otherwise proceed to the next step.

5 On the System Selection panel, complete the following and click **Next**.

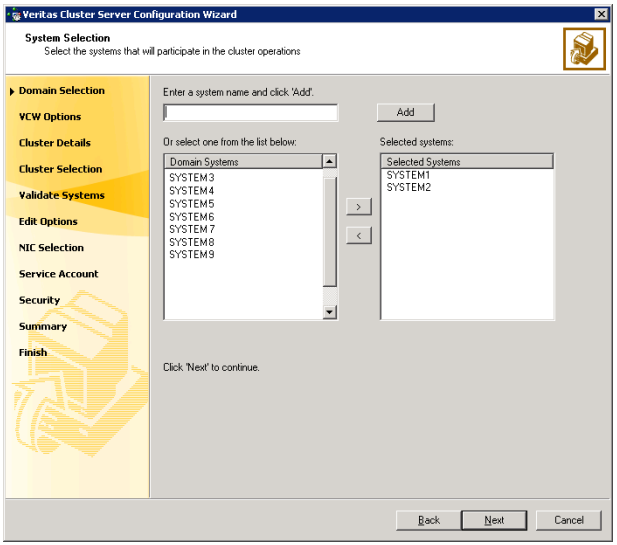


- Type the name of a node in the cluster and click **Add**.
- Type the name of the system to be added to the cluster and click **Add**.

If you specify only one node of an existing cluster, the wizard discovers all nodes for that cluster. To add a node to an existing cluster, you must specify a minimum of two nodes; one that is already a part of a cluster and the other that is to be added to the cluster.

Proceed to step 8 on page 101.

6 On the System Selection panel, specify the systems to be added and the nodes for the cluster to which you are adding the systems.



Enter the system name and click **Add** to add the system to the **Selected Systems** list. Alternatively, you can select the systems from the **Domain Systems** list and click the right-arrow icon.

If you specify only one node of an existing cluster, the wizard discovers all nodes for that cluster. To add a node to an existing cluster, you must specify a minimum of two nodes; one that is already a part of a cluster and the other that is to be added to the cluster.

7 The System Report panel displays the validation status, whether *Accepted* or *Rejected*, of all the systems you specified earlier. Review the status and then click **Next**.

A system can be rejected for any of the following reasons:

- System is not pingable.
- WMI access is disabled on the system.
- Wizard is unable to retrieve the system architecture or operating system.
- VCS is either not installed on the system or the version of VCS is different from what is installed on the system on which you are running the wizard.

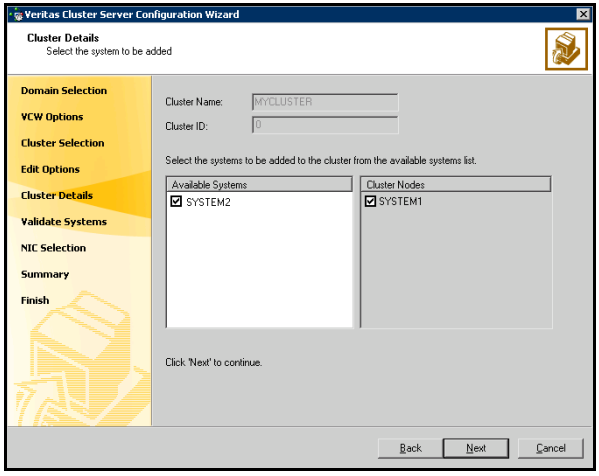
Click on a system name to see the validation details. If you wish to include a rejected system, rectify the error based on the reason for rejection and then run the wizard again.

8 On the Cluster Configuration Options panel, click **Edit Existing Cluster** and click **Next**.

9 On the Cluster Selection panel, select the cluster to be edited and click **Next**.
If you chose to specify the systems manually in step 4, only the clusters configured with the specified systems are displayed.

10 On the Edit Cluster Options panel, click **Add Nodes** and click **Next**.
In the Cluster User Information dialog box, type the user name and password for a user with administrative privileges to the cluster and click **OK**.
The Cluster User Information dialog box appears only when you add a node to a cluster with VCS user privileges, that is when the cluster configuration does not use the Symantec Product Authentication Service for secure cluster communication.

11 On the Cluster Details panel, check the check boxes next to the systems to be added to the cluster and click **Next**.



The right pane lists nodes that are part of the cluster. The left pane lists systems that can be added to the cluster.

12 The wizard validates the selected systems for cluster membership. After the nodes have been validated, click **Next**.
If a node does not get validated, review the message associated with the failure and restart the wizard after rectifying the problem.

13 On the Private Network Configuration panel, configure the VCS private network communication on each system being added and then click **Next**.
How you configure the VCS private network communication depends on

how it is configured in the cluster. If LLT is configured over ethernet, you have to use the same on the nodes being added. Similarly, if LLT is configured over UDP in the cluster, you have to use the same on the nodes being added.

Do one of the following:

- To configure the VCS private network over ethernet, complete the following steps:
  - Select the check boxes next to the two NICs to be assigned to the private network.
    Symantec recommends reserving two NICs exclusively for the private network. However, you could lower the priority of one NIC and use the low-priority NIC for both public and private communication.
  - If you have only two NICs on a selected system, it is recommended that you lower the priority of at least one NIC that will be used for private as well as public network communication.
    To lower the priority of a NIC, right-click the NIC and select **Low Priority** from the pop-up menu.
  - If your configuration contains teamed NICs, the wizard groups them as "NIC Group #N" where "N" is a number assigned to the teamed NIC. A teamed NIC is a logical NIC, formed by grouping several physical NICs together. All NICs in a team have an identical MAC address. Symantec recommends that you do not select teamed NICs for the private network.

  The wizard configures the LLT service (over ethernet) on the selected network adapters.
- To configure the VCS private network over the User Datagram Protocol (UDP) layer, complete the following steps:
  - Select the check boxes next to the two NICs to be assigned to the private network. You can assign maximum eight network links.
    Symantec recommends reserving at least two NICs exclusively for the VCS private network.
  - Specify a unique UDP port for each of the link. Click **Edit Ports** if you wish to edit the UDP ports for the links. You can use ports in the range 49152 to 65535. The default ports numbers are 50000 and 50001 respectively. Click **OK**.
  - For each selected NIC, verify the displayed IP address. If a selected NIC has multiple IP addresses assigned, double-click the field and choose the desired IP address from the drop-down list. In case of IPv4, each IP address can be in a different subnet.

The IP address is used for the VCS private communication over the specified UDP port.

- For each selected NIC, double-click the respective field in the Link column and choose a link from the drop-down list. Specify a different link (Link1 or Link2) for each NIC. Each link is associated with a UDP port that you specified earlier.

The wizard configures the LLT service (over UDP) on the selected network adapters. The specified UDP ports will be used for the private network communication.

14 On the Public Network Communication panel, select a NIC for public network communication, for each system that is being added, and then click **Next**.

This step is applicable only if you have configured the ClusterService service group, and the system being added has multiple adapters. If the system has only one adapter for public network communication, the wizard configures that adapter automatically.

15 Specify the password for the user in whose context the VCS Helper service runs.

16 Review the summary information and click **Add**.

The wizard starts running commands to configure the VCS components on the node. In case of a secure cluster, the wizard also configures the VCS Authentication Service on the new node that is being added.

17 After all commands have been successfully run, click **Finish**.

Chapter 6

Installing and configuring Enterprise Vault for failover

This chapter contains the following topics:

Installing Enterprise Vault

Install Enterprise Vault on the cluster nodes.

For installation instructions, see the Enterprise Vault documentation.

Configuring the Enterprise Vault service group

Before you configure Enterprise Vault in an SFW HA cluster environment, you must configure a service group to represent the Enterprise Vault server.

This section describes how to configure an Enterprise Vault (EV) Server service group using the Enterprise Vault Cluster Setup Wizard.

Before you configure an EV service group

Before you configure an Enterprise Vault service group, do the following:

- Verify that you have installed the Enterprise Vault Cluster Setup Wizard. If you have not installed it during SFW HA installation, use Windows Add or Remove Programs to install it.
- Verify that you have configured a cluster using the VCS Cluster Configuration Wizard (VCW).
- Verify your DNS server settings. You must ensure that a static DNS entry maps the virtual IP address with the virtual server name. Refer to the appropriate DNS document for more information.
- Verify that the Veritas High Availability Daemon (HAD) is running on the system from where you will run the Enterprise Vault Cluster Setup Wizard.
- Ensure that you have Cluster Administrator privileges. You must also be a Local Administrator on the node where you run the wizard.
- If you have configured a Firewall, add the following to the Firewall Exceptions list:
  - Port 14150 or the VCS Command Server service, `%vcs_home%\bin\CmdServer.exe`.
    Here, *%vcs_home%* is the installation directory for VCS, typically `C:\Program Files\Veritas\Cluster Server`.
  - Port 14141
    For a detailed list of services and ports used by SFW HA, refer to the *Veritas Storage Foundation and High Availability Solutions for Windows Installation and Upgrade Guide*.
- Verify that MSMQ is installed locally on each node that will be part of the EV service group.

- Ensure that you mount the shared volumes you created for EV on the node from which you will run the wizard and unmount the volumes from other nodes in the cluster.
  See "About managing disk groups and volumes" on page 82.

Creating an EV service group

Complete the following steps to create a service group for EV.

To create the EV service group

1. Start the EV Cluster Setup Wizard.
   Click **Start > All Programs > Symantec > Veritas Cluster Server > Solutions Configuration Center** to start the Solutions Configuration Center (SCC). Expand the Solutions for Enterprise Vault Server tab and click **High Availability (HA) Configuration (New Server) > Configure the Enterprise Vault Service Group > Enterprise Vault Cluster Setup Wizard**.
2. Review the information in the Welcome panel and click **Next**.
3. On the Wizard Options panel click **Create service group** and then click **Next**.
4. On the Service Group Configuration panel, specify the service group details and then click **Next**.

Service Group Name	Type a name for the EV service group.
Available Cluster Systems	Select the systems on which to configure the service group and click the right arrow to move the systems to the service group's system list. To remove a system from the service group's system list, click the system in the Systems in Priority Order box and click the left arrow. To change a system's priority in the service group's system list, click the system from the Systems in Priority Order and click the up and down arrows. System priority defines the order in which service groups are failed over to systems. The system at the top of the list has the highest priority while the system at the bottom of the list has the lowest priority.

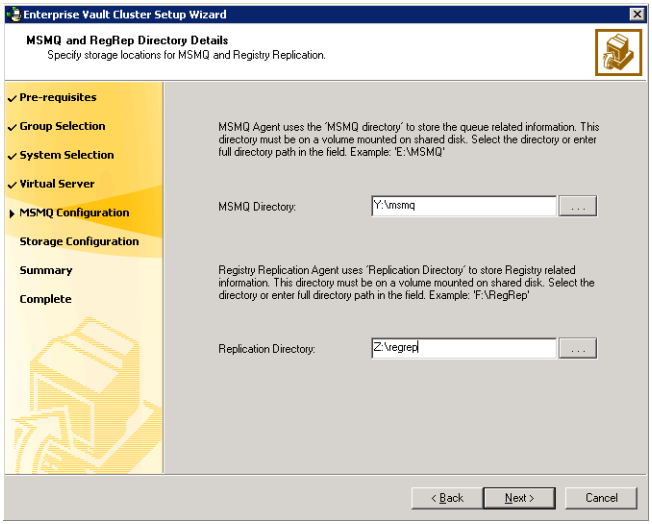
5. On the Virtual Server Configuration panel, specify information related to your network and then click **Next**.

   - Select **IPv4** to configure an IPv4 address for the EV virtual server.

- In the Virtual IP Address field, type a unique virtual IPv4 address for the EV virtual server.
- In the Subnet Mask field, type the subnet to which the virtual IPv4 address belongs.

- Select **IPv6** to configure an IPv6 address for the EV virtual server. The IPv6 option is disabled if the network does not support IPv6.
  - Select the network from the drop-down list. The wizard uses the network prefix and automatically generates an IPv6 address that is valid and unique on the network.
- In the Virtual Server Name field, type a unique name for the EV virtual server. This is the name by which the EV server will be referenced by clients. The virtual name must not exceed 15 characters.
  You will need to specify the same name when running the Enterprise Vault Configuration Wizard.
- For each system in the cluster, select the public network adapter name. The Adapter Display Name field displays the TCP/IP enabled adapters on a system, including the private network adapters, if applicable.
  To view the adapters associated with a system, click the Adapter Display Name field and click the arrow. Verify that you select the adapters assigned to the public network, not the private.
- If you require a computer object to be created in the Active Directory (AD), click **Advanced Settings**, check the **Active Directory Update Required** checkbox, specify the desired Organizational Unit in the domain and then click **OK**.
  This sets the Lanman resource attributes ADUpdateRequired and ADCriticalForOnline to true. This allows the Lanman agent to update Active Directory with the SQL virtual server name.
  You can type the OU details in the format **CN=Computers,DC=domainname,DC=com**.
  To search for the OU, click the ellipsis button and specify the search criteria in the Windows Find Organizational Units dialog box. By default, the Lanman resource adds the virtual server to the default container "Computers."
- Click **OK**. The user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts.

6 On the MSMQ and RegRep Directory Details panel, complete the following and then click **Next**:



MSMQ Directory	Type a path or click ... (ellipsis button) to browse for the directory. All MSMQ data is stored at this location. **Note:** The wizard, by default, also stores the Indexing service and Shopping service data at this location. You can modify the location while configuring the EV Server, later.
Replication Directory	Type a path or click ... (ellipsis button) to browse for the registry replication directory. This directory contains the list of registry keys to replicate. Symantec recommends that you configure the MSMQ and registry replication directories on different volumes.

7 On the Storage Location Details panel, select the volumes that you want to configure for EV data and then click **Next**.
Select the volumes from the Available Volumes box and then click the right arrow button to move them to the Selected Volumes box.
The volumes listed in the Available volumes box do not include the volumes you specified for MSMQ and registry replication.

8 On the Service Group Summary panel, review the service group configuration and click **Next**.

A message appears informing you that the wizard will run commands to modify the service group configuration. Click **Yes**. The wizard starts running commands to create the service group. Various messages indicate the status of these commands.

Resources	Displays a list of configured resources. The wizard assigns unique names to resources. Change the names of resource, if required. To edit a resource name, select the resource name and either click it or press the F2 key. Edit the resource name and then press the Enter key to confirm the changes. To cancel editing a resource name, press the Esc key.
Attributes	Displays the attributes and their configured values, for a resource selected in the Resources list.

9 On the completion dialog box, check **Bring the service group online** check box to bring the EV service group online on the local system, and then click **Finish**.

If you plan to enable fast failover for disk groups, see the following topic:

See "Enabling fast failover for disk groups (optional)" on page 110.

Otherwise, you can proceed to configuring EV using the EV Configuration Wizard.

See "Configuring Enterprise Vault Server in a cluster environment" on page 112.

Enabling fast failover for disk groups (optional)

For service groups that contain many disk groups, you can greatly reduce failover time by implementing the SFW fast failover feature for disk groups.

More information is available about fast failover benefits and requirements.

See "Considerations for a fast failover configuration" on page 75.

To use fast failover for VCS clusters, install the VCS Fast Failover option during SFW HA installation. A license is required to activate the feature.

Use the procedure below to enable fast failover for disk groups after you complete the service group configuration.

Note: The disk group version must be 60 or later for fast failover to work. To verify the disk group version, from the VEA console, right-click the disk group and click **Properties**. Disk group version upgrade is required after upgrading SFW HA on the cluster nodes. Refer to the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for more information.

For implementing the fast failover feature, VCS provides a new attribute, FastFailOver, for the Volume Manager Diskgroup (VMDg) resource. This attribute determines whether or not a disk group is enabled for fast failover.

The following procedure uses the VCS Java Console to enable the FastFailOver attribute. Refer to the *Veritas Cluster Server Administrator's Guide* for more information about the Cluster Manager (Java Console).

To enable the FastFailover attribute for a VMDg resource

1. In Cluster Manager (Java Console), select a service group with a VMDg resource configured for it. Select the **Properties** tab from the right pane.
2. Scroll down to choose the **FastFailOver** attribute and click to edit the attribute value.
3. In the **Edit Attribute** dialog box, check the **FastFailOver** check box and then click **OK**.
4. Repeat these steps for every VMDg resource for which you want to enable fast failover.

Configuring Enterprise Vault Server in a cluster environment

The Enterprise Vault Configuration Wizard provides options for setting up Enterprise Vault in a cluster. You must run the wizard on each node of the cluster.

Before running the wizard, do the following:

- Ensure that the Enterprise Vault service group is configured and online on the first node where you run the Enterprise Vault Configuration Wizard.
- Ensure that Enterprise Vault is installed on all additional nodes where you run the wizard.

To configure Enterprise Vault Server in a cluster environment

1. Click **Start** > **All Programs** > **Symantec** > **Veritas Cluster Server** > **Solutions Configuration Center**. Expand the Solutions for Enterprise Vault tab and click **High Availability (HA) Configuration (New Server) > Configure the Enterprise Vault Server in a cluster environment > Enterprise Vault Configuration Wizard**.
2. Use the Enterprise Vault Configuration Wizard to configure Enterprise Vault on the first node. Follow these guidelines for configuring in the EV cluster environment:
   - When configuring EV on the first node, select the option to create a new Enterprise Vault Server with cluster support.
   - Select the Enterprise Vault service group that you just created as the group in which to configure the resources for the Enterprise Vault services.
   - When prompted to enter the SQL Server that you want to use for the Enterprise Vault database, if SQL Server has been configured for high availability and disaster recovery, enter the name in the format *virtualservername**instancename*. For example, if the SQL virtual server name is virtualsvr and the instance name is EVSQL, enter virtualsvr\EVSQL
   - For the computer alias, use the virtual server name that was specified when creating the Enterprise Vault service group.
   - When you finish running the wizard on the first node, bring the Enterprise Vault resources online and verify that the Enterprise Vault service group is online.
3. To configure Enterprise Vault on any additional node, keep the service group online on the first node. Launch the Enterprise Vault Configuration

Wizard from the additional node. On the additional node, make sure that you select the option to add the node as a failover node for an existing clustered server.

Refer to the EV documentation for more information on the wizard.

Setting service group dependencies for high availability

Since Enterprise Vault requires the SQL database, if you cluster SQL Server using Veritas Cluster Server, Symantec recommends setting a service group dependency between the EV service group and the SQL service group.

For more information on setting service group dependencies, see the *Veritas Cluster Server Administrator's Guide*.

Verifying the Enterprise Vault cluster configuration

Failover simulation is an important part of configuration testing.

To verify the configuration of a cluster, either move the online groups, or shut down an active cluster node.

- Use Veritas Cluster Manager (Java Console) to switch all the service groups from one node to another.
- Simulate a local cluster failover by shutting down an active cluster node.

To switch service groups

1. In the Veritas Cluster Manager (Java Console), click the cluster in the configuration tree, click the Service Groups tab, and right-click the service group icon in the view panel.
   - Click **Switch To**, and click the appropriate node from the menu.
   - In the dialog box, click **Yes.** The service group you selected is taken offline on the original node and brought online on the node you selected.

     If there is more than one service group, you must repeat this step until all the service groups are switched.
2. Verify that the service group is online on the node you selected to switch to in step 1.
3. To move all the resources back to the original node, repeat step 1 for each of the service groups.

To shut down an active cluster node

1. Gracefully shut down or restart the cluster node where the service group is online.
2. In the Veritas Cluster Manager (Java Console) on another node, connect to the cluster.
3. Verify that the service group has failed over successfully, and is online on the next node in the system list.
4. If you need to move all the service groups back to the original node:
   - Restart the node you shut down in step 1.
   - Click **Switch To**, and click the appropriate node from the menu.
   - In the dialog box, click **Yes.**
     The service group you selected is taken offline and brought online on the node that you selected.

Setting up Enterprise Vault

Use the Enterprise Vault Administration Console to set up Enterprise Vault for archiving.

Perform the following tasks depending on your environment:

- Add the EV services to the cluster nodes.
- Create retention categories or edit predefined categories to suit your environment.
- Create a default vault store and partition.
- Review the default settings for the site.
- Implement other types of archiving (for example, Exchange, Outlook Web Access, SharePoint Server) as per your requirements.

Make sure to configure EV Server data files on shared storage. Data file include Indexing service data, Shopping service data, Vault store partitions, PsT holding folders and EMC Centera staging areas.

For more information on how to perform these tasks, see the Enterprise Vault documentation.

Considerations when modifying an EV service group

Table 6-1 lists the items that you can modify in the EV service group. For more information on modifying service groups, see the *Veritas Cluster Server Administrator's Guide*.

Table 6-1 Items that can be modified in an EV service group

Item	Notes
System list	You can add or remove nodes from the service group SystemList. If you want to remove a node, ensure that you do not run the wizard to modify the service group from that node.
Volumes	You can add or remove volumes. If you remove a volume on which an Enterprise Vault service is configured, the service ceases to be highly available and is not monitored.
Virtual IP	You can change the virtual IP address if the service group is offline. You cannot change the virtual server name, which is fixed when you create the service group.

Note the following:

- You must run the wizard from a node on which the service group is online. You can then use the wizard to add resources to or remove them from the configuration.
- You must take the service group partially offline to change the resource attributes. However, the MountV and VMDg resources for the service group should be online on the node where you run the wizard and offline on all other nodes. Mount all the volumes created to store Storage service data (vault stores), registry replication information, Shopping service data, Indexing data and MSMQ data.
- If you want to modify the system list or volumes, the service group must be online.

Note that if you add a system to an online service group, any resources with local attributes may briefly have a status of UNKNOWN. After you add the new node to the group, run the Enterprise Vault Configuration Wizard on this node to configure the Enterprise Vault services for it.

Chapter 7

Configuring disaster recovery for Enterprise Vault

This chapter contains the following topics:

Tasks for configuring disaster recovery for Enterprise Vault

After setting up an SFW HA high availability environment for Enterprise Vault on a primary site, you can create a secondary or "failover" site for disaster recovery.

For Enterprise Vault, the Disaster Recovery (DR) wizard helps you to clone the storage from the primary site to the secondary site. The DR wizard also helps you set up replication and the global cluster (GCO option).

The DR wizard is available from the Solutions Configuration Center. Symantec recommends using the Solutions Configuration Center as a guide for installing and configuring disaster recovery.

See "About the Solutions Configuration Center" on page 35.

Note: Symantec recommends as a best practice to configure SQL Server for disaster recovery before configuring Enterprise Vault for disaster recovery. Configuring SQL Server for disaster recovery is covered in the SQL Server solutions guides. See "Where to get more information" on page 18.

Table 7-1 Configuring the secondary site for disaster recovery

Action	Description
Verify that Enterprise Vault has been configured for high availability at the primary site	Verify that Enterprise Vault has been configured for high availability at the primary site See "Verifying your primary site configuration" on page 121.
Install SFW HA and configure the cluster on the secondary site	For implementing disaster recovery, the following options must be installed on both primary and secondary sites: ■ SFW VVR option ■ VCS GCO option **Caution:** Ensure that the name you assign to the secondary site cluster is different from the name assigned to the primary site cluster. See "Guidelines for installing SFW HA and configuring the cluster on the secondary site" on page 122.
Set up security for VVR	Set up security for VVR See "Setting up security for VVR" on page 122.

Table 7-1 Configuring the secondary site for disaster recovery (Continued)

Action	Description
(Secure cluster only) Assign user privileges	For a secure cluster only, assign user privileges See "Assigning user privileges (secure clusters only)" on page 126.
Start the DR wizard to begin disaster recovery configuration	■ Review prerequisites for the DR wizard ■ Start the DR wizard and make the initial selections: selecting a primary site system, the service group, the secondary site system, and the replication method See "Configuring disaster recovery with the DR wizard" on page 127.
Clone the storage configuration	Clone the storage configuration on the secondary site using the DR wizard See "Cloning the storage on the secondary site using the DR wizard" on page 130.
Install Enterprise Vault on the cluster nodes	See "Installing and configuring Enterprise Vault on the secondary site" on page 133
Create the EV service group configuration on the secondary site	The EV service group must be offline on the primary site before you configure the EV service group on the secondary site. You must use the same service group name and virtual server name as on the primary site. See "Installing and configuring Enterprise Vault on the secondary site" on page 133.
Configure the Enterprise Vault server in a cluster environment	See "Installing and configuring Enterprise Vault on the secondary site" on page 133.
Configure VVR replication and global clustering	Use the DR wizard to configure replication and global clustering See "Configuring VVR replication and global clustering" on page 136.
Verify the disaster recovery configuration	Verify that the secondary site has been fully configured for disaster recovery See "Verifying the disaster recovery configuration" on page 144.

Table 7-1 Configuring the secondary site for disaster recovery (Continued)

Action	Description
(Optional) Add secure communication	Add secure communication between local clusters within the global cluster (optional task) See "Establishing secure communication within the global cluster (optional)" on page 145.
(Optional) Add additional DR sites	Optionally, add additional DR sites to a VVR environment See "Adding multiple DR sites (optional)" on page 147.
Handling service group dependencies after failover	If your environment includes dependent service groups, review the considerations for bringing the service groups online after failover to the secondary site See "Recovery procedures for service group dependencies" on page 148.

Verifying your primary site configuration

Before you begin configuring disaster recovery, make sure that Enterprise Vault has been configured for high availability at the primary site.

If you have not yet configured Enterprise Vault for high availability at the primary site, go to High Availability (HA) Configuration in the Solutions Configuration Center and follow the steps in the order shown.

To verify the configuration, use the Cluster Manager (Java console) on the primary site and check the status of the service group in the tree view. Verify that all the resources are online and that the service group is online.

Guidelines for installing SFW HA and configuring the cluster on the secondary site

Use the following guidelines for installing SFW HA and configuring the cluster on the secondary site.

Note: Symantec recommends as a best practice to configure SQL Server for disaster recovery before configuring Enterprise Vault for disaster recovery. If you have completed SQL Server DR configuration, the following steps may already be complete.

- Ensure that you have set up the components required to run a cluster.
  See "Configuring the storage hardware and network" on page 62.
- Ensure that when installing SFW HA you install the appropriate disaster recovery options at both the primary and secondary sites, as follows:

Global Cluster Option	This VCS option is required for a disaster recovery configuration.
Veritas Volume Replicator	This SFW option is required for VVR replication.

  For more information see the *SFW HA Installation and Upgrade Guide*.
- Configure the cluster with the VCS Cluster Configuration Wizard (VCW). Ensure that the name you assign to the secondary site cluster is different from the name assigned to the primary site cluster.
  See "Configuring the cluster" on page 85.

  Note: You do not need to configure the GCO option while configuring the cluster. This is done later using the Disaster Recovery wizard.

Setting up security for VVR

If you are using Veritas Volume Replicator (VVR) replication, you must configure the VxSAS service on all cluster nodes. For a disaster recovery environment, you configure the service on all nodes on both the primary and secondary sites.

Note: Symantec recommends as a best practice to configure SQL Server for disaster recovery before configuring Enterprise Vault for disaster recovery. If you have completed SQL Server DR configuration, the following procedure may already be complete.

Complete the following procedure to configure the VxSAS service for VVR.

The procedure has these prerequisites:

- You must be logged on with administrative privileges on the server for the wizard to be launched.
- The account you specify must have administrative and log-on as service privileges on all the specified hosts.
- Avoid specifying blank passwords. In a Windows Server environment, accounts with blank passwords are not supported for log-on service privileges.
- Make sure that the hosts on which you want to configure the VxSAS service are accessible from the local host.

Note: For details on this required service, see *Veritas Storage Foundation Veritas Volume Replicator Administrator's Guide*.

To configure the VxSAS service

1. Launch the VVR Security Service Configuration Wizard.
   Click **Start** > **All Programs > Symantec > Veritas Storage Foundation > Configuration Wizards > VVR Security Service Configuration Wizard**.
   or
   Type `vxsascfg.exe` at the command prompt.
2. Read the information provided on the Welcome page and click **Next**.
3. Complete the Account Information panel as follows and then click **Next**:

Account name (domain\account)	Enter the administrative account name.
Password	Specify a password.

   If you have already configured the VxSAS service for one host that is intended to be a part of the RDS, make sure you specify the same username and password when configuring the VxSAS service on the other hosts.

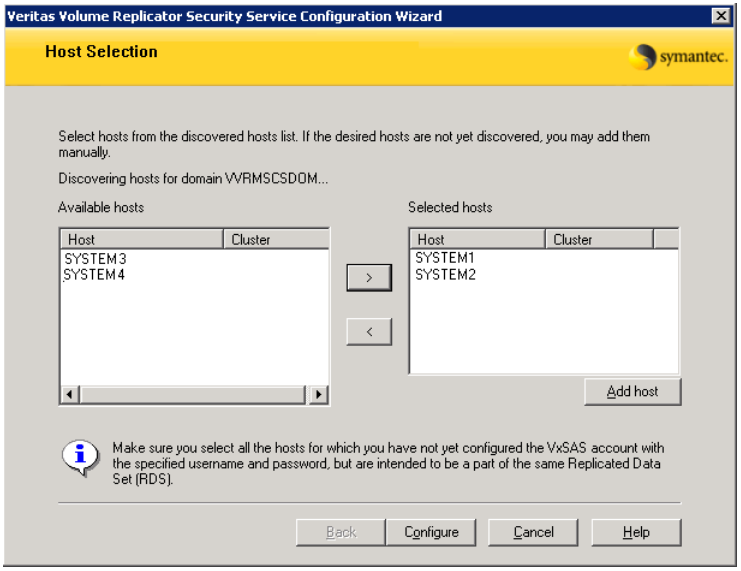
4 On the Domain Selection panel, select the domain to which the hosts that you want to configure belong and then click **Next**:

Selecting domains — The Available domains pane lists all the domains that are present in the Windows network neighborhood.

Move the appropriate name from the Available domains list to the Selected domains list, either by double-clicking it or using the arrow button.

Adding a domain — If the domain name that you require is not displayed, click **Add domain**. This displays a dialog that allows you to specify the domain name. Click **Add** to add the name to the Selected domains list.

5 On the Host Selection panel, select the required hosts:



Selecting hosts — The Available hosts pane lists the hosts that are present in the specified domain.

Move the appropriate host from the Available hosts list to the Selected hosts list, either by double-clicking it or using the arrow button. Use the Shift key with the up or down arrow keys to select multiple hosts.

Adding a host	If the host name you require is not displayed, click **Add host**. In the Add Host dialog specify the required host name or IP in the **Host Name** field. Click **Add** to add the name to the Selected hosts list.

After you have selected a host name, the **Configure** button is enabled. Click **Configure** to proceed with configuring the VxSAS service.

6 After the configuration completes, the Configuration Results page displays whether or not the operation was successful. If the operation was not successful, the page displays the details on why the account update failed, along with the possible reasons for failure and recommendations on getting over the failure.

When configuring the VxSAS service for VVR in a firewall setup, the VxSAS wizard may not be able to configure the machines that are across the firewall, although the Host Selection dialog may list these nodes. In this case, configure the VxSAS service locally on the machines that are across the firewall.

Click **Back** to change any information you had provided earlier.

7 Click **Finish** to exit the wizard.

Assigning user privileges (secure clusters only)

In order to enable remote cluster operations you must configure a VCS user with the same name and privileges in each cluster.

When assigning privileges in secure clusters, you must specify fully-qualified user names, in the format username@domain. You cannot assign or change passwords for users when VCS is running in secure mode.

You must assign service group rights to the Enterprise Vault service group.

See the *Veritas Cluster Server Administrator's Guide*.

To assign user privileges at the primary site

1. Set the configuration to read/write mode:
   ```
   haconf -makerw
   ```
2. Add the user. Specify the name in the format username@domain.
   ```
   hauser -add user [-priv <Administrator|Operator>]
   ```
3. Modify the attribute of the service group to add the user. Specify the application service group.
   ```
   hauser -add user [-priv <Administrator|Operator> [-group
          service_groups]]
   ```
4. Reset the configuration to read-only:
   ```
   haconf -dump -makero
   ```

To assign user privileges at the secondary site

1. Set the configuration to read/write mode:
   ```
   haconf -makerw
   ```
2. Add the user. Specify the name in the format username@domain.
   ```
   hauser -add user [-priv <Administrator|Operator>]
   ```
3. Reset the configuration to read-only:
   ```
   haconf -dump -makero
   ```

Configuring disaster recovery with the DR wizard

In an Enterprise Vault environment, the Disaster Recovery Configuration Wizard (DR wizard) assists you to perform the following tasks for the selected service group:

- Clone the storage configuration
- Configure VVR replication and global clustering

You will need to exit the wizard after the storage cloning task to install the application, configure the Enterprise Vault service group, and configure Enterprise Vault for the cluster environment. Then you start the wizard again.

The DR Wizard list of service groups shows only those that contain a MountV resource.

Warning: Once you have completed configuring replication and global clustering with the DR wizard, you cannot use the wizard to change the method of replication.

Before running the DR wizard to configure disaster recovery, ensure that you meet the following prerequisites:

- SFW HA is installed and a cluster is configured at the secondary site. Ensure that the name assigned to the secondary site cluster is different than the name assigned to the primary site cluster.
- Enterprise Vault is configured for HA at the primary site and the EV service group is online on the primary site.
- Enough free disk space is available at the secondary site to duplicate the storage configuration at the primary site.
- For an IPv4 network, one static IP address is available per application service group to be created.
- For an IPv4 network, a minimum of one static IP address per site is available for each application instance running in the cluster.
- Global Cluster Option (GCO) is installed at the primary and secondary site, and, for an IPv4 network, one static IP address is available at each site for configuring GCO.
- The service group to be cloned can use either IPv4 IP addresses or IPv6 addresses but not a mixture of both.
- A VCS user is configured with the same name and privileges in each cluster.

- If a firewall exists between the wizard and any systems it needs access to, the firewall is set to allow both ingoing and outgoing TCP requests on port 7419.

Note: The DR wizard does not support VVR configurations that include a Bunker secondary site.

In addition, see the following replication prerequisite:

- "Setting up security for VVR" on page 122

To start configuring disaster recovery with the DR wizard

1. Start the DR Configuration Wizard from the Solutions Configuration Center. Click **Start** > **All Programs** > **Symantec** > **Veritas Cluster Server** > **Solutions Configuration Center**. Expand the Solutions for Enterprise Vault tab and click **Disaster Recovery Configuration > Clone the storage on the secondary site**> **Disaster Recovery Configuration Wizard**.

   Note: By design, the DR wizard requires specific settings for the Lanman attributes on the primary and secondary sites. Before beginning the DR configuration, the wizard checks for these values, and if they are not set as required, the wizard will automatically proceed with setting these values, both at the primary and secondary sites.

   ---

2. In the Welcome panel, review the prerequisites to ensure that they are met and click **Next**.
3. In the System Selection panel, complete the requested information:

System Name	Enter the IP address or Fully Qualified Host Name (FQHN) of the primary system where the application is online. If you have launched the wizard on the system where the application is online at the primary site, you can also specify `localhost` to connect to the system.

   Click **Next**.
4. In the Service Group Selection panel, select the Enterprise Vault service group for which you want to configure the storage and replication.

   The panel lists only service groups that contain a MountV resource. The service group must not have a child service group, since the DR wizard does not support such a configuration for VVR replication.
   Click **Next**.

5 In the Secondary System Selection panel, enter the Fully Qualified Host Name (FQHN) or the IP address of the secondary system for which you want to configure disaster recovery.
Click **Next**.

6 In the Replication Options panel, select the replication method. Although you must select the replication method now, configuring replication and the global cluster option is done later, after service group creation. For Enterprise Vault, select the option to configure VVR and the Global Cluster option (GCO).

Configure Veritas Volume Replicator (VVR) and the Global Cluster Option (GCO)	Select this option if you want to configure VVR replication. Select this option even if you plan to configure VVR replication or the GCO option manually. This option is required for the wizard to configure the storage cloning correctly for a VVR environment. The wizard verifies each configuration task and recognizes if a task has been completed successfully. You cannot mix replication methods. That is, if your primary site is using array-based replication, and you select the VVR option, the wizard will warn you that you cannot use VVR replication for the disaster recovery site.
Configure EMC SRDF and the Global Cluster Option (GCO)	Select this replication option if you want to configure the settings for the VCS EMC SRDF agent. All disks used for the service group on the primary site must belong to an EMC SRDF array. Select this option even if you plan to configure EMC SRDF replication or the GCO option manually. The wizard verifies each configuration task and recognizes if a task has been completed successfully.
Configure Hitachi TrueCopy and the Global Cluster Option (GCO)	Select this replication option if you want to configure the settings for the VCS Hitachi TrueCopy agent. All disks used for the service group on the primary site must belong to a Hitachi TrueCopy array. Select this option even if you configure GCO manually. The wizard verifies each configuration task and recognizes if a task has been completed successfully.

Configure the Global Cluster Option (GCO) only	If you select this option, the DR wizard does not configure any replication settings. It configures the global cluster option. Select this option if you want to use the wizard in an array-based replication environment that is not supported by this wizard. You must configure replication manually after you finish the wizard. If you select the GCO only option, the DR wizard sets up the storage and service group configuration on the secondary site for an array-based hardware replication environment. Therefore, you cannot use this option to clone the storage and service group for a VVR replication environment.

Click **Next**.

7 Continue with cloning the storage.

See "Cloning the storage on the secondary site using the DR wizard" on page 130.

Cloning the storage on the secondary site using the DR wizard

The DR wizard enables you to clone the storage configuration present at the primary site on to the secondary site. To do this successfully, the systems at the secondary site must have adequate free storage. If you have created the configuration but there is a mismatch in the volume sizes, the wizard can correct this and then complete the configuration.

If you have not yet started the wizard, see the following topic for the wizard prerequisites before continuing with the storage cloning procedure:

- "Configuring disaster recovery with the DR wizard" on page 127.

To clone the storage configuration from the primary site to the secondary site (VVR replication method)

1 If you have not yet done so, start the Disaster Recovery Configuration Wizard and specify the information for the primary site system, the service group, and the secondary site system. In the Replication Options panel, select the VVR replication method and click **Next**.

2 Review the information in the Storage Validation Results panel. This panel compares the configuration at the secondary site with that on the primary. If the storage is already configured identically on both sites, the panel

shows that results are identical. Otherwise, the panel shows the differences and recommended actions. You can toggle between a summary and detailed view of information about the differences.
The detailed view shows the following:

Disk Group	Displays the disk group name that needs to be created on the secondary site.
Volume	Displays the list of volumes, if necessary, that need to be created at the secondary site.
Size	Displays the size of the volume that needs to be created on the secondary site.
Mount	Displays the mount to be assigned the volume on the secondary site.
Recommended Action	Indicates the action that needs to be taken at the secondary to make the configuration similar to that on the primary. ■ If the volume does not exist, a new volume will be created. ■ If the volume exists but is of a smaller size than that on the primary, the volume will be expanded to the required size. ■ If the volume is of a greater size than that on the primary, the volume will be recreated using the appropriate size. ■ If the volume is the same as that on the primary, the message indicates that the volumes are identical and no action is required.

The summary view shows the following:

Disk groups that do not exist	Displays the names of any disk groups that exist on the primary but do not exist on the secondary.
Existing disk groups that need modification	Displays the names of any disk groups on the secondary that need to be modified to match the primary.
Free disks present on secondary	Displays the list of free disks that exist on the secondary along with details about the free space and total disk space information.

If the panel displays a message indicating that the available disks are inadequate to clone the primary site configuration on the secondary, you can free some disks on the secondary or add more storage. Then click **Refresh/Validate** to have the wizard update its information about the secondary storage configuration.

You continue with the wizard to provide information for the recommended actions. Before proceeding to the service group configuration, the wizard ensures that the configuration of the disk groups and volumes for the service group is the same at the primary and secondary site.
Click **Next**.

3 In the Disk Selection for Storage Cloning panel, for each of the disk groups that does not exist or is not same as the corresponding disk group at the primary site, select disks that the wizard can use to create the respective disk groups at the secondary site.

Selecting Disks	For each of the disk groups that needs to be created, select the required disks from the Available Disks pane. Either double-click on the host name or the **>>** option to move the hosts into the Selected disks pane. Under the Available Disks label, a drop-down list allows you to filter available disks by disk enclosure name. The default is All, which displays all free disks available on all enclosures.

Click **Next**.

4 In the Volume Layout for Secondary Site Storage panel, complete the requested information:

Disk Group	Displays the disk group name to which the volume belongs.
Volume (Volume Size)	Displays the name and the size of the volume, corresponding to that on the primary, that needs to be created on the secondary.
Available Disks	Select the disks on which you want the wizard to create the volumes. From the Available Disks pane, either double-click on the disk name or the **>>** option to move the disks into the Selected Disks pane. For each disk group the Available disks pane displays the list of disks that are part of the disk group. Select disks for each unavailable volume that you want to clone on to the secondary.
Layout	By default, the same layout as the one specified for the primary volume is selected. Click **Edit** to change the layout to suit your specific requirements.
Selected Disks	Displays the list of disks that have been moved in from the Available Disks pane.

View Primary Layout	Displays the volume layout at the primary site. Use this information as a reference to specify the details for the Secondary layout.

Click **Next**.

5 In the Storage Configuration Cloning Summary panel, review the displayed information. If you want to change any selection, click **Back**. Otherwise, click **Next** to allow the wizard to implement the storage configuration at the secondary site.

6 In the Implementation panel, wait until the status for all the completed tasks is marked with a check symbol, indicating successful completion. Wait until the wizard completes cloning the storage. The progress bar indicates the status of the tasks. If some task could not be completed successfully, then the task is marked with an (**x**) symbol. The Information column displays details about the reasons for task failure. Click **Next**.

7 In the Storage Cloning Configuration Result screen, view the results and click **Next**.

8 .When the Application Installation panel is displayed, click **Finish** to exit the wizard.

9 You must complete the following tasks for installing and configuring Enterprise Vault on the secondary site before you restart the Disaster Recovery Wizard:

- Install Enterprise Vault on the secondary site nodes
- Run the Enterprise Vault Cluster Setup Wizard on the first node on the secondary site to configure the Enterprise Vault service group
- Run the Enterprise Vault Configuration Wizard on each node on the secondary site to configure Enterprise Vault for the cluster environment

See "Installing and configuring Enterprise Vault on the secondary site" on page 133.

Installing and configuring Enterprise Vault on the secondary site

Perform the following steps when installing and configuring Enterprise Vault for the cluster on the secondary site.

Be sure to read these instructions before running the Enterprise Vault Cluster Setup wizard and the Enterprise Vault Configuration Wizard on the secondary site.

To install and configure Enterprise Vault on the secondary site:

1. Install Enterprise Vault on each node of the secondary site cluster.
   For installation and configuration instructions, see the Enterprise Vault documentation.
2. Before you launch the wizard to configure the EV service group, storage cloning must be complete. Verify that the cluster disk group is imported to the first node on the secondary site and the volumes are mounted. If volumes were mounted as drive paths (folder mount) on the primary site, the DR Wizard does not mount the volumes on the secondary site and you must format the volumes and mount them manually.
   See "About managing disk groups and volumes" on page 82.
3. Bring the EV service group offline on the primary site.
4. On the first node, launch the Enterprise Vault Cluster Setup Wizard to configure the EV service group.
   Click **Start** > **All Programs** > **Symantec** > **Veritas Cluster Server** > **Solutions Configuration Center**. Expand the Solutions for Enterprise Vault tab and click **Disaster Recovery Configuration > Configure the Enterprise Vault service group on the secondary site > Enterprise Vault Cluster Setup Wizard.**
   Specify the same service group name and virtual server name on the secondary site as on the primary site.
   For example, if the service group name on the primary site is EV_SG, use EV_SG for the service group name on the secondary site. If the virtual server name on the primary site is EV-VS, use EV-VS for the virtual server name on the secondary site.
   Specify the same MSMQ and Replication Directory paths on the secondary site as on the primary site.
   Use the same procedure as when configuring the service group on the primary site. Be sure to choose the wizard option to bring the service group online after creating it.
   See "Configuring the Enterprise Vault service group" on page 106.
5. Use the Enterprise Vault Configuration Wizard to configure Enterprise Vault on each node on the secondary site, beginning with the node on which the service group is online (the first node).
   To launch the wizard, click **Start** > **All Programs** > **Symantec** > **Veritas Cluster Server** > **Solutions Configuration Center**. Expand the Solutions for Enterprise Vault tab and click **Disaster Recovery Configuration > Configure**

Enterprise Vault Server in a cluster environment > Enterprise Vault Configuration Wizard.

Follow these guidelines on the first node on the secondary site:

- On the first node, select the option to create a new Enterprise Vault Server with cluster support, rather than the option to add the node as a failover node for an existing clustered server.
- Select the Enterprise Vault service group that you just created as the group in which to configure the resources for the Enterprise Vault services.
- When prompted to enter the SQL Server that you want to use for the Enterprise Vault database, specify the same database that you selected on the primary site. If SQL Server has been configured for high availability and disaster recovery, enter the name in the format *virtualservername**instancename*. For example, if the SQL virtual server name is virtualsvr and the instance name is EVSQL, enter virtualsvr\EVSQL.

  The wizard detects the existing database and updates it.
- When you finish running the wizard, bring the Enterprise Vault resources online and verify that the Enterprise Vault service group is online. The EV resources will be in an unknown state on the failover node because the Enterprise Vault Configuration Wizard has not yet been run on that node.

For additional information on the wizard, see the Enterprise Vault documentation.

6 To configure Enterprise Vault on any additional node, keep the service group online on the first node. Launch the Enterprise Vault Configuration Wizard from the additional node. On the additional node, make sure that you select the option to add the node as a failover node for an existing clustered server.

7 Once configuration is complete, verify the configuration on the secondary site by switching the service group from the first node to the failover node on the secondary site.

8 Take the service group offline on the secondary site and bring it online on the primary site.

Configuring VVR replication and global clustering

You use the DR wizard to configure VVR replication and global clustering.

Before you begin, ensure that you have met the following prerequisites:

- Ensure that Veritas Volume Replicator is installed at the primary and secondary site.
- Ensure that Global Cluster Option (GCO) is installed at the primary and secondary site. One static IP address must be available per site for configuring GCO.
- Ensure that a minimum of one static IP address per site is available for each application instance running in the cluster.
- Ensure that you set the IP preference, whether VVR should use IPv4 or IPv6 addresses, before configuring replication. The default is IPv4.
  When you specify host names while configuring replication, VVR resolves the host names with the IP addresses associated with them. This setting determines which IP protocol VVR uses to resolve the host names.
  Use Veritas Enterprise Administrator (VEA) (Control Panel > VVR Configuration > IP Settings tab) to set the IP preference.
- Ensure that you configure a VCS user with the same name and privileges in each cluster.
- Ensure that VVR Security Service (VxSAS) is configured at the primary and secondary site.
  See "Setting up security for VVR" on page 122.
- Ensure that the storage has been cloned on the secondary site.
  See "Cloning the storage on the secondary site using the DR wizard" on page 130.
- Ensure that Enterprise Vault is installed and configured on the secondary site.
  See "Installing and configuring Enterprise Vault on the secondary site" on page 133.
- Bring the EV service group offline at the secondary site and online at the primary site.

Use the following procedure to configure VVR replication and global clustering with the DR wizard.

To configure VVR replication and GCO

1 Verify that the application server service group is online at the primary site and the appropriate disk groups are imported at the secondary site.

2 Launch the wizard and proceed to the Replication Setup panel as follows:

- Start the DR Configuration Wizard from the Solutions Configuration Center. Click **Start** > **All Programs** > **Symantec** > **Veritas Cluster Server** > **Solutions Configuration Center**.

  Expand the Solutions for Enterprise Vault tab and click **Disaster Recovery Configuration > Configure replication and the global cluster option (GCO)** > **Disaster Recovery Configuration Wizard**.
- On the Welcome panel, click **Next** and continue through the wizard, providing the requested information.
- On the Replication Methods panel, click **Configure VVR and the Global Cluster Option (GCO)**. Click **Next**.

  The wizard proceeds to the storage cloning panel. If it detects that the storage is identical on the secondary site, it proceeds to the next task. If it detects that the service group is created on the secondary site, it proceeds to the Internet Protocol panel.

3 In the Internet Protocol panel, select IPv4 or IPv6 depending on which type of network you are using. (You must use the same on primary and secondary sites.) Click **Next**.

4 In the Replication Setup panel, review the replication requirements. If you have met the requirements, click **Next**. If not, click **Cancel** and restart the wizard after meeting the requirements.

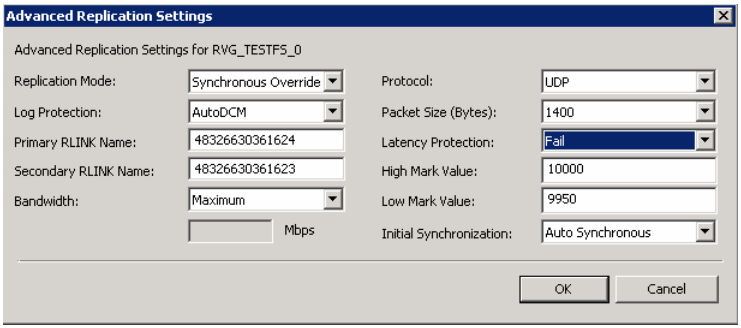
5 In the Replication Settings for Replicated Volume Group panel, specify the requested information. If you are adding a DR site to an existing DR configuration, fields that must match the existing settings, such as the RVG or RDS name, are dimmed so that you cannot change them.

Disk Group	The left column lists the disk groups. By design, an RVG is created for each disk group.
RVG Name	Displays the default RVG name. If required, change this to a name of your choice.
RDS Name	Displays the default Replicated Data Set (RDS) name. If required, change this to a name of your choice.
Available Volumes	Displays the list of available volumes that have not been selected to be a part of the RVG. Either double-click on the volume name or use the > option to move the volumes into the Selected RVG Volumes pane.

Selected RVG Volumes	Displays the list of volumes that have been selected to be a part of the RVG. To remove a selected volume, either double-click the volume name or use the < option to move the volumes into the Available Volumes pane.
Primary SRL	If you did not create a Replicator Log volume on the primary site, click **Create New** on the drop-down menu. On the New Volume dialog box, specify the name, size, and disk. Otherwise, select the appropriate primary Replicator Log volume from the drop-down menu and enter an appropriate size.
Secondary SRL	If you did not create a Replicator Log volume on the primary site, click **Create New** on the drop-down menu. On the New Volume dialog box, specify the same name and size as you specified for the primary SRL. Otherwise, select the appropriate secondary Replicator Log volume from the drop-down menu and enter an appropriate size.
Start Replication after the wizard completes	Select this check box to start replication automatically after the wizard completes the necessary configurations. Once replication is configured and running, deselecting the checkbox does not stop replication.

- Click **Advanced Settings** to specify some additional replication properties. The options on the dialog box are described column-wise, from left to right; refer to the *Veritas Volume Replicator*

Administrator's Guide for additional information on VVR replication options.



Replication Mode

Select the required mode of replication; **Synchronous**, **Asynchronous**, or **Synchronous Override**. The default is synchronous override.

Log Protection

Select the appropriate log protection from the list.

The **AutoDCM** is the default selected mode for the Replicator Log overflow protection when all the volumes in the Primary RVG have a DCM log. The DCM is enabled when the Replicator Log overflows.

The **Off** option disables Replicator Log Overflow protection.

The **Override** option enables log protection. If the Secondary node is still connected and the Replicator Log is about to overflow then the writes are stalled until a predetermined amount of space, that is, 5% or 20 MB (whichever is lesser) becomes available in the Replicator Log.

If the Secondary becomes inactive due to disconnection or administrative action then Replicator log protection is disabled, and the Replicator Log overflows.

The **Fail** option enables log protection. If the log is about to overflow the writes are stalled until a predetermined amount of space, that is, 5% or 20 MB (whichever is lesser) becomes available in the Replicator Log. If the connection between primary and secondary RVG is broken, then, any new writes to the primary RVG are failed.

Primary RLINK Name	Enter a name of your choice for the primary RLINK. If you do not specify any name then the wizard assigns a default name.
Secondary RLINK Name	Enter a name of your choice for the Secondary RLINK. If you do not specify any name then the wizard assigns a default name.
Bandwidth	By default, VVR replication uses the maximum available bandwidth. You can select **Specify** to specify a bandwidth limit. The default unit is Mega bits per second (Mbps) and the minimum allowed value is 1 Mbps.
Protocol	Choose TCP or UDP. UDP/IP is the default replication protocol.
Packet Size (Bytes)	Default is 1400 Bytes. From the drop-down list, choose the required packet size for data transfer. The default unit for the packet size is Bytes. You can set the packet size only if the protocol is UDP/IP.
Latency Protection	By default, latency protection is set to **Off**. When this option is selected the **High Mark Value** and the **Low Mark Value** are disabled. Select the **Fail** or **Override** option to enable Latency protection. This **Override** option behaves like the **Off** option when the Secondary is disconnected and behaves like the **Fail** option when the Secondary is connected.
High Mark Value	This option is enabled only when Latency Protection is set to **Override** or **Fail**. It specifies the maximum number of pending updates by which the secondary site can be behind the primary site. The default value is 10000. To ensure that latency protection is most effective the difference between the high and low mark values must not be very large.
Low Mark Value	This option is enabled only when Latency Protection is set to **Override** or **Fail**. When the updates in the Replicator log reach the **High Mark Value,** then the writes to the system at the primary site continues to be stalled until the number of pending updates on the Replicator log falls back to the **Low Mark Value**. The default is 9950.

Initial Synchronization	If you are doing an initial setup, then use the **Auto Synchronous** option to synchronize the secondary site and start replication. This is the default. When this option is selected, VVR by default performs intelligent synchronization to replicate only those blocks on a volume that are being used by the file system. If required, you can disable intelligent synchronization. If you want to use the **Synchronize from Checkpoint** method then you must first create a checkpoint. If you have a considerable amount of data on the primary data volumes then you may first want to synchronize the secondary for existing data using the backup-restore method with checkpoint. After the restore is complete, use the **Synchronize from Checkpoint** option to start replication from the checkpoint to synchronize the secondary with the writes that happened when backup-restore was in progress.

To apply changes to advanced settings, click **OK.** On the Replication Settings for Replicated Volume Group panel click **Next**.

6 In the Replication Attribute Settings panel, specify required replication attribute information for the cluster at the primary and secondary site. Click the arrow icon to expand an RVG row and display the replication attribute fields. If you are configuring an additional secondary site (multiple DR sites), some fields are disabled.

Disk Group	Displays the list of disk groups that have been configured.
RVG Name	Displays the Replicated Volume Groups corresponding to the disk groups.
IP Address	For IPv4 networks, enter replication IPs that will be used for replication, one for the primary site and another for the secondary site. For IPv6, select the network from the dropdown list. An IP address will be generated.
Subnet Mask or Prefix	For IPv4, enter the subnet mask for the system at the primary site and the secondary site. For IPv6, enter the prefix.

Public NIC	Select the public NIC from the drop-down list for the system at the primary and secondary site. For IPv6, available NICs are those belonging to the selected network.
Copy	Enables you to copy the above network settings to any additional RVGs that are listed on this screen. If there is only one RVG, this option does not apply.

After specifying the replication attributes for each of the RVGs, click **Next**.

7 In the Global Cluster Settings panel specify the heartbeat information for the wide-area connector resource. You must specify this information for the primary and the secondary cluster. Any existing WAC resource information can be reused. If you are adding a DR site to an existing DR configuration, GCO is already configured at the primary site, so the primary site fields are dimmed.

Use existing settings	Allows you to use a WAC resource that already exists at either the primary or secondary site. Click Primary or Secondary, depending on the site at which the WAC resource already exists.
Resource Name	Select the existing WAC resource name from the resource name list box.
Create new settings	Select the appropriate site, primary or secondary, for which you want to create a new WAC resource.
IP Address	For IPv4, enter a virtual IP for the WAC resource. For IPv6, select the network from the dropdown list. An IP address will be generated.
Subnet Mask or Prefix	For IPv4, enter the subnet mask for the system at the primary site and the secondary site. For IPv6, enter the prefix.
Public NIC	Select the public NIC for each system from the drop-down list for the system at the primary and secondary site.

Start GCO after configuration	Select this check box to bring the cluster service group online and start GCO automatically after the wizard completes the necessary configurations. Otherwise, you must bring the service group online and start GCO manually, after the wizard completes. Once GCO is configured and running, deselecting the checkbox does not stop GCO.

8 In the Settings Summary panel, review the displayed information. Click **Back** if you want to change any of the parameters. If you have a printer installed, you can click the printer icon at the bottom of the scrollable list to print the settings.
Click **Next** to implement the settings.

9 In the Implementation panel, wait till the wizard completes creating the replication configuration and the WAC resource required for global clustering. If a task could not be completed successfully, it is marked with an (**x**) symbol. For any critical errors, the wizard displays an error message. For less critical errors, the Information column displays a brief description about the task failure and the next screen displays additional information on what action you can take to remedy it. Click **Next**.

10 In the Finish panel, review the displayed information. If a task did not complete successfully, the panel displays an error message, which will provide some insight into the cause for failure. Click **Finish** to exit the wizard.

Setting service group dependencies for disaster recovery

Since Enterprise Vault requires the SQL database, if you cluster SQL Server using Veritas Cluster Server, Symantec recommends setting a service group dependency between the EV service group and the SQL service group.

In the disaster recovery environment with VVR replication, the EV Replicated Volume Group (RVG) should be linked as a parent to the SQL Server service group as a child. Set the same service group dependencies on the primary and secondary site clusters.

For the VVR environment, the DR wizard can configure DR only for a service group that has no child. Therefore, set service group dependencies only after running the DR wizard.

For more information on setting service group dependencies, see the *Veritas Cluster Server Administrator's Guide*.

Verifying the disaster recovery configuration

After the DR wizard has completed, you can confirm the following to verify the DR configuration:

- Confirm that the configuration of disk groups and volumes at the DR site have been created by the DR wizard storage cloning.
- Confirm that the application VCS service group has been created in the DR cluster including the same service group name, same resources, and same dependency structure as the primary site's application VCS service group.
- Confirm that the application service group is online at the primary site. The application service group should remain offline at the DR site.
- Ensure VVR replication configuration. This includes ensuring that the RVGs have been created at primary and secondary with the correct volume inclusion, replication mode, Replicator Log configuration, and any specified advanced options.
- Confirm that the replication state matches what was specified during configuration. If specified to start immediately, ensure that it is started. If specified to start later, ensure that it is stopped.
- Ensure that the VVR RVG VCS service group is configured on the primary and secondary clusters, including the correct dependency to the application service group, the specified IP for replication, and the correct disk group and RVG objects within the RVG VCS service group.
  See also “Setting service group dependencies for disaster recovery” on page 143.
- Confirm that the RVG service groups are online at the primary and secondary sites.
- Confirm that the RVG Primary resources are online in the primary cluster's application service group. If they are offline, then bring them online in the primary site's cluster's application service group. Do not bring them online in the secondary site application service group.
- Ensure that the application service groups are configured as global.
- Check to ensure that the two clusters are communicating and that the status of communication between the two clusters has a state of Alive.
- If you are configuring an additional DR site, verify the heartbeat and replication configuration between all sites.
- If you chose to start replication manually in the DR wizard, to avoid replicating large amounts of data over the network the first time, then you

will need to start the process necessary to synchronize from checkpoint. This typically consists of

- starting a VVR replication checkpoint
- performing a block level backup
- ending the VVR replication checkpoint
- restoring the block level backup at the DR site
- starting replication from the VVR replication checkpoint

To learn more about the process of starting replication from a checkpoint, refer to the *Veritas Volume Replicator Administrator's Guide.*

- Do not attempt a wide area failover until data has been replicated and the state is consistent and up to date.

Establishing secure communication within the global cluster (optional)

A global cluster is created in non-secure mode by default. You may continue to allow the global cluster to run in non-secure mode or choose to establish secure communication between clusters.

The following prerequisites are required for establishing secure communication within a global cluster:

- The clusters within the global cluster must be running in secure mode.
- You must have Administrator privileges for the domain.

The following information is required for adding secure communication to a global cluster:

- The active host name or IP address of each cluster in the global configuration.
- The user name and password of the administrator for each cluster in the configuration.
- If the local clusters do not point to the same root broker, the host name and port address of each root broker.

Adding secure communication involves the following tasks:

- Taking the ClusterService-Proc (wac) resource in the ClusterService group offline on the clusters in the global environment.
- Adding the -secure option to the StartProgram attribute on each node.
- Establishing trust between root brokers if the local clusters do not point to the same root broker.

- Bringing the ClusterService-Proc (wac) resource online on the clusters in the global cluster.

To take the ClusterService-Proc (wac) resource offline on all clusters

1. From Cluster Monitor, log on to a cluster in the global cluster.
2. In the **Service Groups** tab of the Cluster Explorer configuration tree, expand the **ClusterService** group and the Process agent.
3. Right-click the **ClusterService-Proc** resource, click **Offline**, and click the appropriate system from the menu.
4. Repeat step 1 to step 3 for the additional clusters in the global cluster.

To add the -secure option to the StartProgram resource

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the **ClusterService-Proc** resource under the **Process** type in the **ClusterService** group.
2. Click **View**, and then **Properties** view.
3. Click the Edit icon to edit the **StartProgram** attribute.
4. In the Edit Attribute dialog box, add `-secure` switch to the path of the executable Scalar Value.
   For example:
   `"C:\Program Files\Veritas\Cluster Server\bin\wac.exe" -secure`
5. Repeat step 4 for each system in the cluster.
6. Click **OK** to close the Edit Attribute dialog box.
7. Click the **Save and Close Configuration** icon in the tool bar.
8. Repeat step 1 to step 7 for each cluster in the global cluster.

To establish trust between root brokers if there is more than one root broker

- Establishing trust between root brokers is only required if the local clusters do not point to the same root broker.
  Log on to the root broker for each cluster and set up trust to the other root brokers in the global cluster. The complete syntax of the command is:
  `vssat setuptrust --broker <host:port> --securitylevel <low|medium|high> [--hashfile <filename> | --hash <root hash in hex>]`
  For example, to establish trust with a low security level in a global cluster comprised of Cluster1 pointing to RB1 and Cluster2 pointing to RB2:
  from RB1, type:

```
vssat setuptrust --broker RB2:14141 --securitylevel low
```

from RB2, type:

```
vssat setuptrust --broker RB1:14141 --securitylevel low
```

To bring the ClusterService-Proc (wac) resource online on all clusters

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, expand the **ClusterService** group and the Process agent.
2. Right-click the **ClusterService-Proc** resource, click **Online**, and click the appropriate system from the menu.
3. Repeat step 1 and step 2 for the additional clusters in the global cluster.

Adding multiple DR sites (optional)

In a Veritas Volume Replicator replication environment only, you can use the DR wizard to add additional secondary DR sites. Veritas Cluster Server supports up to four DR sites. In other replication environments, additional DR sites require manual configuration.

Run the DR wizard and on the Secondary System selection panel, select the new site.

Before you start the wizard on the task of configuring replication and global clustering, ensure that the cluster service group is online at the existing primary and secondary sites. This enables the wizard to configure GCO not only between the selected primary site and the new secondary site but also between the new site and the earlier configured secondary site. Otherwise, the wizard displays a warning message after the global clustering task.

When configuring the VVR replication settings with the wizard for the additional site, fields that must match existing settings are dimmed so that you cannot change them. For example, you cannot change the RVG name or RVG layout on the Replication Settings panel. Similarly, on the Global Cluster Settings panel, GCO has already been configured at the primary site, so the primary site fields are dimmed.

Recovery procedures for service group dependencies

Service group dependencies have special requirements and limitations for disaster recovery configuration and for actions to be taken in a disaster recovery scenario.

See "Supported disaster recovery configurations for service group dependencies" on page 57.

The procedure and requirements for bringing service group dependencies online at the secondary site depends on their configuration: soft, firm, or hard.

In general, if a child or parent remains online at the primary site, you take it offline before you bring the child and parent service groups online in the correct order on the secondary site.

An exception is the RVG service group, used for VVR replication, which the wizard creates with an online, local, hard dependency. The RVG group remains online at the primary site in all cases and should be left online at the primary site.

The following tables show the recovery requirements if a child or parent service group fails at the primary site and is unable to fail over on the primary site, thus requiring the secondary site to be brought online.

Using a scenario of a parent and one child, the following table shows the expected results and necessary actions you must take for an online, local, soft dependency link.

Table 7-2 Online, local, soft dependency link

Failure condition	Results	Action required
The child service group fails	■ The parent remains online on the primary site. ■ An alert notification at the secondary site occurs for the child service group only. ■ The RVG group remains online.	1 Primary site: Manually take the parent service group offline at the primary site. Leave the RVG group online. 2 Secondary site: Bring the parent and child service groups online in the appropriate order (child first, then parent).

Table 7-2 Online, local, soft dependency link

Failure condition	Results	Action required
The parent service group fails	■ The child remains online on the primary site. ■ An alert notification at the secondary site occurs for the parent only. ■ The RVG group remains online.	1 Primary site: Manually take the child service group offline at the primary site. Leave the RVG group online. 2 Secondary site: Bring the service groups online in the appropriate order (child first, then parent).

Using a scenario of a parent and one child, the following table shows the expected results and necessary actions you must take for an online, local, firm dependency link.

Table 7-3 Online, local, firm dependency link

Failure condition	Results	Action required
The child service group fails	■ The parent goes offline on the primary site. ■ An alert notification at the secondary site occurs for the child service group only. ■ The RVG group remains online.	Secondary site: Bring the service groups online in the appropriate order (child first, then parent). Leave the RVG group online at the primary site.
The parent service group fails	■ The child remains online on the primary site. ■ An alert notification at the secondary site occurs for the parent only. ■ The RVG group remains online.	1 Primary site: Manually take the child service group offline at the primary site. Leave the RVG group online. 2 Secondary site: Bring the service groups online in the appropriate order (child first, then parent).

Using a scenario of a parent and one child, the following table shows the expected results and necessary actions you must take for an online, local, hard dependency link.

Table 7-4 Online, local, hard dependency link

Failure condition	Results	Action required
The child service group fails	■ The parent goes offline on the primary site. ■ An alert notification at the secondary site occurs for the child service group only. ■ The RVG group remains online.	Secondary site: Bring the service groups online in the appropriate order (child first, then parent). Do not take the RVG group offline at the primary site.
The parent service group fails	■ The child remains online on the primary site. ■ An alert notification at the secondary site occurs for the parent only. ■ The RVG group remains online.	1 Primary site: Manually take the child service group offline at the primary site. Leave the RVG group online. 2 Secondary site: Bring the service groups online in the appropriate order (child first, then parent).

Index