Veritas Storage Foundation™ and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SharePoint 2010

Windows Server 2008 (x64)

5.1 Service Pack 2

Veritas Storage Foundation and HA Solutions HA and Disaster Recovery Solutions Guide for Microsoft SharePoint 2010

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

Product version: 5.1. Service Pack 2

Document version: 5.1.SP2.0

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

Contents

Section 1

Introduction and Concepts

This section contains the following chapters:

Chapter 1

Introducing Veritas Storage Foundation and High Availability Solutions for SharePoint Server 2010

This chapter contains the following topics:

About clustering solutions with SFW HA

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

- High availability failover cluster on the same site
- Campus cluster, in a two-node configuration with each node on a separate site
- Replicated data cluster, with a primary zone and a secondary zone existing within a single cluster, which can stretch over two buildings or data centers connected with Ethernet
- Wide area disaster recovery, with a separate cluster on a secondary site, with replication support using Veritas Volume Replicator or hardware replication

This guide describes the high availability and disaster recovery solutions for SharePoint Server 2010.

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 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 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. 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.

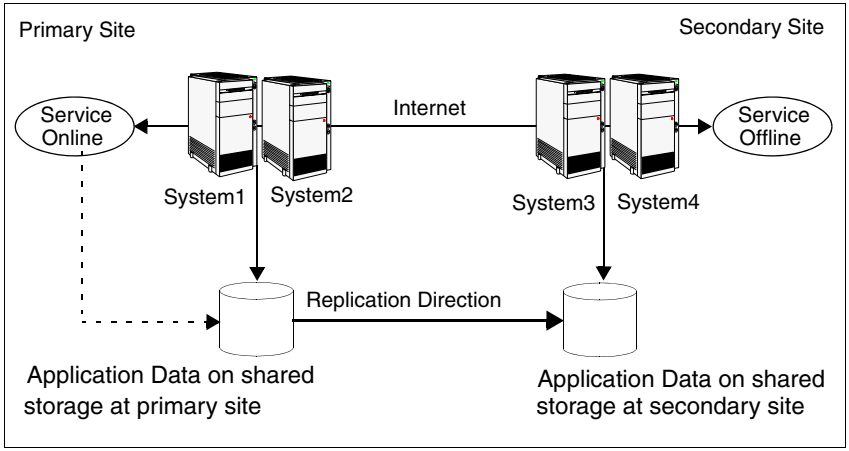
Strategically planning a DR solution provides businesses with affordable ways to meet their service level agreements, comply with government regulations, and minimize their business risks.

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.

About high availability support for SharePoint Server 2010

The high availability (HA) solution for SharePoint Server 2010 is a combination of monitoring and recovery support for SharePoint 2010 applications and high availability support for SQL Server databases used by SharePoint Server 2010.

The SharePoint 2010 high availability configuration components are as follows:

- VCS provides a new agent for SharePoint 2010 that performs the task of managing the SharePoint 2010 Web Applications, Service Applications, and services configured in the server farm. Depending on the configuration, the agent monitors, starts, and stops the SharePoint components in the cluster.
- SharePoint 2010 Web Applications are configured in a VCS parallel service group. A parallel service group runs simultaneously on multiple nodes in a cluster. The parallel service group manages the Web Applications configured in the farm. The state of the parallel service group represents the state of the Web Applications configured in the farm. If a Web Application becomes unavailable, the agent attempts to restart the application in the farm.
- SharePoint 2010 Service Applications and services are configured in a separate service group that is created locally on each cluster node. The service group manages the components configured on the local node only. If any of the components become unavailable, the agent attempts to restart the component on the local node.
- The VCS SQL Server database agents are used to configure high availability for the SharePoint databases. The agents monitor the health of the SharePoint databases as well as underlying resources and hardware. If a failure occurs, predefined actions bring up SQL Server on another node in the cluster.

About disaster recovery support for SharePoint Server 2010

Disaster recovery (DR) support for SharePoint Server 2010 involves configuring service groups for the SharePoint Web and Application servers at the primary and secondary sites and configuring DR for the SharePoint databases using the VCS DR solution for SQL Server.

After you have configured a primary site for high availability, you can set up a secondary site to create a wide area disaster recovery environment. Wide area disaster recovery uses a global cluster to enable SQL Server to failover between clusters at geographically-dispersed sites.

You can configure SharePoint Web and Application servers on the secondary site to allow for running applications and services on the secondary site if the

primary site fails. After completing the configuration, you will be able to efficiently bring your application and web services and data online at an alternate site in the event of a catastrophic failure at your primary production site.

Note: For configuring DR for SharePoint 2010, the SharePoint servers at the primary site and the secondary site must belong to the same SharePoint farm.

About quick recovery support for SharePoint Server 2010

Quick recovery (QR) solution for SharePoint Server 2010 involves scheduling and creating snapshot copies of production volumes of the SQL database. Configuring QR requires using the SFW FlashSnap technology along with Microsoft Volume Shadow Copy Services (VSS) framework to quiesce the database and ensure a persistent snapshot of the production data.

Use the FlashSnap solution to take snapshots of the SharePoint 2010 Web Applications data, Service Applications data, and the farm configuration data. You create a VSS snapshot from the SQL cluster node that hosts the SharePoint Server components data. You use the VSS snapshot wizard to take snapshots of the volumes associated with the SQL databases.

Refer to the *SFW Administrator's Guide* for more details.

For more information on quick recovery for SQL Server, refer to the Quick Recovery Solutions Guides.

Where to get more information

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

Table 1-1 shows the available solutions guides for Veritas Storage Foundation and High Availability Solutions for SQL Server 2008 and 2008 R2.

Table 1-1 SFW HA solutions guides for SQL Server 2008 and 2008 R2

Title	Description
Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008	Solutions for SQL Server 2008 and 2008 R2, and Veritas Cluster Server clustering with 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 Microsoft Clustering Solutions Guide for Microsoft SQL 2008	Solutions for SQL Server 2008 and 2008 R2, 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 2008	Quick Recovery solutions for SQL Server 2008 and 2008 R2 using either Veritas Storage Foundation for Windows or Storage Foundation HA for Windows.

Table 1-2 shows the available solutions guides for Veritas Storage Foundation and High Availability Solutions for SQL Server 2005.

Table 1-2 SFW HA solutions guides for SQL Server 2005

Title	Description
Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL	Solutions for SQL Server 2005 and Veritas Cluster Server clustering with 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 Microsoft Clustering and Quick Recovery Solutions Guide for Microsoft SQL	Quick Recovery solutions for SQL Server 2005 using either Veritas Storage Foundation for Windows or Storage Foundation HA for Windows. Solutions for SQL Server 2000/2005 and Microsoft clustering with Veritas Storage Foundation for Windows: ■ High availability (HA) ■ Campus clusters ■ Disaster recovery (DR) with Veritas Volume Replicator

Chapter 2

Introducing the VCS agent for SharePoint Server 2010

This chapter contains the following topics:

This chapter describes the VCS agent for SharePoint Server 2010 and lists the resource type definition and attribute definitions of the agent. The resource type represents the VCS configuration definition of the agent and specifies how the agent is defined in the cluster configuration file, main.cf. The Attribute Definitions lists the attributes associated with the agent. The Required Attributes table lists the attributes that must be configured for the agent to function properly.

About the VCS agent for Microsoft SharePoint Server 2010

The VCS application agent for Microsoft SharePoint Server manages SharePoint Server 2010 Service Applications, Web Applications, and services in a VCS cluster. The agent provides monitoring support in making a SharePoint Server 2010 applications highly available in a VCS environment.

Depending on the configuration, the agent performs the following operations:

- monitors and starts the configured SharePoint services
- monitors the configured Web Applications, brings them online, and takes them offline
- monitors the configured Service Applications, brings them online, and takes them offline

If any of the configured SharePoint component fails or is unavailable, the agent attempts to start the component on the local node. If the components fails to start, the agent declares the resource as faulted.

SharePoint Server 2010 agent functions

Agent functions include the following:

Online	Starts the configured Web Applications, Service Applications, or services.
Offline	Stops the configured Web Applications and Service Applications. The agent also stops monitoring the configured services on the node.
Monitor	Verifies the status of the configured Web Application, Service Application or service. If the components are running, the agent reports the resource as ONLINE. If any of the components are not running, the agent reports the resource as FAULTED.
Clean	Forcibly stops the configured Web Applications and Service Applications. The agent also stops monitoring the configured services on the node.

SharePoint Server 2010 agent state definitions

Agent state definitions are as follows:

ONLINE	Indicates that the configured Web Applications, Service Applications, or services are running on the cluster node.
OFFLINE	Indicates that the configured Web Applications and Service Applications are stopped on the cluster node. It also indicates that the monitoring for the services is also stopped.
FAULTED	Indicates that the agent is unable to start the configured Web Applications, Service Applications, or services on the cluster node.
UNKNOWN	Indicates that the agent is unable to determine the status of the configured SharePoint components on the cluster node.

SharePoint Server 2010 agent resource type definition

The SharePoint Server 2010 agent is represented by the SharePointServer resource type.

The resource definition is as follows:

```
type SharePointServer (
    static i18nstr ArgList[] = { AppType,
    AppName, AppPoolMon, FarmAdminAccount, FarmAdminPassword,
    ServiceIDList }
    str AppType
    i18nstr AppName
    str AppPoolMon = NONE
    i18nstr FarmAdminAccount
    str FarmAdminPassword
    i18nstr ServiceIDList[]
    )
```

SharePoint Server 2010 agent attribute definitions

Review the following information to familiarize yourself with the agent attributes for a SharePointServer resource type. This information will assist you during the agent configuration.

Table 2-1 SharePoint Server 2010 agent required attributes

Required Attributes	Type and Dimension	Definition
AppType	string-scalar	Defines whether the agent is configured to monitor a SharePoint Web Application, Service Application, or service. This attribute can take one of the following values: ■ WebApp ■ ServiceApp ■ SPSService The default value is WebApp. If this attribute value is set to WebApp or ServiceApp, then you must specify a value for the AppName attribute. If this attribute value is set to SPSService, the AppName attribute value is ignored.

Table 2-1 SharePoint Server 2010 agent required attributes (Continued)

Required Attributes	Type and Dimension	Definition
AppPoolMon	string-scalar	Defines the monitoring modes for the application pool associated with the Web site being monitored. Configure this attribute only if AppType attribute value is set to WebApp and IIS is configured to run in the Worker Process Isolation mode. The attribute can take one of the following values: ■ NONE: Indicates that the agent does not monitor the application pool associated with the Web site. ■ DEFAULT: Indicates that the agent monitors the root application pool associated with the Web site. If this attribute is set, the agent starts, stops, and monitors the root application pool associated with the Web site. If the root application pool is stopped externally, the service group faults; the agent then attempts to start the root application pool. ■ ALL: Indicates that the agent starts all the application pools associated with the Web site, but monitors and stops the root application pool only. If any application pool is stopped externally, the service group faults; the agent then attempts to start the application pool. The default value is NONE.

Table 2-1 SharePoint Server 2010 agent required attributes (Continued)

Required Attributes	Type and Dimension	Definition
ServiceIDList	string-vector	Defines the service IDs of the SharePoint services that are managed by the agent. This attribute is always local, that is, it is different for each cluster node. This attribute can take the following values: ■ If AppType attribute value is set to WebApp, specify the service ID of the Microsoft SharePoint Foundation Web Application service. ■ If AppType attribute value is set to ServiceApp, specify the service ID of the service on which the Service Application depends. ■ If AppType attribute value is set to SPSService, specify the service IDs of the SharePoint services. **Note:** If you are configuring this attribute manually, use the VCS hadiscover command or the SharePoint server cmdlets to retrieve the service IDs.

Table 2-2 SharePoint Server 2010 agent optional attributes

Optional Attribute	Type and Dimension	Definition
AppName	string-scalar	The name of the SharePoint Web Application or Service Application that is managed by the agent. The value of this attribute depends on the value of the AppType attribute. This attribute can take the following values: ■ If AppType attribute value is set as WebApp, specify the Web Application name. ■ If AppType attribute value is set as ServiceApp, specify the application pool ID for the SharePoint Service Application. **Note:** This attribute is ignored if AppType attribute value is set as SPSService.

Table 2-2 SharePoint Server 2010 agent optional attributes (Continued)

Optional Attribute	Type and Dimension	Definition
FarmAdminAccount	string-scalar	A user account that has the SharePoint Server Farm Admin privileges. User name can be of the form *username@domain.com*, *domain\username*, or *domain.com\username*. The agent uses the Farm Admin user account context to manage the services specified in the ServiceIDList attribute value.
FarmAdminPassword	string-scalar	The password of the user specified in the FarmAdminAccount attribute value. The password is stored in the VCS configuration in an encrypted form.

Section 2

Configuration Workflows

This section contains the following chapters:

Chapter 3

Configuration workflows for SharePoint Server 2010

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 SharePoint Server.

See "About the Solutions Configuration Center" on page 39.

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

Table 3-1 outlines the high-level objectives and the tasks to complete each objective for a high availability configuration.

Note: Symantec recommends as a best practice to configure SQL Server for high availability before configuring SharePoint Server 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 20.

Table 3-1 SharePoint Server: High availability configuration tasks

Action	Description
Verify hardware and software requirements	See "Reviewing the requirements" on page 52.
Review the HA configuration	■ Understand active-passive configuration See "Reviewing the HA configuration" on page 57.
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment ■ Verify the DNS entries for the systems on which SharePoint Server will be installed See "Configuring the storage hardware and network" on page 66.
Install SFW HA	■ Verify the driver signing option for the system ■ Install Veritas Storage Foundation HA for Windows ■ Select the option to install the Veritas Cluster Server Application Agent for SharePoint Server 2010 ■ To configure SQL Server for high availability, select the option to install Veritas Cluster Server Agent for Microsoft SQL Server See "Installing Veritas Storage Foundation HA for Windows" on page 68.

Table 3-1 SharePoint Server: High availability configuration tasks (Continued)

Action	Description
Configure VCS cluster	You can include both SQL Server and SharePoint Server systems in the same cluster if they use the same operating system platform. If you are configuring SharePoint Server in a separate cluster, perform the following tasks: ■ 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 72. If you are adding the SharePoint systems to the existing SQL Server cluster, perform the following task: ■ Run the VCS Cluster Configuration Wizard (VCW) to add the nodes See "Adding nodes to an existing cluster" on page 86.
Install SharePoint Server on the cluster nodes	■ Install and configure Microsoft SharePoint Server on each cluster node and configure the farm. While installing, select the **Complete** installation mode. The **Stand-alone** install mode is not supported. Refer to the SharePoint Server documentation for installation instructions
Create SharePoint Server service groups	■ Launch the VCS SharePoint Server Configuration Wizard on a node on which SharePoint is installed and configured to create SharePoint service groups See "Configuring SharePoint Server service groups" on page 94.
Verify the HA configuration	Test failover between nodes See "Verifying the SharePoint cluster configuration" on page 98.

Disaster recovery configuration

For configuring disaster recovery, you first begin by configuring the primary site for high availability.

See "High availability (HA) configuration" on page 34.

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

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

Table 3-2 Configuring the secondary site for disaster recovery

Action	Description
Configure SQL Server for disaster recovery at the secondary site	For the steps for configuring SQL Server for high availability and disaster recovery, see *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL* *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008 and 2008 R2*
Modify the SQL Server service group on the primary and secondary site	Edit the SQL Server service group on both the primary and secondary site to allow updating the NLB details if a disaster recovery failover occurs. See "Configuring the SQL Server service group for DR in the SharePoint environment" on page 103.
Verify that SharePoint has been configured for high availability at the primary site	Verify that SharePoint has been configured for high availability at the primary site. See Chapter 7, "Installing and configuring SharePoint Server 2010 for high availability".

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

Action	Description
Install SFW HA and configure the cluster on the secondary site	Install SFW HA on the SharePoint server systems on the secondary site. Ensure that you select the option to install the Veritas Cluster Server Application Agent for SharePoint Server 2010. You can optionally use the same SFW HA cluster for both SQL Server and SharePoint Server if all systems use the same operating system platform. Otherwise, create a separate cluster for SharePoint. See "Configuring the secondary site for SharePoint disaster recovery" on page 111.
Install SharePoint on the cluster nodes on the secondary site	Install Microsoft SharePoint Server on the SharePoint servers on the secondary site. Run the Microsoft SharePoint Products Configuration wizard to add the servers to the existing primary site farm. Choose the option to connect to an existing server farm. **Note:** You do not need to configure the same number of web servers or service applications on the secondary site as on the primary site. However, you should provide for all required services.
Create the SharePoint service groups on the secondary site	Configure the SharePoint Server service groups for the secondary site The VCS SharePoint Server Configuration Wizard helps you create SharePoint Server service groups. See "Configuring SharePoint Server service groups" on page 94.
Verify the disaster recovery configuration	In the Veritas Cluster Server Java console, ensure that you can bring the SharePoint service groups online and offline.
Configure the Search service application for DR	Providing disaster recovery for the search service application includes configuring DR for the following components on the secondary site: Crawl component Query and indexing components Administration component Property and Administration databases See "Configuring the Search service application for disaster recovery" on page 112.

Section 3

Requirements and Planning

This section contains the following chapter:

- Requirements and planning for your HA and DR configurations

Chapter 5

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

For normal operation, all installations require an additional 50 MB of disk space.

Table 5-1 estimates disk space requirements for SFW HA.

Table 5-1 Disk space requirements

Installation options	Install directory/drive
SFW HA + all options + client components	1564 MB
SFW HA + all options	1197 MB
Client components	528 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 5.1 Service Pack 2 Hardware Compatibility List to confirm supported hardware:
  http://entsupport.symantec.com/docs/358407
- Review the SFW HA 5.1 Service Pack 2 Software Compatibility List to confirm supported software:
  http://entsupport.symantec.com/docs/358406
- Review the SharePoint 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 Global Clustering Option and depending on your replication solution select Veritas Volume Replicator or a hardware replication agent.

- When installing SFW HA for a Replicated Data Cluster configuration, ensure that you select the option to install Veritas Volume Replicator.

Supported SharePoint versions

SFW HA 5.1 Service Pack 2 provides support for SharePoint Server 2010.

SharePoint 2010 is supported with SFW HA 5.1 SP2 on the following operating systems:

- Windows Server 2008 with Service Pack 2 or later, x64 Edition
- Windows Server 2008 R2, x64 Edition

See the Microsoft documentation for details on required SQL Server database versions supported with Sharepoint Server 2010.

System requirements for SFW HA

Systems must meet the following requirements for SFW HA:

- Memory must be a minimum 1 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 56.
- NIC teaming is not supported for the VCS private network.
- All servers must have the same system architecture, run the same operating system, and be at the same service pack (SP) level.

Network requirements for SFW HA

SFW HA has the following network requirements:

- Install SFW HA on servers in a Windows Server 2003 or Windows Server 2008 domain.
- 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 for the following purposes:
  - 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.

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.
- You must install the operating system in the same path on all systems. For example, if you install Windows Server on C:\WINDOWS of one node, installations on all other nodes must be on C:\WINDOWS. Make sure that the same drive letter is available on all nodes and that the system drive has adequate space for the installation.
- 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

Symantec recommends as a best practice to configure SQL Server for high availability before configuring SharePoint Server.

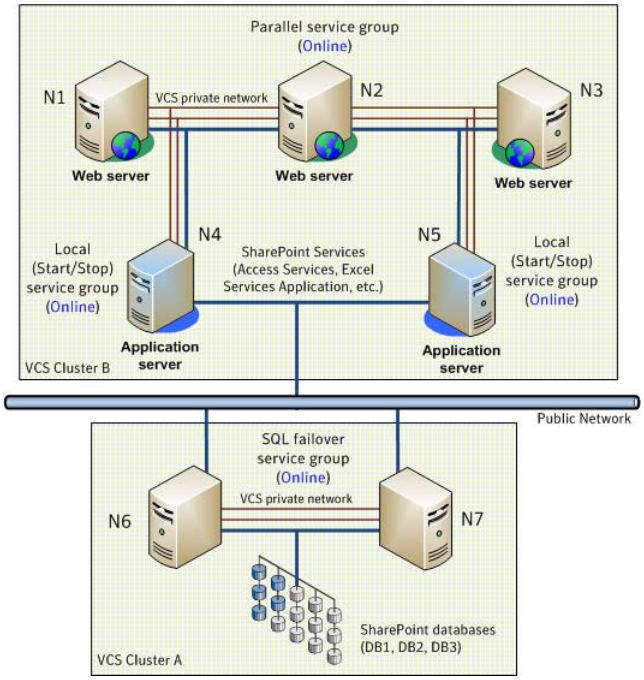
Configuring SQL Server for high availability is covered in the SQL Server solutions guides. See “Where to get more information” on page 20.

In a typical example of a SharePoint Server 2010 high availability environment, SharePoint Web Applications and Service Applications are configured on a separate set of cluster nodes. A VCS parallel service group manages the Web Applications residing on the Web servers and local service groups manage the application servers. The SharePoint databases are made highly available using the VCS SQL Server service group. The databases reside on shared storage that is accessible from all the SharePoint server nodes in the cluster.

Figure 5-1 illustrates a typical SharePoint Server 2010 configuration. The SharePoint farm layout is as follows:

- Nodes N1, N2, and N3 are the Web front end servers
- Nodes N4 and N5 are the application servers
- Nodes N6 and N7 host the SharePoint SQL databases

Figure 5-1 SharePoint Server 2010 high availability configuration



The graphic displays SQL and SharePoint Servers in different clusters. However, if the SharePoint Servers and SQL Servers are using the same operating system and platform, you can configure both SQL and SharePoint nodes in the same cluster.

The SharePoint Web Applications are configured in a parallel service group that is online on Nodes N1, N2, and N3. The application servers host SharePoint services such as Access Services and Excel Services that are used by the Web servers. These application services are configured in local service groups on nodes N4 and N5 separately. If any of the configured Web or Service applications become unavailable, the SharePoint agent attempts to restart those components in the cluster. If the component fails to come online, the agent declares the resource as faulted.

The databases are made highly available by the SQL service group that is configured on nodes N6 and N7. The databases are configured on the shared storage. The SQL virtual server is online on node N6. All client requests are handled by node N6. N7 waits in a warm standby state as a backup node, prepared to begin handling client requests if N6 becomes unavailable. If N6 fails, N7 becomes the active node and the SQL virtual server comes online on N7.

From the user's perspective there will be a small delay as the backup node comes online, but the interruption in effective service is minimized.

Sample SharePoint Server 2010 HA configuration

A sample setup is used to illustrate the installation and configuration tasks for the HA configuration.

Table 5-2 shows a sample SharePoint configuration. If you plan to take snapshots of SharePoint components using FlashSnap, you must ensure that the SharePoint database components are configured on volumes on shared storage.

Table 5-2 Sample SharePoint Server 2010 HA configuration objects

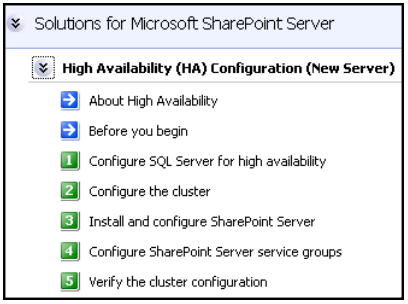
Name	Object
N1, N2, N3, N4, N5	SharePoint Server nodes
N6, N7	SQL Server nodes
SharePoint_Config-WebApplication1	Name of the parallel service group configured for the SharePoint Web Applications.
SharePoint_Config-N4-ServiceApp1 SharePoint_Config-N5-ServiceApp2	Names of the local service groups configured for the SharePoint Service Applications or services.
INST1	SQL Server instance name
INST1_DG	cluster disk group
INST1-VS	SQL Server virtual server name
INST1_SG	SQL Server service group name
INST1_DB1_VOL	Volume for SQL Server database
INST1_DB1_LOG	Volume for SQL Server database logs

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 SharePoint Server.

Figure 5-2 shows the workflow under the High Availability (HA) Configuration in the Solutions Configuration Center.

Figure 5-2 Configuration steps in the Solutions Configuration Center



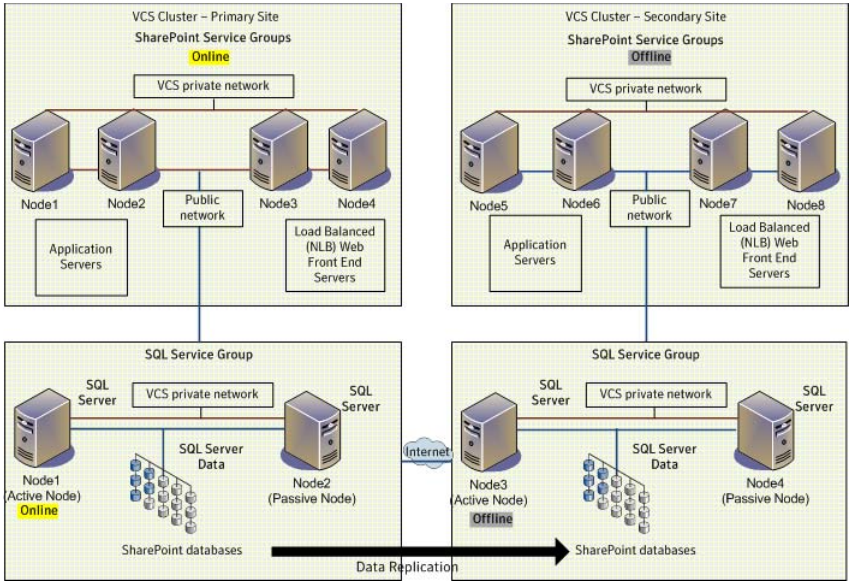
Reviewing the disaster recovery configuration

You configure SQL Server for disaster recovery before configuring SharePoint Server.

Configuring SQL Server for disaster recovery is covered in the SQL Server solutions guides. See “Where to get more information” on page 20.

Figure 5-3 shows an example SharePoint Server disaster recovery configuration.

Figure 5-3 Example SharePoint Server disaster recovery configuration



The example configuration for SharePoint disaster recovery shows SharePoint configured in a separate cluster from SQL Server. However, you can optionally configure SharePoint Server in the same cluster as SQL Server if all systems use the same operating system.

In the example setup, there are eight SharePoint servers, four for the primary site and four for the secondary site. This is an example only; any supported farm configuration can be used. The SharePoint nodes will form two separate clusters, one at the primary site and one at the secondary site.

Note: You do not need to configure the same number of SharePoint web servers or application servers on the secondary site as on the primary site. However, you should provide for all required services to be available on the secondary site.

The sample setup for SQL Server 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. Disaster recovery configuration for SQL Server configures a global cluster with replication of the databases from the primary to the secondary site.

If the SQL Server primary site fails, the replicated SQL Server databases on the secondary site come online, along with SQL Server. In addition, the SharePoint Servers on the secondary site will automatically start responding to clients.

If the SharePoint Servers fail on the primary site, but SQL Server remains online on the primary site, you would need to manually switch the SQL Server service group to the secondary site. This would be necessary for the secondary site SharePoint servers to respond to clients.

Section 4

Deployment

This section contains the following chapters:

Chapter 6

Installing and configuring SFW HA

This chapter contains the following topics:

Configuring the storage hardware and network

Use the following procedures to configure the hardware and verify DNS settings. Repeat this procedure for every node in the cluster.

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 using the following guidelines:
   - 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

1. From the Control Panel, access the Network Connections window.
2. Ensure the public network adapter is the first bound adapter as follows:
   - From the Advanced menu, 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.
3. Ensure that DNS name resolution is enabled. Make sure that you use the public network adapter, and not those configured for the private network. Do the following:
   - In the Network Connections window, double-click the adapter for the public network to access its properties.
   - In the Public Status dialog box, on the General tab, click **Properties**.

- In the Public Properties dialog box, on the General tab, select the **Internet Protocol (TCP/IP)** check box and click **Properties**.
- Select the **Use the following DNS server addresses** option and verify the correct value for the IP address of the DNS server.
- Click **Advanced**.
- In the DNS tab, make sure the **Register this connection's address in DNS** check box is selected. Make sure the correct domain suffix is entered in the **DNS suffix for this connection** field.

Installing Veritas Storage Foundation HA for Windows

The product installer enables you to install the software for Veritas Storage Foundation HA for Windows. The installer automatically installs Veritas Storage Foundation for Windows and Veritas Cluster Server. On the SQL Server systems, select the option to install the Veritas Cluster Server Database Agent for SQL. On the SharePoint Server systems, select the option to install the Veritas Cluster Server Application Agent for SharePoint Server 2010.

When installing Veritas Storage Foundation HA for Windows, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

Installing Symantec Trusted certificate for unsigned drivers

The product installer provides an installation option for Symantec Trusted Software Publisher Certificate for Veritas Storage Foundation for Windows drivers that are not certified by Microsoft.

If you select this installation option, a Symantec Trusted certificate is installed on the systems you select for installation.

Warning: On Windows Server 2008, if this option is not selected, a remote install will not install any SFW drivers that are not certified by Microsoft. No notification is given and it will appear that installation was successful, but issues can arise later because the drivers were not installed.

If installing locally on Windows Server 2008, if this option is not selected, a driver signing popup will be displayed requiring user interaction.

Installing Storage Foundation HA for Windows

Install Veritas Storage Foundation HA for Windows.

To install the product

1. Insert the DVD containing the installation software into your system's disk drive or download the installation software from the Symantec website.
2. Allow the autorun feature to start the installation or double-click **Setup.exe.**
3. Review the links on the DVD browser panel.
   The panel provides the **Late Breaking News** link to access the latest information about updates, patches, and software issues regarding this

release, and a link to run the Configuration Checker to verify that your configurations meet all pertinent software and hardware requirements.

The panel provides links to install the software (Storage Foundation for Windows or Storage Foundation HA for Windows) and access the documentation (Getting Started Guide, Installation and Upgrade Guide, and Release Notes).

The panel also provides links to access the Veritas Operations Services (VOS) site (VOS provides you four types of detailed reports about your computer and Symantec enterprise products, a checklist of configuration recommendations, and system and patch requirements to install or upgrade your software), contact the Symantec Technical Support, and see the contents of the DVD.

4 Under Install Storage Foundation HA, do one of the following:

- Click the **Complete/Custom** link to install server or client or both the components.
- Click the **Administrative Console** link to install only the client components.

Click the Complete/Custom link.

5 On the Welcome panel, review the Welcome message and the listed prerequisites. Ensure that the prerequisites are met prior to proceeding. Click **Next**.

6 On the License Agreement panel, read the license agreement. If you agree to the license terms, click **I accept the terms of the License Agreement**, and then click **Next**.

7 On the License panel, enter the product license key before adding license keys for features. Click **Enter license key(s)**, provide the license key in the field below it, and then click **Add**.

If you do not have a license key, click **Use embedded evaluation license key** to use the default evaluation license key. This license key is valid only for a limited evaluation period.

To remove a license key, click the key, and then click **Remove**. To see a license key's details, click the key to display its details in the License key details area.

Click **Next** to continue.

8 On the Option Selection panel, select the appropriate SFW product options, and click **Next**. On the SharePoint Server systems, ensure that you select the option to install the SharePoint 2010 Configuration Wizard.

9 On the System Selection panel, do the following, and then click **Next**:

- To add a computer for installation, provide the name of the computer in the System Name box.

OR

If you do not know the name of the computer, click **Browse** to search for the computers available in your domain. The Selected Systems dialog box appears. Select a computer from the Available Systems area, move it to the Selected Systems area, and then click **OK** to add it for installation.

- To change the installation path of an added computer, click the folder icon for the computer, and then select the installation path in the Browse For Folder dialog box.
- To know the verification status and other information of the added computer, click the information icon.
- To remove an added computer, select it, and then click the recycle bin icon.

Note: When installing the software on multiple computers in a single installation using the product installer, all computers must have the same platform type (for example, x86 or x64). However, the computers can have different Windows operating systems. For example, you can install the software on multiple computers at once running Windows 2003 and Windows 2008.

The installer checks the prerequisites for the added computers and displays the results in the Status column. If a computer fails validation, address the issue, and repeat the validation process by clicking **Re-verify**.

10 Depending upon your earlier product installer selections and operating system, you may receive one or more of the following messages. If applicable to your installation, perform the procedure mentioned in the messages.

If you are using multiple paths and selected a specific DSM, you receive the Veritas Dynamic Multi-pathing warning:	The time to install the Veritas Dynamic Multi-pathing MPIO feature depends on the number of physical paths connected during the installation. To reduce installation time for this feature, Symantec recommends only one physical path connection during installation. After the installation completes, reconnect additional physical paths before rebooting the system.
If you are using multiple paths and selected a specific DSM on a Windows Server 2008 machine, you receive an additional message:	On Windows Server 2008, the Microsoft Multipath input/output (Microsoft MPIO) feature must be enabled before installing DMP Device Specific Modules (DSMs).

When installing Veritas Storage Foundation for Windows (Server Components) with the MSCS option selected, you receive the following message:	When installing Veritas Storage Foundation for Windows (Server Components) with the Microsoft Cluster Server (MSCS) option, you may want to adjust the minimum and maximum time for quorum arbitration to ensure optimal functioning of Veritas Storage Foundation for Windows dynamic volumes with MSCS. For more information, see the *Veritas Storage Foundation Administrator's Guide*.

Review the messages, and then click **OK**.

11 On the Pre-install Summary panel, the Pre-install Report is displayed with summarized information about the installation. Review the Pre-install Report. Click **Back** to make changes, if necessary. Click **Save Report** to save the report as a web page or text file on your computer.
It is recommended that you select the **Automatically reboot systems after installer completes the operation** check box to restart the computer after the installation is complete.
Click **Install** to install the software.

12 The Installation panel displays status messages and the progress of the installation.
If an installation fails, click **Next** to review the report, and address the reason for failure. You may have to either repair the installation or uninstall and re-install the software.

13 On the Post-install Summary panel, the Post-install Report is displayed with summarized information about the installation results along with links to the log files and installation summary for the computer. Click **Save Report** to save the report as a web page or text file on your computer. Review the Post-install Report and log files, and then click **Next**.

14 On the Finish panel, click **Finish** to complete the installation.

15 Click **Yes** to restart the local node.

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 Cluster Management Console (Single Cluster Mode) also referred to as Web Console, notification, and global clusters.

Complete the following tasks before creating a cluster:

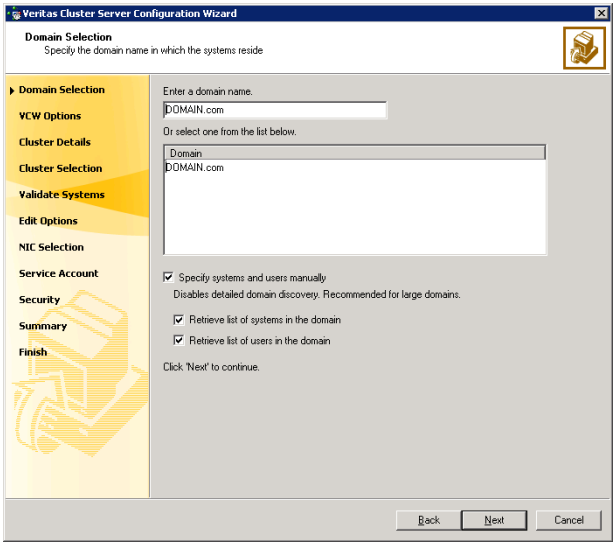
- Verify that each node uses static IP addresses and that name resolution is configured for each node.
- Verify that you have the required privileges.
  See "Reviewing the requirements" on page 52.

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 74.
- 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**.

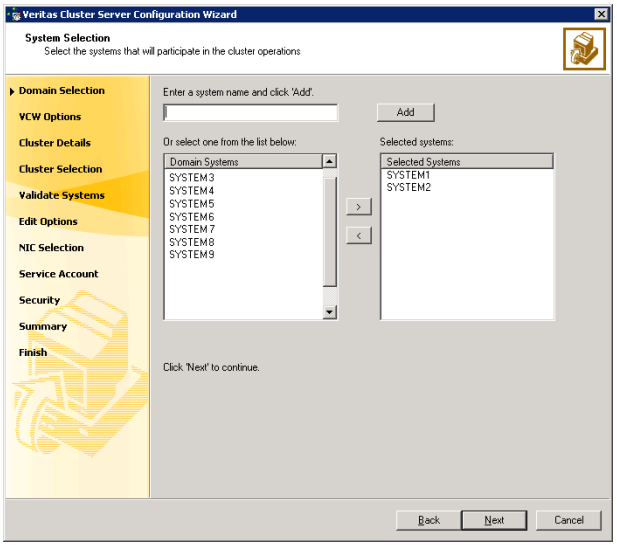
    If you chose to retrieve the list of systems, proceed to step 6 on page 74. Otherwise, proceed to the next step.

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 74.

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**.

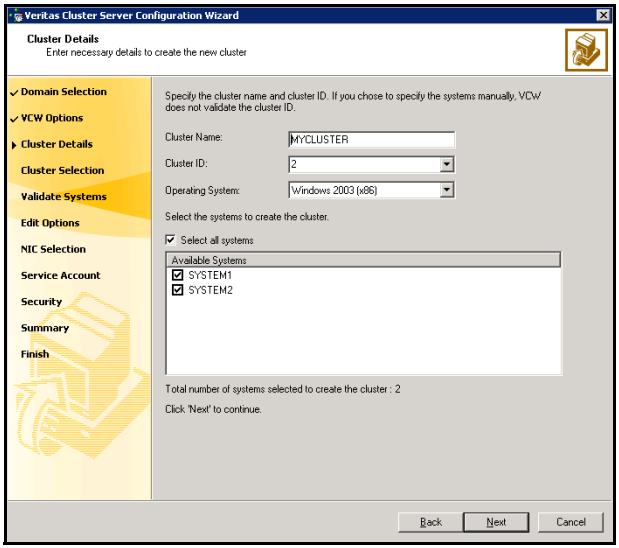
A system can be rejected for any of the following reasons:

- 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 **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 255.

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 32-bit and a 64-bit 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**.

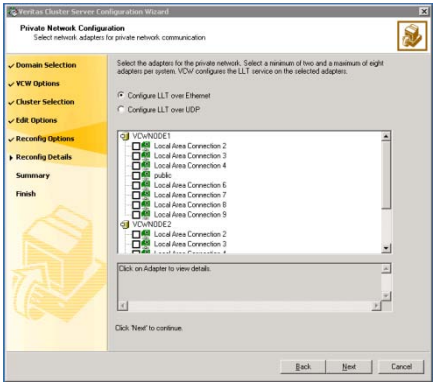
If a system is not validated, review the message associated with the failure and restart the wizard after rectifying the problem.

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 78.

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 the ethernet or over the User Datagram Protocol (UDP) layer.

Do one of the following:

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



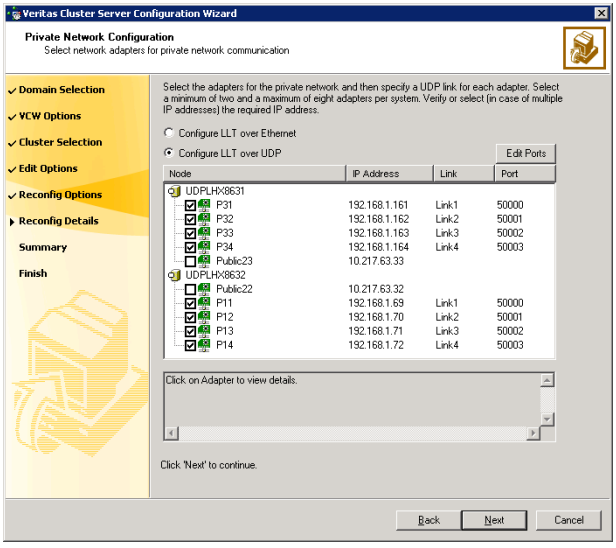
- Select the check boxes next to the two NICs to be assigned to the private network.

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 **Configure LLT over UDP**.
- 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.

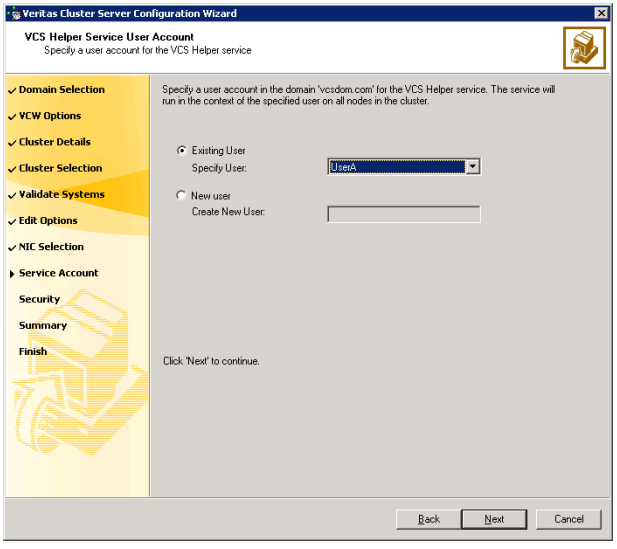
- Specify a unique UDP port for each of the link. Click **Edit Ports** if you wish to edit the UDP ports for the links. You can use ports in the range 49152 to 65535. The default ports numbers are 50000 and 50001 respectively. Click **OK**.
- For each selected NIC, verify the displayed IP address. If a selected NIC has multiple IP addresses assigned, double-click the field and choose the desired IP address from the drop-down list. 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.

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.

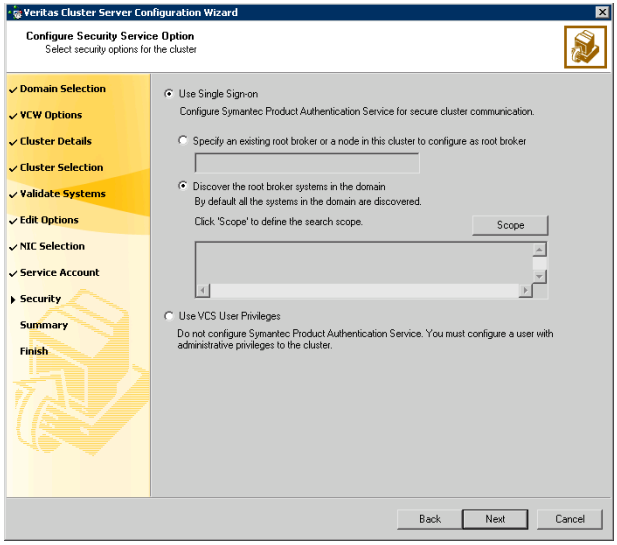


Specify a domain user as follows:

- 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 73, 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 and then click **Next**.
Do one of the following:

- To use the single sign-on feature, complete the following steps:



  - Click **Use Single Sign-on**. In this mode, the Symantec Product Authentication Service is used to secure communication between cluster nodes and clients, including the Java console, 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.

For more information about secure communications in a cluster, see the *Veritas Storage Foundation and High Availability Solutions Quick Start Guide for Symantec Product Authentication Service*.

- If you know the name of the system that will serve as the root broker, click **Specify an existing root broker or a node in this cluster to configure as root broker**, type the system name, and then click **Next**.

  If you specify a cluster node, the wizard configures the node as the root broker and other nodes as authentication brokers. Authentication brokers reside one level below the root broker and serve as intermediate registration and certification authorities. These brokers can authenticate clients, such as users or services, but cannot authenticate other brokers. Authentication brokers have certificates signed by the root.

  If you specify a system outside of the cluster, make sure that the system is configured as a root broker; the wizard then configures all nodes in the cluster as authentication brokers.
- If you want to search the system that will serve as root broker, click **Discover the root broker systems in the domain** and click **Next**. The wizard will discover root brokers in the entire domain, by default.
- If you want to define a search criteria, click **Scope**. In the Scope of Discovery dialog box, click **Entire Domain** to search across the domain, or click **Specify Scope** and select the Organization Unit from the Available Organizational Units list, to limit the search to the specified organization unit. Use the Filter Criteria options to search systems matching a certain condition.

  For example, to search for systems managed by a user *Administrator*, select **Managed by** from the first drop-down list, **is (exactly)** from the second drop-down list, type the user name **Administrator** in the adjacent field, click **Add**, and then click **OK**.

  To search for all Windows Server 2003 systems, select **Operating System** from the first drop-down list, **is (exactly)** from the second drop-down list, type ***2003*** in the adjacent field, click **Add** and then click **OK**.

Table 6-1 contains some more examples of search criteria.

Table 6-1 Search criteria examples

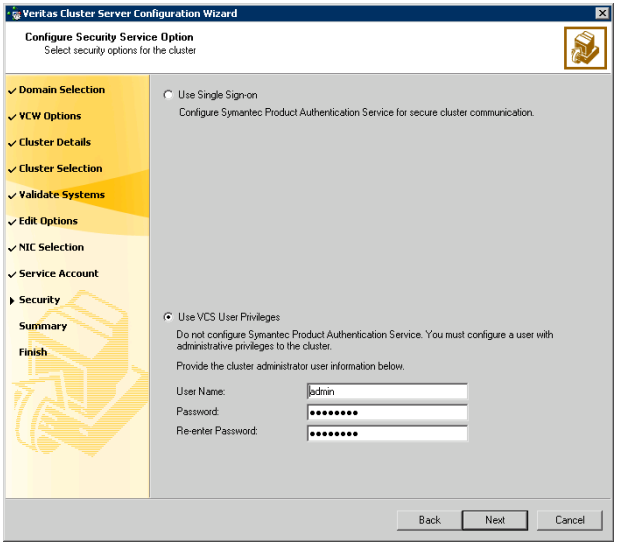
1st drop-down list value	2nd drop-down list value	Adjacent field entry	Search result
Name	is (exactly)	*system	Displays all systems with names that end with *system*.
Name	is (exactly)	*vcsnode*	Displays all systems with names that contain *vcsnode*.
Operating System	is (exactly)	*2003*	Displays all Windows Server 2003 systems.
Operating System	is (exactly)	*Enterprise*	Displays all Windows Server Enterprise Edition systems.
Operating System Version	is (exactly)	5.*	Displays all systems whose operating system version is 5.x, where x could be 0, 1, 2, etc.

You can add multiple search criterion; the wizard will search for systems that match all the conditions specified.

- Click **Next**. The wizard discovers and displays a list of all the root brokers. Click to select a system that will serve as the root broker and then click **Next**.

If the root broker is a cluster node, the wizard configures the other cluster nodes as authentication brokers. If the root broker is outside the cluster, the wizard configures all the cluster nodes as authentication brokers.

- To use a VCS user privilege, complete the following steps:



  - 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 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.
  - Click **Next**.

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 service 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.

Refer to the *Veritas Cluster Server Administrator's Guide* for complete details on the Notification resource.

The GCO Option applies only if you are configuring a Disaster Recovery environment and are not using the Disaster Recovery wizard. The Disaster Recovery chapters discuss how to use the Disaster Recovery wizard to configure the GCO option.

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

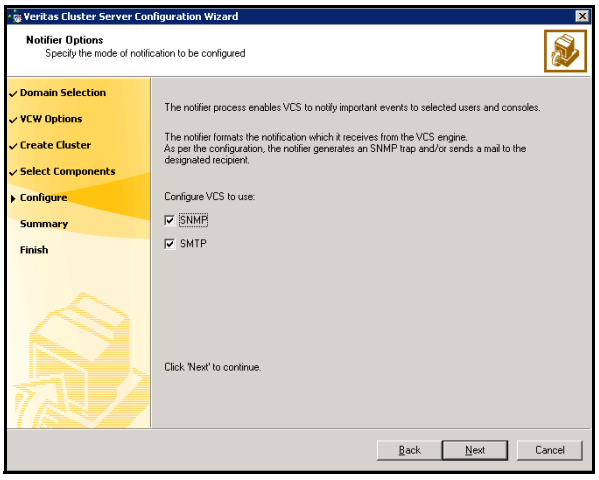
- Check the **Notifier Option** checkbox to configure notification of important events to designated recipients.
  See "Configuring notification" on page 83.

Configuring notification

This section describes steps to configure notification.

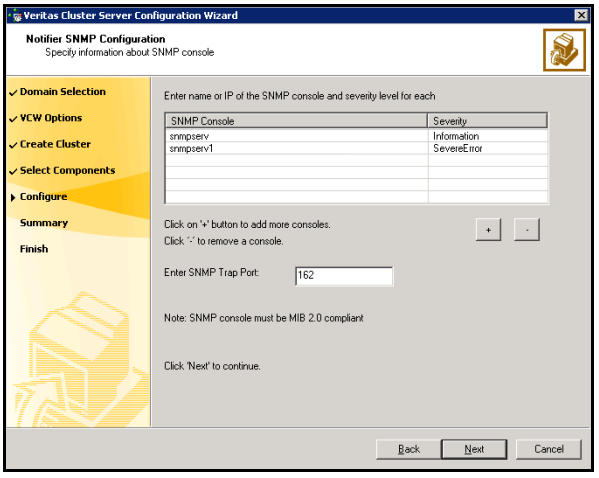
To configure notification

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



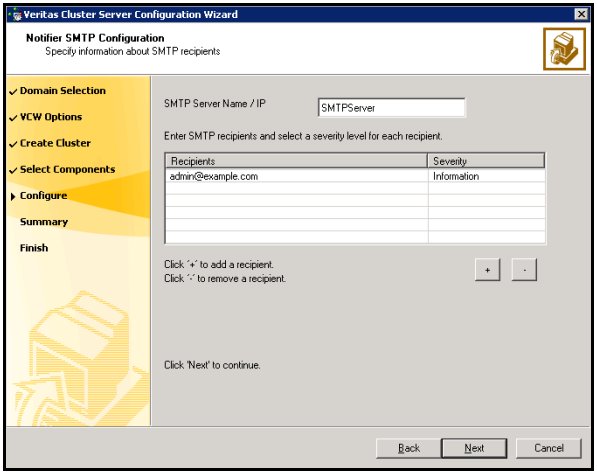
You can configure VCS to generate SNMP (V2) traps on a designated server and send emails to designated recipients in response to certain events.

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



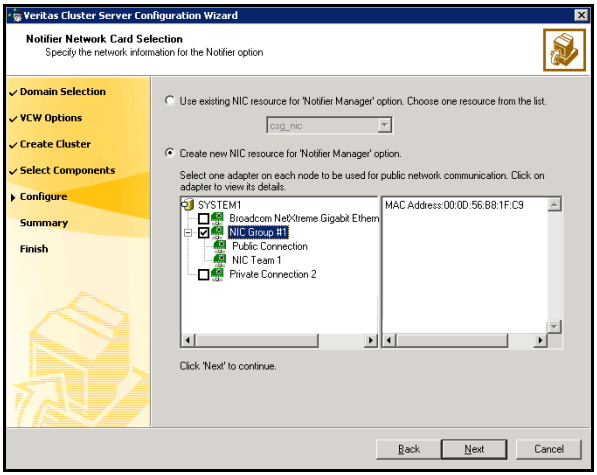
- Click a field in the SNMP Console column and type the name or IP address of the console. The specified SNMP console must be MIB 2.0 compliant.
- Click the corresponding field in the Severity column and select a severity level for the console.
- Click '**+**' to add a field; click '**-**' to remove 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 nodes to an existing cluster

Optionally, you can configure both the SQL Server and SharePoint Server systems in the same SFW HA cluster if all systems use the same operating system and platform. If you have an existing SQL Server cluster and want to add the SharePoint systems to it, you can use this procedure.

To add a node to a VCS cluster

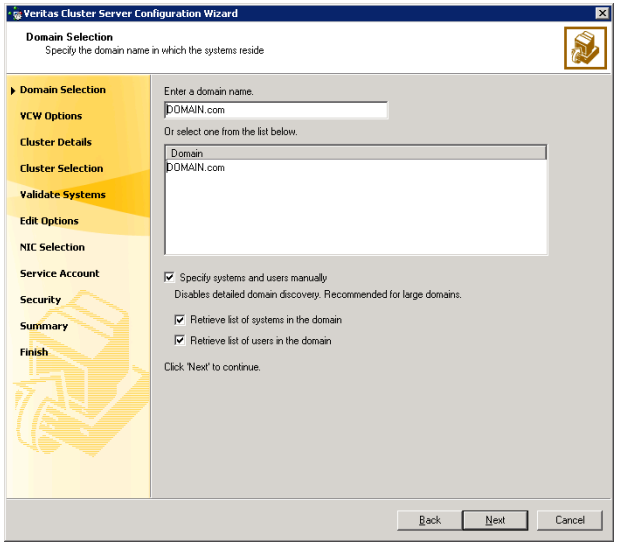
1 Start the VCS Cluster Configuration wizard.
Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Cluster Configuration Wizard**.

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:

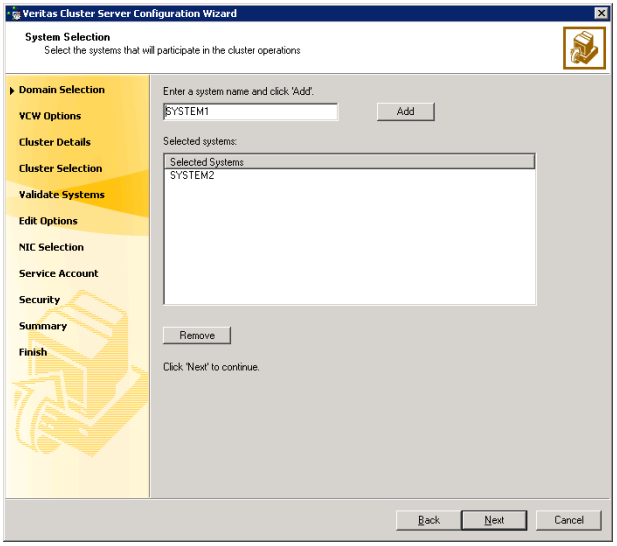
- To discover information about all the systems and users in the domain:
  - Clear the **Specify systems and users manually** check box.
  - Click **Next**.

  Proceed to step 8 on page 90.
- 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 89. Otherwise proceed to the next step.

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

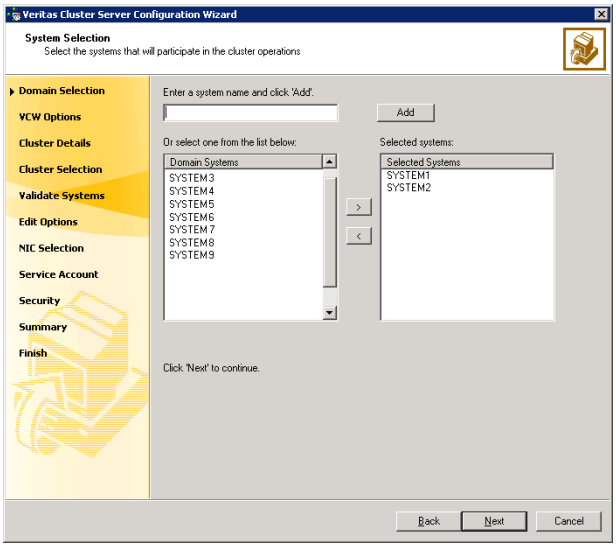


- Type the name of a node in the cluster and click **Add**.
- Type the name of the system to be added to the cluster and click **Add**.

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 90.

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.

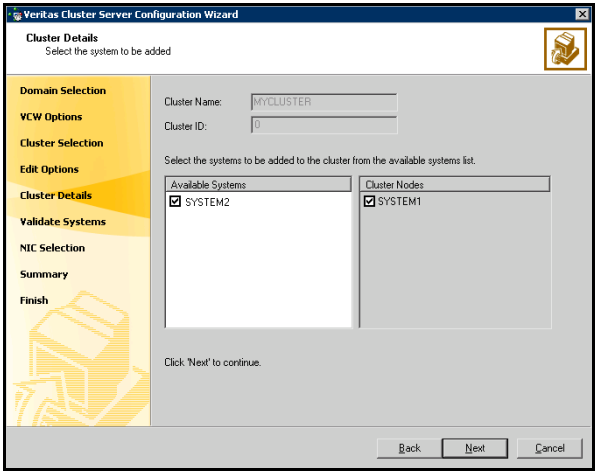
Click on a system name to see the validation details. If you wish to include a rejected system, rectify the error based on the reason for rejection and then run the wizard again.

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 will configure 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**.
  - 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. 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 will configure 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**.

17 The wizard starts running commands to add the node. After all commands have been successfully run, click **Finish**.

Chapter 7

Installing and configuring SharePoint Server 2010 for high availability

This chapter contains the following topics:

Installing and configuring SharePoint Server

Install and configure Microsoft SharePoint Server on all the nodes that will be part of the SharePoint Server service group and configure the farm.

Note the following before you proceed:

- Symantec recommends that you first configure SQL Server for high availability before configuring SharePoint Server 2010.
- While installing SharePoint Server, ensure that you select **Server Farm** installation and then select **Complete** Server Type installation (Microsoft SharePoint Server 2010 installer > Server Type tab).

  Note: The **Stand-alone** Server Type installation is not supported.

- VCS does not require you to install the SharePoint Server 2010 components on shared storage. You can install SharePoint to the local system disks.
- During configuration, for the database server name for the farm configuration database, specify the SQL Server that you configured for high availability earlier.

For installation and configuration instructions, see the Microsoft SharePoint Server documentation.

Configuring SharePoint Server service groups

Configuring the SharePoint Server service group involves the following tasks:

- creating a parallel service group for the SharePoint Web Applications running on the front-end Web servers
- creating service groups for SharePoint Service Applications or services locally on the application servers

Use the VCS SharePoint Server Configuration Wizard to create the required service groups and its resources and define the attribute values for the configured resources.

Note the following before you proceed:

- The wizard discovers the Web Applications, Service Applications, and services in the farm where the local node resides and then configures them in the service groups.
- The wizard automatically configures all the discovered SharePoint applications and services configured in the local cluster farm. You cannot choose applications or services for the service group configuration.

If you do not want to configure an application or a service, host it on a server outside the local cluster.

- The wizard has a single workflow that performs service group creation as well as modification tasks. If you wish to add or remove a SharePoint component from the configuration, you must run the wizard again.
  If you run the wizard after configuring the SharePoint service groups, the wizard modifies the existing service group configuration. The wizard rediscovers the SharePoint configuration in the farm and then adds or removes resources depending on the changes made.
  For example, if you add a node to the server farm, the wizard adds the required resources and service groups to the configuration. If an application is removed from the server farm, the wizard removes the corresponding resources from the service group and also updates the VCS configuration.
- If you have configured the Web Applications and Service Applications in different clusters, then you must run the configuration wizard once from a node in each cluster.
- After configuring the SharePoint service groups, you can add custom resources such as IP or NIC to monitor the network availability of the cluster nodes in the configuration. You can add these resources manually from the Cluster Manager (Java Console).
  If you run the wizard again, these custom resources are ignored.

Before you configure a SharePoint service group

Before you configure a SharePoint service group, do the following:

- Verify that you have installed the VCS agent for SharePoint Server 2010. If you have not installed it during SFW HA installation, use Windows Add or Remove Programs to install it.
  - In Add or Remove Programs, select **Veritas Storage Foundation 5.1 SP2 for Windows (Server Components)** and then click **Change** to launch the installer.
  - On the Mode Selection page select **Add or Remove**, and then click **Next**.
  - On the Option Selection panel choose **Veritas Cluster Server Application Agent for SharePoint Server 2010** under High Availability Application Agents.
  - Click **Next** and complete the installation.
- Verify that you have configured a cluster using the VCS Cluster Configuration Wizard (VCW).

- Verify that you have installed and configured SharePoint Server 2010 on all the nodes that will be part of the SharePoint service groups.
- Ensure that the SharePoint Server 2010 Timer service is running on all the nodes that will be part of the SharePoint service groups.
- Ensure that the Veritas Command Server service is running on all the nodes that will be part of the SharePoint service groups.
- Verify that the Veritas High Availability Daemon (HAD) is running on the system from where you run the VCS SharePoint Server Configuration Wizard.
- Ensure that you have VCS Cluster Administrator privileges. This privilege is required to configure service groups.
- Ensure that the logged-on user has SharePoint Server 2010 Farm Administrator privileges on the SharePoint Server.
- Ensure that you run the wizard from a node where SharePoint Server 2010 is installed and configured.
- 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*.

Creating a SharePoint service group

Complete the following steps to create a service group for SharePoint Server.

To create the SharePoint Server service group

1. Launch the VCS SharePoint Server Configuration Wizard.
   Click **Start > All Programs > Symantec > Veritas Cluster Server > Solutions Configuration Center** to start the Solutions Configuration Center (SCC). Expand the Solutions for SharePoint Server tab and click **High Availability (HA) Configuration > Configure SharePoint Server Service Groups > SharePoint 2010 Configuration Wizard**.
2. Review the information in the Welcome panel and click **Next**.

3 On the Farm Admin User Details panel, specify the SharePoint Farm Admin user credentials and then click **Next**.

Farm Name	Displays the name of the farm configuration database where the node resides.
Farm Admin User Name	Specify a user account that has Farm Admin privileges in the SharePoint farm where the current node resides. Click the ellipsis button to launch the Windows Select User dialog box and then specify the appropriate user account. The Farm Admin user account is used to manage the SharePoint applications and services configured in the SharePoint service groups in the cluster.
Password	Type the password of the user account specified in the Farm Admin User Name field. The wizard stores the user password in the VCS configuration in an encrypted form.

4 On the Web Applications Details panel, review the list of Web Applications that the wizard discovers in the farm and then click **Next**.
The wizard configures these Web Applications in a parallel service group. The wizard configures only those components that are part of the local cluster.

5 On the Service Applications Details panel, review the list of Service Applications and services that the wizard discovers in the farm and then click **Next**.
The wizard configures these Service Applications and services in a local service group on each node. The wizard configures only those components that are part of the local cluster.

6 On the Service Groups Summary panel, review the service group configuration, edit the service group and resource names if required, and then click **Next**.

Resources	Displays a list of configured service groups and its resources. The wizard assigns unique names to service group and resources. ■ For parallel service groups, the wizard uses the following naming convention: *FarmConfigurationDatabaseName-WebApplications* ■ For local service groups, the wizard uses the following naming convention: *FarmConfigurationDatabasename-NodeName-ServiceApps* You can edit resource names only in the create mode. You cannot modify names of service groups and resources that already exist in the configuration. To edit a 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.

7 Click **Yes** on the message that informs that the wizard will run commands to modify the service group configuration. The wizard starts running commands to create the service groups. Various messages indicate the status of these commands.

8 On the completion panel, check **Bring the service group online** check box to bring the SharePoint service groups online in the cluster, and then click **Finish**.
This completes the SharePoint service group configuration.

Verifying the SharePoint cluster configuration

Failover simulation is an important part of configuration testing. To verify the configuration in the cluster, you can take the service groups offline, or manually stop the configured applications on the active cluster node.

You can also simulate a local cluster failover for the SQL databases configured in the VCS SQL Server service group. Refer to the VCS SQL documentation for instructions.

Use Veritas Cluster Manager (Java Console) to perform all the service groups operations.

To take the service groups offline and bring them online

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 **Offline** and then choose the local system.
   - In the dialog box, click **Yes.** The service group you selected is taken offline on the node.
     If there is more than one service group, you must repeat this step until all the service groups are offline.
2. Verify that the applications and services configured in the service groups are in the stopped state.
3. To start all the stopped services, bring all the services groups online on the node.

To manually stop the configured applications and services

1. To verify that the SharePoint applications and services are properly configured with VCS, manually stop these components either from the SharePoint Central Administration console or from the IIS Manager.
2. From the IIS Manager, in the Connections pane on the left, select a configured Web site and then in the Actions pane on the right, click **Stop**. The status of the Web Site will show as stopped.
3. In the Cluster Manager (Java Console) the corresponding service group resource state may temporarily show as faulted as the SharePoint agent attempts to start the stopped application.
4. When the resource comes online, refresh the IIS Manager view to verify that the IIS site is in the started state.

Considerations when modifying a SharePoint service group

Note the following while modifying SharePoint service groups:

- The wizard has a single workflow that performs service group creation as well as modification tasks. If you wish to add or remove a SharePoint component from the configuration, you must run the wizard again.

If you run the wizard after configuring the SharePoint service groups, the wizard modifies the existing service group configuration. The wizard rediscovers the SharePoint configuration in the farm and then adds or removes resources depending on the changes made.

For example, if you add a node to the server farm, the wizard adds the required resources and service groups to the configuration. If an application is removed from the server farm, the wizard removes the corresponding resources from the service group and also updates the VCS configuration.

- 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.
- The wizard automatically configures all the discovered SharePoint applications and services configured in the local cluster farm. You cannot choose applications or services for the service group configuration.

  If you do not want an application or a service to be part of the configuration, host it on a server outside the local cluster.
- When you run the wizard after configuring the SharePoint service groups, the wizard ignores any custom resources that you may have added to the service groups. If you wish to add, remove, or modify those custom resources, you must do so manually. The wizard does not provide any options to modify custom resources.
- 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 VCS SharePoint Server Configuration Wizard on this node to configure the SharePoint services for it.

Chapter 8

Configuring disaster recovery for SharePoint Server 2010

This chapter contains the following topics:

Tasks for configuring disaster recovery for SharePoint Server 2010

After setting up an SFW HA high availability environment for a SharePoint Server 2010 farm on a primary site, you can create a secondary or “failover” site for disaster recovery.

In addition to configuring DR for the SQL Server components of the SharePoint farm, you can configure DR for SharePoint applications and services.

The following table lists the main tasks and sequence for configuring SharePoint applications and services for DR on the secondary site.

Table 8-1 Configuring the secondary site for disaster recovery

Action	Description
Configure SQL Server for disaster recovery at the secondary site	For the steps for configuring SQL Server for high availability and disaster recovery, see *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2000 and 2005* *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008 and 2008 R2*
Modify the SQL Server service group on the primary and secondary site	Edit the SQL Server service group on both the primary and secondary site to allow updating the NLB details if a disaster recovery failover occurs. See "Configuring the SQL Server service group for DR in the SharePoint environment" on page 103.
Verify that SharePoint has been configured for high availability at the primary site	Verify that SharePoint has been configured for high availability at the primary site. See Chapter 7, "Installing and configuring SharePoint Server 2010 for high availability".
Install SFW HA and configure the cluster on the secondary site	Install SFW HA on the SharePoint server systems on the secondary site. Ensure that you select the option to install the Veritas Cluster Server Application Agent for SharePoint Server 2010. You can optionally use the same SFW HA cluster for both SQL Server and SharePoint Server if all systems use the same operating system platform. Otherwise, create a separate cluster for SharePoint. See "Configuring the secondary site for SharePoint disaster recovery" on page 111.

Table 8-1 Configuring the secondary site for disaster recovery (Continued)

Action	Description
Install SharePoint on the cluster nodes on the secondary site	Install Microsoft SharePoint Server on the SharePoint servers on the secondary site. Run the Microsoft SharePoint Products Configuration wizard to add the servers to the existing primary site farm. Choose the option to connect to an existing server farm. **Note:** You do not need to configure the same number of web servers or service applications on the secondary site as on the primary site. However, you should provide for all required services.
Create the SharePoint service groups on the secondary site	Configure the SharePoint Server service groups for the secondary site The VCS SharePoint Server Configuration Wizard helps you create SharePoint Server service groups. See "Configuring SharePoint Server service groups" on page 94.
Verify the disaster recovery configuration	In the Veritas Cluster Server Java console, ensure that you can bring the SharePoint service groups online and offline.
Configure the Search service application for DR	Providing disaster recovery for the search service application includes configuring DR for the following components on the secondary site: Crawl component Query and indexing components Administration component Property and Administration databases See "Configuring the Search service application for disaster recovery" on page 112.

Configuring the SQL Server service group for DR in the SharePoint environment

To create the VCS SQL Server service group on the primary site, follow the instructions in the SQL Server solutions guide, as follows:

- *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL,* which covers SFW HA solutions for Microsoft SQL Server 2005

- *Veritas Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft SQL 2008 and 2008 R2*

After creating the SQL Server service group, you edit the default configuration of the service group to automate updating the Network Load Balancing (NLB) details when you switch between sites.

The following provide additional details:

- Edit the service group to change the attribute settings of the VCS Lanman agent resource.
  See "Updating the SQL Server IP address" on page 104.
- Optionally, depending on your environment, edit the service group to add a process resource that implements a VCS script to update the NLB details of the SharePoint farm. You must customize the script configuration settings file separately for each site.
  See "Updating the IP address for web requests" on page 105.

Updating the SQL Server IP address

You configure the VCS Lanman agent to update the DNS server with the virtual IP address for the SQL Server instance that is being brought online. The Lanman agent resource is created automatically as part of the SQL Server service group. However, you need to edit the default Lanman settings.

You must specify the following attribute settings for the Lanman agent, at a minimum:

DNSUpdate	True This setting causes the update of the SQL Server IP address on the DNS server.
DNSCriticalForOnline	True The server will not be able to come online if the DNS update is not successful.
DNSOptions	PurgeDuplicate Removes duplicate DNS entries from the DNS servers.

More information on Lanman agent settings is provided in the agent documentation.

See *Cluster Server Bundled Agents Reference Guide.*

The procedure shows how to edit the Lanman resource of an existing SQL Server service group from the VCS Cluster Manager Java Console. You do this after you

create the service group on the primary site and again on the secondary site after creating the service group there.

To configure the Lanman agent resource to update the SQL Server IP address

1. Start the Cluster Manager Java Console, log on to the cluster, and open the Cluster Explorer window (click anywhere in the active Cluster Monitor panel).
2. In the Cluster Explorer configuration tree, expand the SQL Server service group and expand **Lanman**.
3. Under Lanman, right-click the resource icon (labeled with the service group name and the “-Lanman" suffix) and click **View > Properties View**.
4. Expand the Properties View window as necessary to see all attributes under Type Specific Attributes.
5. Edit the following attribute settings by locating the row containing the setting, clicking the Edit icon in that row, and editing the setting as follows in the Edit Attribute dialog box. Leave Global (the default) enabled to apply the attribute to all nodes in the cluster. If initially prompted to switch to read/write mode, click **Yes**.

DNSUpdateRequired	Check DNSUpdateRequired and click **OK**.
DNSCriticalForOnline	Check DNSCriticalForOnline and click **OK**.
DNSOptions	Under Vector Values, click the plus icon to display the list, select **PurgeDuplicate** and click **OK**.

6. If your site uses additional DNS servers, edit the setting for AdditionalDNSServers to specify the IP addresses.
7. In the Cluster Explorer window, click **File > Save Configuration**, and then click **File > Close Configuration**.
8. If you are configuring a resource for the web servers, continue with that procedure; otherwise, log off the cluster and exit the Cluster Manager.
   See “Configuring a resource for the web servers” on page 108.

Updating the IP address for web requests

You can configure VCS to update the DNS server with a site-specific IP address for the SharePoint NLB. This update occurs as part of the process of bringing the SQL Server service group online.

To automate this, you configure a VCS process resource as part of the SQL Server service group. You configure the resource after you create the service

group on the primary site and you repeat the procedure on the service group that you create on the secondary site.

See "Configuring a resource for the web servers" on page 108.

The process resource uses Perl scripts. The scripts read information from a configuration settings file that you must customize separately for each site.

See "Customizing the DNS update settings for the web servers" on page 107.

Requirements

The DNS update script files are available in the following directory:

```
%VCS_HOME%\bin\SQLServer2008
```

The files consist of the following:

- dnsupdate-online.pl
- dnsupdate-offline.pl
- dnsupdate-monitor.pl
- dnsupdate-settings.txt

You customize the settings file for your environment. You need two copies of the settings file, one with settings for the primary site and one with settings for the secondary site.

See "Customizing the DNS update settings for the web servers" on page 107.

After customizing the settings file for each site, place the script files and the appropriate settings file for the site in a location where they are available from the cluster nodes. Since you specify the file names and locations as part of the service group process resource, you can choose the file names and locations. To avoid editing the service group again on the secondary site, you must use the same names and locations on both sites.

Warning: Do not place the settings file on a replicated volume. Otherwise, the active site's settings file would overwrite the passive site's settings file during replication.

In addition, the scripts require the Dnscmd.exe command line tool. Dnscmd.exe is installed as part of the Windows Server 2008 DNS Server Tools feature.

The scripts log to the engine log. The name of the log is engine_A.txt.

Customizing the DNS update settings for the web servers

You customize the settings file dnsupdate-settings.txt with the values required by the script used to update the DNS server. For each keyword (in brackets) you enter a value.

Table 8-2 describes the contents of the settings file.

Table 8-2 DNS update settings file

Keyword	Value	Notes
[web alias]	The web server (or NLB) name	Same in both setting files
[local ip]	Comma delimited pair of IP addresses: IP address for the web server or NLB on this site, IP address for the DNS server to be updated Example: 192.168.1.2, 192.168.10.10	When editing the primary site settings file, the local IP is that of the primary site web server or NLB. For the secondary site file, the local IP is that of the secondary site web server or NLB. If you have additional IP addresses for additional web servers or DNS servers, enter them as a comma delimited pair on separate lines.
[remote ip]	Comma delimited pair of IP addresses: IP address for the web server or NLB on the remote site, IP address of the DNS server to be updated Example: 192.168.1.1, 192.168.10.10	When editing the primary site settings file, the remote IP is that of the secondary site web server or NLB. For the secondary site file, the remote IP is that of the primary site web server or NLB. The DNS server to be updated is the one that manages the IP address for the web server or NLB. If you have additional IP addresses for additional web servers or DNS servers, enter them as a comma delimited pair on on separate lines.

Table 8-2 DNS update settings file

Keyword	Value	Notes
[dns command]	Path to the location of DNScmd.exe Example: \Windows\System32\dnscmd.exe	By default, on Windows Server 2008, the script will look for DNScmd.exe in \Windows\System32\dnscmd.exe on the drive where SFW HA is installed, unless you specify another value.
[domain name]	Fully qualified domain of the web server Example: symantecdomain.com	Same in both settings files
[nslookup command]	Full path for nslookup.exe Example: \Windows\System32\nslookup.exe	By default, the script will look for nslookup.exe on the drive where SFW HA is installed in the default directory shown, unless you specify another value.

Configuring a resource for the web servers

You can add a process resource to the SQL Server service group to enable switching to the web servers at the site where the SQL Server service group is brought online. The process resource executes a Perl script to update the DNS server IP address for the web servers.

You add the process resource after you create the service group on the primary site. After you create the service group on the secondary site, you add the process resource to that service group as well.

The procedure shows how to add a resource using the Java Console. You can also use other methods, as described in the VCS documentation.

See *Veritas Cluster Server Administrator's Guide*.

Verify that the Perl executable, the scripts, and the customized settings file is available from the systems on which the service group is configured.

In addition, ensure that DNScmd.exe is installed to the same drive as the SFW HA application.

To configure a resource for the web servers

1. Start the Cluster Manager Java Console, log on to the cluster, and open the Cluster Explorer window (click anywhere in the active Cluster Monitor panel).
2. In the Cluster Explorer configuration tree, right-click the name of the SQL service group and click **Add Resource**. If prompted to switch to read-write mode, click **Yes**.
3. In the Add Resource dialog box, specify a name for the resource and in the Resource Type list, click **Process**.
4. Edit the following process resource attributes:

StartProgram	The full path names of the following, in the order shown, separated by spaces: ■ The Perl script executable ■ The dnsupdate-online script ■ The script settings file Example: c:\Program Files\Veritas\VRTSPerl\bin\perl.exe c:\bin\dnsupdate-online.pl c:\bin\dnsupdate-settings.txt
StopProgram	The full path names of the following, in the order shown, separated by spaces: ■ The Perl script executable ■ The dnsupdate-offline script ■ The script settings file Example: c:\Program Files\Veritas\VRTSPerl\bin\perl.exe c:\bin\dnsupdate-offline.pl c:\bin\dnsupdate-settings.txt
MonitorProgram	The full path names of the following, in the order shown, separated by spaces: ■ The Perl script executable ■ The dnsupdate-monitor script ■ The script settings file Example: c:\Program Files\Veritas\VRTSPerl\bin\perl.exe c:\bin\dnsupdate-monitor.pl c:\bin\dnsupdate-settings.txt
UserName	The name of the user account to run the script. The account must have access and change rights to the DNS server.
Password	The password for the user account.

Domain	The domain name for that user account.

5 In the Add Resource dialog box, check **Enabled** and click **OK**.

6 In the Resource view, right-click the process resource you just created and click **Link**.

7 On the Link Resources dialog box, in the list of resources, select the name of the SQL Server resource and click **OK**.

8 In the Cluster Explorer window, click **File > Save Configuration**, and then click **File > Close Configuration**.

Configuring the secondary site for SharePoint disaster recovery

See the following topics:

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.

- Ensure that you have configured the SharePoint Server systems for the SFW HA cluster.
  See "Configuring the storage hardware and network" on page 66.
- If you have not yet done so, install SFW HA on the SharePoint Server systems. Ensure that when installing SFW HA on the SharePoint systems, you select the option to install the Veritas Cluster Server Application Agent for SharePoint Server 2010.
- If both SQL Server and SharePoint Server systems use the same operating system platform, you can optionally use the same SFW HA cluster for both. In such a case, you can add the SharePoint Server systems to the existing SQL Server cluster on the secondary site. Otherwise, create a separate cluster for the SharePoint systems on the secondary site.
  - See the following:
    "Configuring the cluster" on page 72
    "Adding nodes to an existing cluster" on page 86

Installing the SharePoint servers on the secondary site

When you install the SharePoint servers on the secondary site, ensure that you select the installation option that allows you to add the servers to the existing primary site farm. During configuration with the Microsoft SharePoint Products

Configuration Wizard, on the Connect to a server farm panel, select the option to connect to an existing server farm.

You do not need to configure the same number of SharePoint web servers or application servers on the secondary site as on the primary site. However, you should provide for all required services to be available on the secondary site.

Configuring the SharePoint service groups on the secondary site

Run the VCS SharePoint Server Configuration Wizard from a SharePoint server system on the secondary site. Configure the SharePoint Server service groups for the secondary site using the same process as on the primary site. The SharePoint Server service groups can be online on both the primary and secondary site.

See "Configuring SharePoint Server service groups" on page 94.

Verifying the service group configuration

In the Veritas Cluster Server Java console, ensure that you can bring the SharePoint service groups online and offline.

For information on bringing service groups online and offline, see the *Veritas Cluster Server Administrator's Guide*

Configuring the Search service application for disaster recovery

Providing disaster recovery for the search service application includes configuring DR for the following components on the secondary site:

- Crawl component
- Query and indexing components
- Administration component
- Property and Administration databases

The following table describes the tasks you perform on the secondary site for providing DR for each component.

Table 8-3 DR for Search application service

Component	Task
Crawl component	Create a new Crawl component on the secondary site servers for each service application topology for which you need to provide DR. If the primary site crawl components fail, the secondary site crawl components will provide the crawling functionality to the farm.
Query component	Create a mirror Query component on the secondary site servers for each Query component in the index partitions. Mark these mirrors as FailOverOnly. If all the index partitions on the primary site fail, the secondary site will provide the index server functionality to the farm.

Administration component	Each Search service application topology has a single Administration component. You can use Windows Powershell cmdlets to change the system on which the Administration component is running. For example, if the primary site fails, you would run the cmdlets on a system on the secondary site.
	On the server on which you want to run the Administration component, execute the following Windows Powershell commands for each search service application:
	`$searchapp = Get-SPEnterpriseSearchServiceApplication "Search service application name"`
	`$admin = Get-SPEnterpriseSearchAdministrationComponent -SearchApplication $searchapp`
	`$admin | Set-SPEnterpriseSearchAdministrationComponent -SearchServiceInstance Target System Name -Force`

Property and Administration databases	Configuring disaster recovery for SQL Server ensures that the Property and Administration databases are available on the secondary site.

Index

L

N

P

R

S

T

V

W