

Symantec Storage Foundation™ and High Availability Solutions Microsoft Clustering Solutions Guide for Microsoft Exchange 2007

Windows

6.1

Symantec Storage Foundation™ and High Availability Solutions Microsoft Clustering Solutions Guide for Microsoft Exchange 2007

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

Product version: 6.1

Document version: 6.1 Rev 0

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. See the Third-party Legal Notices document for this product, which is available online or included in the base release media.

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

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

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

disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

About Symantec Connect

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

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

Documentation

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

doc_feedback@symantec.com

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

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

Contents

Technical Support	4	
Chapter 1	Introducing SFW solutions for a Microsoft cluster	10
	About Microsoft clustering solutions with SFW	10
	Advantages of using SFW in a Microsoft cluster	11
	About high availability clusters	11
	About campus clusters	12
	About disaster recovery clusters	13
	About the solutions guides for Exchange Server	15
Chapter 2	Workflows for deploying Exchange Server with SFW in a Microsoft cluster	16
	Workflow for a high availability (HA) configuration	16
	Workflow for a campus cluster configuration	18
	Workflow for a disaster recovery configuration	22
	Using the Solutions Configuration Center workflow	24
Chapter 3	Planning for deploying Exchange Server with SFW in a Microsoft cluster	26
	Requirements for deploying Exchange Server with SFW in a Microsoft cluster	26
	Supported software	26
	Disk space requirements for SFW	28
	System requirements for Microsoft clustering solutions	28
	Additional SFW installation requirements for a Microsoft cluster	29
	Planning your Exchange Server high availability configuration	30
	Configuring the quorum device for high availability	31
	Planning your campus cluster configuration	31
	Microsoft campus cluster failure scenarios	34
	Microsoft cluster quorum and quorum arbitration	36
	Planning your disaster recovery configuration	38

Chapter 4	Installing SFW with Microsoft clustering	42
	Tasks for installing and configuring SFW with Microsoft clustering	42
	Configuring the storage hardware and network	43
	Establishing a Microsoft failover cluster	44
	Campus cluster: Connecting the two nodes	45
	Installing SFW with Microsoft Failover Cluster option	45
Chapter 5	Configuring SFW storage	47
	Tasks for configuring SFW storage	47
	Planning for SFW cluster disk groups and volumes	48
	Sample Exchange Server high availability cluster storage configuration	50
	Sample campus cluster storage configuration	51
	Considerations when creating disk groups and volumes for a campus cluster	51
	Considerations when creating volumes for a DR configuration using Volume Replicator replication	53
	Viewing the available disk storage	53
	Creating dynamic cluster disk groups	54
	Adding disks to campus cluster sites	56
	Creating dynamic volumes for high availability clusters	57
	Creating dynamic volumes for campus clusters	62
	Managing disk group and volumes	69
	Importing a disk group and mounting a volume	70
	Unmounting a volume and deporting a disk group	70
Chapter 6	Implementing a dynamic mirrored quorum resource	72
	Tasks for implementing a dynamic mirrored quorum resource	72
	Creating a dynamic cluster disk group and a mirrored volume for the quorum resource	73
	Adding a Volume Manager Disk Group resource for the quorum	74
	Changing the quorum resource to a dynamic mirrored quorum resource	75
Chapter 7	Installing Exchange Server and configuring resources	76
	Tasks for installing and configuring Exchange Server	76
	Adding a Volume Manager Disk Group resource for Exchange 2007 installation	77

Installing Exchange Server	78
Adding the Volume Manager Disk Group resources to the Exchange group	79
Setting the database dependency on the disk group resource	80
Moving Exchange databases and logs to shared storage	80
Verifying the Exchange Server group in the Microsoft cluster	82
 Chapter 8 Configuring disaster recovery for Exchange Server in a Microsoft cluster	 83
Tasks for configuring the secondary site for disaster recovery for Exchange	84
Verifying the primary site configuration	85
Creating a parallel environment for Exchange Server on the secondary site	85
Installing Exchange on the secondary site	87
Setting up the Exchange group on the secondary site	88
Volume Replicator components overview	89
Setting up security for Volume Replicator	90
Creating resources for Volume Replicator	92
Configuring Volume Replicator: Setting up an RDS	93
Prerequisites for setting up the RDS	93
Creating a Replicated Data Set (RDS)	94
Creating the RVG resource	104
Setting the Exchange server resource dependency on the RVG resource	105
Normal Volume Replicator operations and recovery procedures	106
Monitoring the status of the replication	106
Performing planned migration	106
Replication recovery procedures	107
 Index	 110

Introducing SFW solutions for a Microsoft cluster

This chapter includes the following topics:

- [About Microsoft clustering solutions with SFW](#)
- [Advantages of using SFW in a Microsoft cluster](#)
- [About high availability clusters](#)
- [About campus clusters](#)
- [About disaster recovery clusters](#)
- [About the solutions guides for Exchange Server](#)

About Microsoft clustering solutions with SFW

Microsoft clustering may be used with Symantec Storage Foundation for Windows (SFW) to provide the following solutions:

- High availability failover cluster in an active/passive configuration on the same site
- Campus cluster, in a two-node configuration with each node on a separate site
- Disaster recovery with a separate cluster on a Secondary site, with replication support using Volume Replicator

The example configurations do not include Dynamic Multi-pathing (DMP).

For instructions on how to add DMP to a clustering configuration, see *Symantec Dynamic Multi-Pathing for Windows Solutions Guide* .

Advantages of using SFW in a Microsoft cluster

One of the key advantages of using SFW with Microsoft clustering is the ability to create a mirrored quorum resource that adds fault tolerance to the quorum and protects the cluster. Microsoft clustering uses the quorum architecture, where the cluster database resides in the quorum resource. The quorum resource maintains the cluster database and critical recovery information in a recovery log.

Adding SFW to the configuration protects the quorum disk from being a single point of failure in the cluster because SFW provides dynamic volumes and software mirroring of the quorum device. If the quorum resource fails, the mirror takes over for the resource.

Using SFW also offers other advantages over using Microsoft clustering alone. SFW lets you add fault tolerance to your data volumes. Mirroring of log volumes is recommended, and a mirrored striped RAID layout is recommended for your data volumes. SFW also offers multiple disk groups, multiple mirrors, capacity management and Automatic Volume Growth, online storage migration, performance tuning, hot relocation, dirty region logging, RAID-5 logging, Dynamic Multi-pathing, and enhanced snapshot capabilities with FlashSnap.

About high availability clusters

A high availability solution maintains continued functioning of applications in the event of computer failure, where data and applications are available using redundant software and hardware. High availability can refer to any software or hardware that provides fault tolerance, but generally it has become associated with clustering.

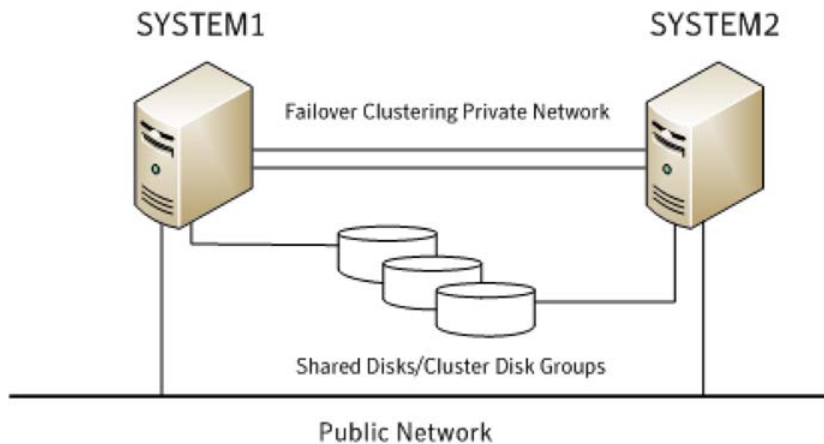
A cluster is a group of independent computers working together as a single system to ensure that mission-critical applications and resources are highly available. The cluster is managed as a single system, shares a common namespace, and is specifically designed to tolerate component failures and to support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

Clustered systems have several advantages, including fault tolerance, high availability, scalability, simplified management, and support for rolling upgrades.

In a high availability cluster with Symantec Storage Foundation for Windows, you configure dynamic cluster disk groups and volumes for the application on shared storage and install the application database and log to the appropriate SFW volumes.

Figure 1-1 shows an example of a two-node high-availability configuration.

Figure 1-1 High availability active/passive configuration



About campus clusters

Campus clusters are multiple-node clusters that provide protection against disasters. The nodes can be located in separate buildings miles apart. Nodes are located within a single subnet and connected by a Fibre Channel SAN. Each node has its own storage array and contains mirrored data of the storage on the other array.

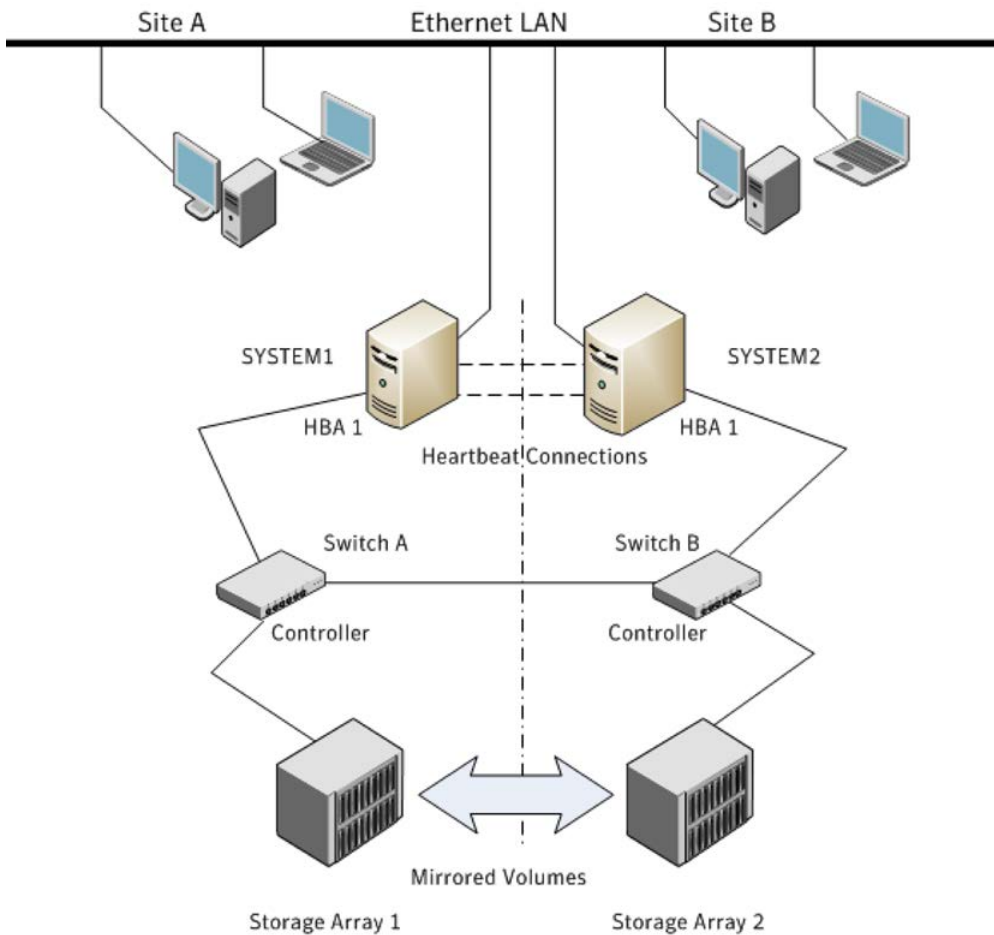
Typical campus clusters involve two sites; you can use more than two sites for additional redundancy.

This environment also provides a simpler solution for disaster recovery than a more elaborate Symantec disaster recovery environment with replication software; however, a campus cluster generally stretches a shorter distance than a replication-based solution depending on the hardware.

Both local clusters and campus clusters have SFW dynamic disk groups and volumes, but the volumes on each campus cluster node are mirrors of one another. Each disk group should contain the same number of disks on each site for the mirrored volumes.

Figure 1-2 shows an example of a two-node campus cluster configuration.

Figure 1-2 Campus cluster configuration



About disaster recovery clusters

A typical disaster recovery configuration requires that you have a source host on the Primary site and a destination host on the Secondary site. The application data is stored on the Primary site and replicated to the Secondary site by using a tool such as the Volume Replicator. The Primary site provides data and services during normal operation. If a disaster occurs on the Primary site and its data is destroyed, a Secondary host can take over the role of the Primary host to make the data accessible. The application can be restarted on that host.

Using Volume Replicator with Microsoft clustering provides a replicated backup of your application data, which can be used for recovery after an outage or disaster. However, this solution does not provide the automated failover capability for disaster recovery that can be achieved using Volume Replicator with Symantec Cluster Server (VCS).

In a typical clustered Volume Replicator configuration 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. In a Microsoft cluster environment, each site has its own quorum volume.

If the 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 (for instance, after an earthquake that destroys the datacenter in which the Primary site resides), the replication solution is activated. If there is a disaster at the Primary site, SYSTEM3 at the Secondary site takes over. The data that was replicated to the Secondary site is used to restore the application services to clients.

Figure 1-3 shows an example disaster recovery configuration before a failure.

Figure 1-3 Disaster recovery configuration

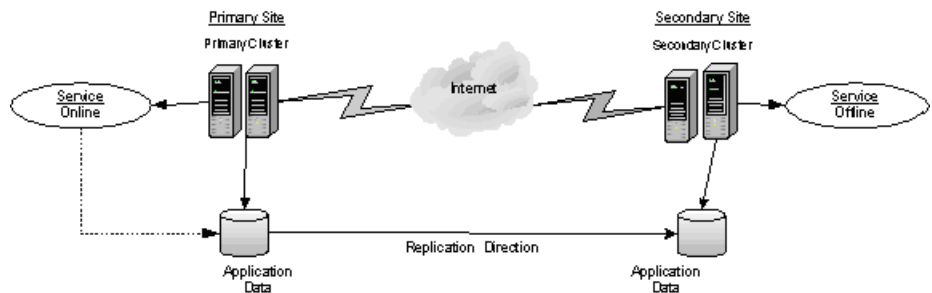
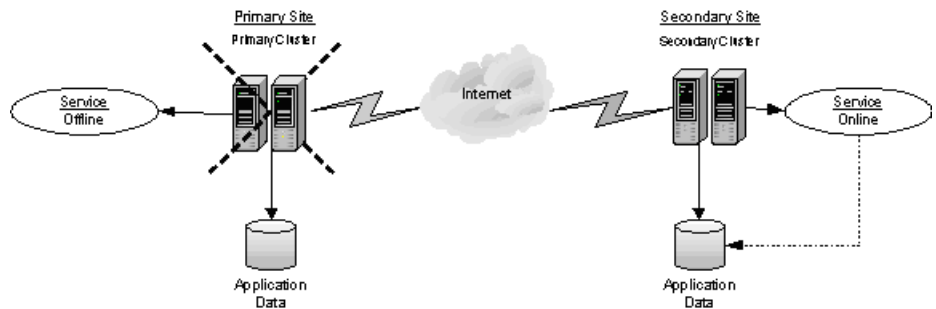


Figure 1-4 shows an example disaster recovery configuration after a failure.

Figure 1-4 Disaster recovery after a failure



About the solutions guides for Exchange Server

Table 1-1 shows the available Symantec Storage Foundation and High Availability Solutions solutions guides for Exchange Server. Separate guides are available for Microsoft SQL, Enterprise Vault, and additional application solutions.

Table 1-1 SFW HA solutions guides for Exchange Server

Title	Description
<i>Symantec Storage Foundation and High Availability Solutions HA and Disaster Recovery Solutions Guide for Microsoft Exchange 2007 and 2010</i>	Solutions for Exchange Server 2007 and 2010 and Symantec Cluster Server clustering with Symantec Storage Foundation and High Availability Solutions: ■ High availability (HA) ■ Campus clusters ■ Replicated data clusters ■ Disaster recovery (DR) with Symantec Storage Foundation Volume Replicator or hardware array replication
<i>Symantec Storage Foundation and High Availability Solutions Quick Recovery Solutions Guide for Microsoft Exchange 2007 and 2010</i>	Quick Recovery solutions for Exchange Server 2007 and 2010 using either Symantec Storage Foundation for Windows or Symantec Storage Foundation and High Availability Solutions.
<i>Symantec Storage Foundation and High Availability Solutions Microsoft Clustering Solutions Guide for Microsoft Exchange 2007</i>	Solutions for Exchange Server 2007 and Microsoft clustering with Symantec Storage Foundation for Windows: ■ High availability (HA) ■ Campus clusters ■ Disaster recovery (DR) with Symantec Storage Foundation Volume Replicator

Workflows for deploying Exchange Server with SFW in a Microsoft cluster

This chapter includes the following topics:

- [Workflow for a high availability \(HA\) configuration](#)
- [Workflow for a campus cluster configuration](#)
- [Workflow for a disaster recovery configuration](#)
- [Using the Solutions Configuration Center workflow](#)

Workflow for a high availability (HA) configuration

You can install and configure Storage Foundation for Windows (SFW) and Exchange Server in a Microsoft cluster for high availability on a single site.

Table 2-1 Process for deploying Exchange Server with SFW in a Microsoft high-availability cluster

Action	Description
Verify hardware and software prerequisites	See “Requirements for deploying Exchange Server with SFW in a Microsoft cluster” on page 26.
Understand the configuration	See “Planning your Exchange Server high availability configuration” on page 30.

Table 2-1 Process for deploying Exchange Server with SFW in a Microsoft high-availability cluster (*continued*)

Action	Description
Configure the storage hardware and network	- Set up the storage hardware for a cluster environment. - Verify the DNS entries for the systems on which Exchange will be installed. See “Configuring the storage hardware and network” on page 43.
Establish a Microsoft cluster	Establish the cluster before installing SFW. See “Establishing a Microsoft failover cluster” on page 44.
Install SFW with the Microsoft Failover Cluster option	Perform a rolling installation. See “Installing SFW with Microsoft Failover Cluster option” on page 45. Ensure that you select the following options during installation of SFW: - Select the option to install SFW. - On the product options screen, select the option to install Cluster Option for Microsoft Failover Cluster. - Verify that the Symantec Storage Foundation for Windows (Client Components) check box is checked, to install the client component. - If you plan to set up a secondary site for disaster recovery with Volume Replicator, install the Symantec Storage Foundation Volume Replicator option.
Configure and manage disk groups and volumes	Use the VEA console to create disk groups and volumes for the application and for the quorum resource. See “Tasks for configuring SFW storage” on page 47. Note: Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. To use these disks when you create your SFW cluster disk groups, you must first remove the physical disk resources from the cluster. Otherwise, a reservation conflict occurs.

Table 2-1 Process for deploying Exchange Server with SFW in a Microsoft high-availability cluster (*continued*)

Action	Description
Implement a dynamic mirrored quorum resource	■ Create a dynamic cluster disk group with a mirrored volume for the quorum disks. ■ Create a Volume Manager Disk Group (VMDG) resource for the quorum disk group. ■ Change the cluster quorum resource to the dynamic mirrored quorum resource. See “Tasks for implementing a dynamic mirrored quorum resource” on page 72.
Add the VMDG Resource for the First Storage group to the quorum group	Add the VMDG disk group resource(s) for the First Storage Group to the quorum group. See “Adding a Volume Manager Disk Group resource for Exchange 2007 installation” on page 77.
Install Exchange Server	See “Installing Exchange Server” on page 78.
Add the VMDG resources to the Exchange group	See “Adding the Volume Manager Disk Group resources to the Exchange group” on page 79.
Set the database dependency on the disk group resource	See “Setting the database dependency on the disk group resource” on page 80.
Move Exchange databases and logs to shared storage.	See “Moving Exchange databases and logs to shared storage” on page 80.
Verify the cluster configuration	Move the online Exchange Server cluster group to the second node and back to the first node. See “Verifying the Exchange Server group in the Microsoft cluster” on page 82.

Workflow for a campus cluster configuration

You can install and configure Storage Foundation for Windows (SFW) and Exchange Server in a Microsoft campus cluster.

This configuration workflow describes a two-node campus cluster with each node at a separate site.

The procedures for setting up a campus cluster are nearly the same as those for local clusters, with the following differences:

- A campus cluster has the nodes located in separate buildings. Therefore, the hardware setup requires SAN interconnects that allow these connections.
- In a campus cluster, each node has its own storage array rather than having a shared storage array between the two clusters.
- Both local clusters and campus clusters have SFW dynamic disk groups and volumes, but the volumes on each campus cluster node are mirrors of one another. Each disk group must contain the same number of disks on each site for the mirrored volumes.
- For campus clusters, you enable site allocation, assigning disks to one or the other campus cluster sites.

Table 2-2 Process for deploying Exchange Server with SFW in a Microsoft campus cluster

Action	Description
Verify hardware and software prerequisites	See “Requirements for deploying Exchange Server with SFW in a Microsoft cluster” on page 26.
Understand the configuration	See “Planning your campus cluster configuration” on page 31.
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment. ■ Verify the DNS entries for the systems on which Exchange will be installed. See “Configuring the storage hardware and network” on page 43.
Establish a Microsoft cluster	See “Establishing a Microsoft failover cluster” on page 44. Connect the two campus cluster nodes after setting up the Microsoft cluster. See “Campus cluster: Connecting the two nodes” on page 45.

Table 2-2 Process for deploying Exchange Server with SFW in a Microsoft campus cluster (*continued*)

Action	Description
Install SFW with the Microsoft Failover Cluster option	Perform a rolling installation. See “Installing SFW with Microsoft Failover Cluster option” on page 45. Ensure that you select the following options during SFW installation: ■ Select the option to install SFW. ■ On the product options screen, select the option to install Cluster Option for Microsoft Failover Cluster. ■ Verify that the Symantec Storage Foundation for Windows (Client Components) check box is checked, to install the client component.
Configure and manage disk groups and volumes	■ Use the VEA console to create disk groups and volumes for the application and for the quorum resource. See “Tasks for configuring SFW storage” on page 47. Ensure that the disk group you configure on each site contains the same number of disks and that you configure mirrored volumes. See “Considerations when creating disk groups and volumes for a campus cluster” on page 51. After creating the disk group, add the disks to a campus cluster site to enable site allocation. See “Adding disks to campus cluster sites” on page 56. Note: Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. To use these disks when you create your SFW cluster disk groups, you must first remove the physical disk resources from the cluster. Otherwise, a reservation conflict occurs.
Implement a dynamic mirrored quorum resource	■ Create a dynamic cluster disk group with a mirrored volume for the quorum disks. ■ Create a Volume Manager Disk Group (VMDG) resource for the quorum disk group. ■ Change the cluster quorum resource to the dynamic mirrored quorum resource. See “Tasks for implementing a dynamic mirrored quorum resource” on page 72.

Table 2-2 Process for deploying Exchange Server with SFW in a Microsoft campus cluster (*continued*)

Action	Description
Add the VMDG Resource for the First Storage group	Add the VMDG disk group resource(s) for the First Storage Group to the quorum group. See “Adding a Volume Manager Disk Group resource for Exchange 2007 installation” on page 77.
Install Exchange Server	See “Installing Exchange Server” on page 78.
Add the VMDG resources to the Exchange group	See “Adding the Volume Manager Disk Group resources to the Exchange group” on page 79.
Set the database dependency on the disk group resource	See “Setting the database dependency on the disk group resource” on page 80.
Move Exchange databases and logs to shared storage.	See “Moving Exchange databases and logs to shared storage” on page 80.
Create a group for the application in the failover cluster	■ Create a group within the failover cluster for the application. ■ Include the cluster disk group or groups for the application as Volume Manager Disk Group type resources in the group.
Install the application on cluster nodes	■ Install the application program files on the local drive of the first node. ■ Install files relating to the data and logs on the shared storage. ■ Move the cluster resources to the second node. ■ Make sure that the volumes on the second node have the same drive letters or mount points that they had on the first node. ■ Install the application on the second node.
Complete the setup of the application group in the failover cluster	■ Refer to the application documentation for help on creating its resource. ■ Establish the appropriate dependencies.
Verify the cluster configuration	Move the online Exchange Server cluster group to the second node and back to the first node. See “Verifying the Exchange Server group in the Microsoft cluster” on page 82.

Workflow for a disaster recovery configuration

After creating a high-availability cluster on a primary site, you can install and configure Storage Foundation for Windows (SFW) and Exchange Server on a secondary site cluster for disaster recovery.

This disaster recovery solution requires Volume Replicator.

Table 2-3 Process for deploying Exchange Server with SFW and Volume Replicator for disaster recovery in a Microsoft cluster

Action	Description
Ensure that you have set up the primary site for high availability, including the required options for disaster recovery	For details on setting up high-availability on the primary site: See “Workflow for a high availability (HA) configuration” on page 16. For a disaster recovery configuration, you must install the Volume Replicator option on the primary as well as the secondary site. Ensure that you are using static IP addresses as required for Volume Replicator.
Review the prerequisites and planning information	Verify the prerequisites on the secondary site. See “Requirements for deploying Exchange Server with SFW in a Microsoft cluster” on page 26. Note: If the DR site is on a different network segment, ensure that you allocate two IP addresses for the virtual server, one for the primary site and one for the DR site. Understand the DR configuration. See “Planning your disaster recovery configuration” on page 38.
Review how to create a parallel high availability configuration on the secondary site	Ensure that you follow the secondary site requirements and guidelines for IP addresses, disk groups and volumes, the Exchange Server resource group, and Exchange Server installation. See “Creating a parallel environment for Exchange Server on the secondary site” on page 85.
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment. ■ Verify the DNS entries for the systems on which Exchange will be installed. See “Configuring the storage hardware and network” on page 43.

Table 2-3 Process for deploying Exchange Server with SFW and Volume Replicator for disaster recovery in a Microsoft cluster (*continued*)

Action	Description
Establish a Microsoft cluster	Establish the cluster before installing SFW. See “Establishing a Microsoft failover cluster” on page 44.
Install SFW with the Microsoft Failover Cluster option	Perform a rolling installation. See “Installing SFW with Microsoft Failover Cluster option” on page 45. Ensure that you select the following options during SFW installation: ■ Select the option to install SFW. ■ On the product options screen, select the option to install Cluster Option for Microsoft Failover Cluster. ■ On the product options screen, select the option to install Volume Replicator. ■ Verify that the Symantec Storage Foundation for Windows (Client Components) check box is checked, to install the client component.
Configure and manage disk groups and volumes	■ Use the VEA console to create disk groups and volumes. Make sure the following is exactly the same as the cluster on the primary site: - Disk group name - Volume names and sizes - Drive letters See “Tasks for configuring SFW storage” on page 47. Note: Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. To use these disks when you create your SFW cluster disk groups, you must first remove the physical disk resources from the cluster. Otherwise, a reservation conflict occurs.
Implement a dynamic mirrored quorum resource	■ Create a dynamic cluster disk group with a mirrored volume for the quorum disks. ■ Create a Volume Manager Disk Group (VMDG) resource for the quorum disk group. ■ Change the cluster quorum resource to the dynamic mirrored quorum resource. See “Tasks for implementing a dynamic mirrored quorum resource” on page 72.

Table 2-3 Process for deploying Exchange Server with SFW and Volume Replicator for disaster recovery in a Microsoft cluster (*continued*)

Action	Description
Create the parallel Microsoft cluster configuration with SFW and Exchange 2007 on the secondary site	Many procedures are the same as on the primary site. However, there is a different procedure for installing Exchange and setting up the Exchange resource group. See “Creating a parallel environment for Exchange Server on the secondary site” on page 85.
Set up security for Volume Replicator	Set up the security for Volume Replicator on all nodes on both the primary and secondary sites. See “Setting up security for Volume Replicator” on page 90.
Understand the Volume Replicator components	See “Volume Replicator components overview” on page 89.
Create the cluster resources for Volume Replicator	■ Create an IP address for the Replicated Volume Group (RVG). ■ Create a Network Name resource for the Replicated Volume Group (RVG). See “Creating resources for Volume Replicator” on page 92.
Set up an RDS	Create a replicated data set (RDS) using the Volume Replicator wizard. See “Configuring Volume Replicator: Setting up an RDS” on page 93.
Create the RVG resource (primary and secondary sites)	Create the RVG resource on both primary and secondary sites. See “Creating the RVG resource” on page 104.
Set up the Exchange Server resource dependencies	Change the Exchange Server resource dependency properties so that it depends on the RVG resource instead of the Volume Manager Disk Group resource. See “Setting the Exchange server resource dependency on the RVG resource” on page 105.

Using the Solutions Configuration Center workflow

The SFW HA product includes a Solutions Configuration Center for various application and configuration solutions.

For Microsoft clustering, the campus cluster configuration solution is available as a workflow on the Configuration Center, with online help linking to the appropriate topics.

To use the Microsoft campus cluster workflow in the Solutions Configuration Center

- 1 Start the Solutions Configuration Center in one of the following ways:
 - From **Start > Programs > Symantec > Symantec Storage Foundation > Solutions Configuration Center** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
 - From the **Start** menu (the **Start** screen on Windows 2012 operating systems), type **Run**, and then press **Enter** to open the **Run** dialog box. In the **Run** dialog box, type **scc**, and then click **OK**.
- 2 Click to expand Solutions for Microsoft Exchange Server.
- 3 Click to expand the Microsoft Campus Cluster workflow.

Planning for deploying Exchange Server with SFW in a Microsoft cluster

This chapter includes the following topics:

- [Requirements for deploying Exchange Server with SFW in a Microsoft cluster](#)
- [Planning your Exchange Server high availability configuration](#)
- [Planning your campus cluster configuration](#)
- [Planning your disaster recovery configuration](#)

Requirements for deploying Exchange Server with SFW in a Microsoft cluster

Verify the requirements for your configuration before deploying Exchange Server with SFW in a Microsoft cluster.

Supported software

For the latest information on hardware and software supported for Symantec Storage Foundation for Windows (SFW) and Symantec Storage Foundation HA for Windows (SFW HA), see the following compatibility lists:

- For the Hardware Compatibility List (HCL):
<http://www.symantec.com/docs/TECH208993>
- For the Software Compatibility List (SCL):

<http://www.symantec.com/docs/TECH209010>

For deploying SFW in a Microsoft cluster, include the following option during SFW installation:

- Cluster Option for Microsoft Failover Cluster

For a DR configuration with Volume Replicator, include the following option during installation:

- Volume Replicator option

Supported Exchange Server 2007 versions

Note: For Exchange 2007, you can only cluster the Mailbox server role. Refer to the Microsoft documentation for other Exchange requirements.

Table 3-1 lists the Microsoft Exchange 2007 versions supported in this release of SFW HA.

Table 3-1 Microsoft Exchange Server 2007 supported environments

Microsoft Exchange Server 2007	Windows Servers
Microsoft Exchange Server 2007 SP1, SP2, or SP3 Standard or Enterprise Edition (Mailbox server role required)	■ Windows Server 2008 x64 Editions (for AMD64 or Intel EM64T): Standard, Enterprise, or Datacenter Edition ■ Windows Server 2008 R2 without Hyper-V on Standard, Enterprise, Datacenter Editions ■ Windows Server 2008 R2 on Standard, Enterprise, Datacenter Editions (for physical host or guest, not parent partition/Hyper-V integration) ■ Windows Server 2008 R2 Web Edition ■ Windows Server 2008 x64 on all current editions and architectures Symantec currently supports (SP2 required)

Supported operating systems for server components

Your server must run one of the operating systems listed below to install the SFW or SFW HA server software.

Note: SFW software for servers supports Hyper-V and parent partitions.

Table 3-2 Supported operating systems for servers

Windows Server	Platform	Edition	Version
Windows 2008 Server Core	x64		RTM or SP2
Windows 2008 R2 Server Core	x64		RTM or SP1
Windows Server 2008	x64	Standard, Enterprise, Datacenter	RTM or SP2
Windows Web Server 2008	x64		RTM or SP2
Windows Server 2008 R2	x64	Standard, Enterprise, Datacenter	RTM or SP1
Windows Web Server 2008 R2	x64		RTM or SP1
Windows Storage Server 2008	x64		
Windows Storage Server 2008 R2	x64		
Windows Small Business Server 2008	x64	Standard, Premium	
Windows Small Business Server 2011	x64	Standard, Premium	

Disk space requirements for SFW

[Table 3-3](#) summarizes approximate disk space requirements for SFW.

Table 3-3 Disk space requirements

Installation options	Required disk space
SFW + all options	1124 MB
SFW Client components	632 MB

System requirements for Microsoft clustering solutions

Refer to Microsoft documentation for Microsoft cluster requirements.

Use the following system requirements as a guideline for SFW with Microsoft Exchange Server in a Microsoft cluster:

- One CD-ROM drive accessible to the system on which you are installing SFW.
- Each system requires 1 GB of RAM for SFW.
- A minimum of 2 GB of RAM per server is required for Exchange 2007; refer to the Microsoft documentation for more information.

- SCSI or Fibre Channel host bus adapters (HBAs) can be used to access shared storage.
- Microsoft clustering requires at least two network adapters per system (one NIC to connect each system to the public network, and one NIC for the private network on each system). Symantec recommends using three network adapters (two NICs exclusively for the private network and one for the public network). Route each private NIC through a separate hub or switch to avoid single points of failure.
- Using static IP addresses for the public network and private network cards is highly recommended and is required for a Volume Replicator configuration. You also need a static IP address for the cluster itself. Verify that name resolution is configured for each node.
- Verify that the DNS and Active Directory Services are available. Make sure a reverse lookup zone exists in the DNS. Refer to the Microsoft documentation for instructions on creating a reverse lookup zone.
- Typical failover cluster configurations require shared disks to support applications that migrate between nodes in the cluster. Symantec recommends two disks for Exchange 2007: one for Exchange database files and one for Exchange log files.
- For a campus cluster configuration, the following applies:
 - The configuration requires two sites with a storage array for each site, with an equal number of disks at each site for the mirrored volumes.
 - Interconnects between the clusters are required for the storage and the network.
- Each system in a Microsoft cluster must be in the same Windows Server domain and must be using the same operating system version.
- For a disaster recovery configuration, the administrator account for the Exchange virtual server (clustered mailbox server) on the primary site must be the same account used for the Exchange virtual server on the secondary site.
- For a disaster recovery configuration, the cluster on the secondary site must reside in the Active Directory domain of the cluster on the primary site.

Additional SFW installation requirements for a Microsoft cluster

SFW requires administrator privileges to install the software.

To install SFW, a Microsoft cluster must be running. Before you install SFW, you must set up the hardware and install the operating system and Microsoft clustering feature on all systems and establish the Microsoft cluster.

Installing SFW requires a reboot, but a reboot on the active cluster node causes it to fail over. Therefore, use a "rolling install" procedure to install SFW first on the inactive cluster node. Then move the cluster resources to the other node and install on the now inactive node.

See ["Installing SFW with Microsoft Failover Cluster option"](#) on page 45.

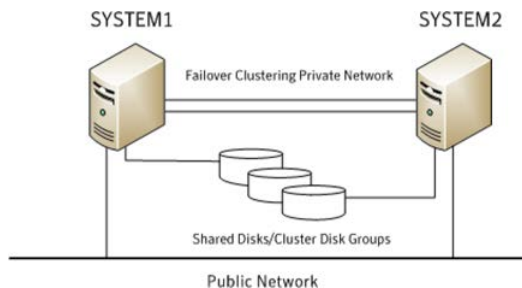
Note: You can install the SFW option for Microsoft Failover Cluster on a machine that is not a member of a Microsoft cluster. However, if that machine becomes the first node in a Microsoft cluster, the Volume Manager Disk Group resource type must be manually registered. For more information, see the *Symantec Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Planning your Exchange Server high availability configuration

You can configure Storage Foundation for Windows (SFW) and Exchange Server in a Microsoft cluster for high availability on a single site.

The following illustration shows a typical two-node active/passive configuration with Exchange. To set up one to one failover capabilities, the Exchange clustered mailbox server can fail over from SYSTEM1 to SYSTEM2 and vice versa.

Figure 3-1 High availability active/passive configuration



Some key points about the configuration:

- The Exchange clustered mailbox server is configured on the active node (SYSTEM1). If SYSTEM1 fails, SYSTEM2 becomes the active node and the Exchange clustered mailbox server comes online on SYSTEM2.
- One or more application servers can exist in a cluster, but each server must be managed by a separate application group configured with a distinct set of nodes in the cluster.

- The Exchange databases are configured on the shared storage on volumes contained in one or more cluster disk groups.
- SFW enables you to create a dynamic mirrored quorum. If the quorum resource fails, the mirror takes over for the resource.
 In this configuration, Symantec recommends creating a three-way mirror for the quorum to provide additional fault tolerance. If possible, do not use the disks assigned to the quorum for any other purpose.
- SFW enables you to add fault-tolerance to data volumes. Symantec recommends mirroring log volumes and a mirrored striped RAID layout for data volumes.

During the configuration process you will create virtual IP addresses for the following:

- Cluster IP address, used by Microsoft cluster
- Exchange clustered server IP address, which should be the same on all nodes

You should have these IP addresses available before you start deploying your environment.

Configuring the quorum device for high availability

The proper configuration of a quorum device is critical to providing the highest availability with SFW storage.

Although a single basic disk used as a physical disk resource can serve as the Microsoft clustering quorum device, this introduces a nonredundant component into an otherwise highly available system.

In general, a disk group containing a dedicated, three-way mirrored volume makes an ideal quorum device. Such a device tolerates two disk failures, because it is mirrored, and server and interconnect failures, because SFW can import it when the disks and at least one server are running.

For a server to take ownership of a disk group containing the cluster quorum device, SFW must successfully import the disk group, and obtain SCSI reservations on more than half of its disks. Disk groups containing odd numbers of disks are best for use as quorum devices because of this behavior.

An SFW cluster disk group containing a volume used as a quorum device should contain that volume only. Any other volumes in that disk group fail over whenever the quorum device changes ownership.

Planning your campus cluster configuration

The procedures for setting up a campus cluster are nearly the same as those for local clusters, with the following differences:

- A campus cluster has the nodes located in separate buildings. Therefore, the hardware setup requires SAN interconnects that allow these connections.
- In a campus cluster, each node has its own storage array rather than having a shared storage array between the two clusters.
- Both local clusters and campus clusters have SFW dynamic disk groups and volumes, but the volumes on each campus cluster node are mirrors of one another.
- Each disk group must contain the same number of disks on each site for the mirrored volumes.

More information is available on disk group and volume configuration.

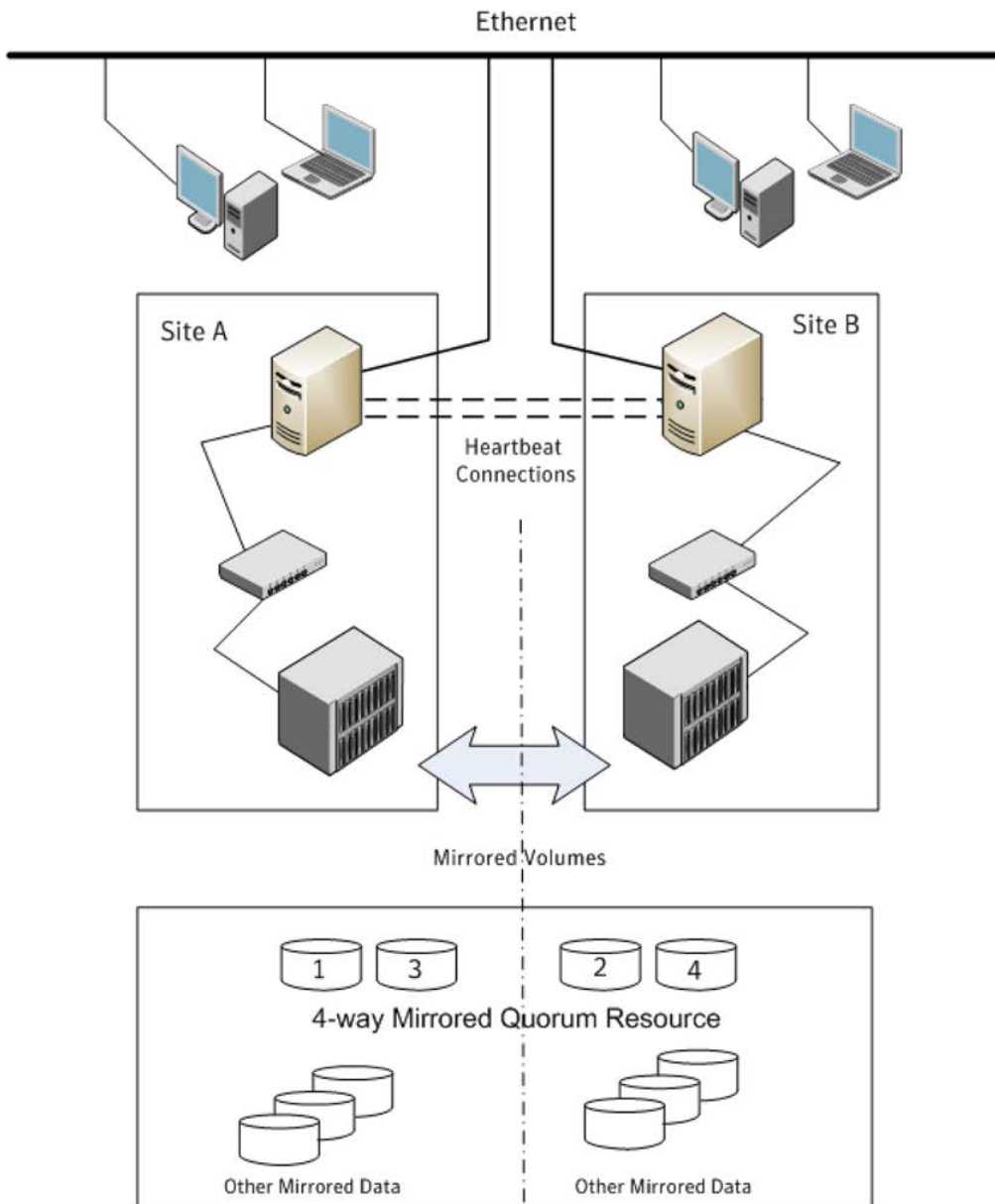
See [“Planning for SFW cluster disk groups and volumes”](#) on page 48.

Although a campus cluster setup with Microsoft clustering can work without Storage Foundation for Windows, SFW provides key advantages over using Microsoft clustering alone. Through a dynamic mirrored volume that functions on multiple disks across multiple sites, SFW protects the quorum resource in the cluster from being the single point of failure in the cluster.

Most customers use hardware RAID to protect the quorum disk, but that does not work when a natural disaster takes down the primary node and its attached storage. If the quorum resource is lost to the cluster, the cluster fails, because none of the cluster servers can gain control of the quorum resource and ultimately the cluster. Microsoft clustering alone cannot provide fault tolerance to the quorum disk.

[Figure 3-2](#) shows a Microsoft cluster campus cluster configuration with mirrored storage across clusters and a mirrored quorum resource. The 4-way mirrored quorum has an extra set of mirrors for added redundancy.

Figure 3-2 Typical campus clustering configuration



Microsoft campus cluster failure scenarios

Different failure and recovery scenarios can occur with a Microsoft campus cluster and SFW installed.

The site scenarios that can occur when there is a cluster server failure include the following:

- If the site not owning the quorum volume and the cluster goes offline, the quorum and data volumes stay online at the other site and other cluster resources stay online or move to that site. Storage Foundation for Windows lets the owning cluster node remain online with 50% ownership of the disks in the quorum group.
- If the site owning the quorum volume goes offline, the remaining site cannot gain control of the quorum volume because it cannot reserve a majority of disks in the quorum group. This is a safeguard to prevent multiple nodes from bringing online members of a cluster disk group to which they have access.

Manual failover of a cluster between two sites should be performed only after coordination between the two sites to ensure that the primary server has in fact failed. If the primary server is still active and you manually import a cluster disk group containing the cluster quorum to the secondary (failover) server, a split-brain situation occurs. There may be data loss if the split-brain situation occurs because each plex of the mirrored volume may be updated independently when the same disk group is imported on both nodes.

For additional details on the manual failover scenario, see the following topic:

See [“Microsoft cluster quorum and quorum arbitration”](#) on page 36.

[Table 3-4](#) lists failure situations and the outcomes that occur.

Table 3-4 List of failure situations and possible outcomes

Failure Situation	Outcome	Comments
Application fault May mean the services stopped for an application, a NIC failed, or a database table went offline.	Failover	If the services stop for an application failure, the application automatically fails over to the other site.
Server failure (Site A) May mean that a power cord was unplugged, a system hang occurred, or another failure caused the system to stop responding.	Failover	Assuming a two-node cluster pair, failing a single node results in a cluster failover. There will be a temporary service interruption for cluster resources that are moved from the failed node to the remaining live node.

Table 3-4 List of failure situations and possible outcomes (*continued*)

Failure Situation	Outcome	Comments
Server failure (Site B) May mean that a power cord was unplugged, a system hang occurred, or another failure caused the system to stop responding.	No interruption of service.	Failure of the passive site (Site B) does not interrupt service to the active site (Site A).
Partial SAN network failure May mean that SAN fiber channel cables were disconnected to Site A or Site B Storage.	No interruption of service.	Assuming that each of the cluster nodes has some type of Dynamic Multi-pathing (DMP) solution, removing one SAN fiber cable from a single cluster node should not effect any cluster resources running on that node, because the underlying DMP solution should seamlessly handle the SAN fiber path failover.
Private IP Heartbeat Network Failure May mean that the private NICs or the connecting network cables failed.	No interruption of service.	With the standard two-NIC configuration for a cluster node, one NIC for the public cluster network and one NIC for the private heartbeat network, disabling the NIC for the private heartbeat network should not effect the cluster software and the cluster resources, because the cluster software will simply route the heartbeat packets through the public network.
Public IP Network Failure May mean that the public NIC or LAN network has failed.	Failover. Mirroring continues.	When the public NIC on the active node, or public LAN fails, clients cannot access the active node, and failover occurs.
Public and Private IP or Network Failure May mean that the LAN network, including both private and public NIC connections, has failed.	No interruption of service. No Public LAN access. Mirroring continues.	The site that owned the quorum resource right before the "network partition" remains as owner of the quorum resource, and is the only surviving cluster node. The cluster software running on the other cluster node self-terminates because it has lost the cluster arbitration for the quorum resource.

Table 3-4 List of failure situations and possible outcomes (*continued*)

Failure Situation	Outcome	Comments
Lose Network Connection (SAN & LAN), failing both heartbeat and connection to storage May mean that all network and SAN connections are severed, for example if a single pipe is used between buildings for the Ethernet and storage.	No interruption of service. Disks on the same node are functioning. Mirroring is not working.	The node/site that owned the quorum resource right before the "network partition" remains as owner of the quorum resource, and is the only surviving cluster node. The cluster software running on the other cluster node self-terminates because it has lost the cluster arbitration for the quorum resource. By default Microsoft clustering clussvc service will try to auto-start every minute, so after LAN/SAN communication has been re-established, Microsoft clustering clussvc will auto-start and will be able to re-join the existing cluster.
Storage Array failure on Site A, or on Site B May mean that a power cord was unplugged, or a storage array failure caused the array to stop responding.	No interruption of service. Disks on the same node are functioning. Mirroring is not working.	The campus cluster is divided equally between two sites with one array at each site. Completely failing one storage array should not effect on the cluster or any cluster resources that are currently online. However, you will not be able to move any cluster resources between nodes after this storage failure, because neither node will be able to obtain a majority of disks within the cluster disk group.
Site A failure (power) Means that all access to site A, including server and storage, is lost.	Manual failover.	If the failed site contains the cluster node that owned the quorum resource, then the overall cluster would be offline and cannot be brought online on the remaining live site without manual intervention.
Site B failure (power) Means that all access to site B, including server and storage, is lost.	No interruption of service. Disks on the same node are functioning. Mirroring is not working.	If the failed site did not contain the cluster node that owned the quorum resource, then the cluster would still be alive with whatever cluster resources that were online on that node right before the site failure.

Microsoft cluster quorum and quorum arbitration

This section explains the quorum and quorum arbitration in Microsoft clusters.

- See ["Quorum"](#) on page 37.

- See “[Cluster ownership of the quorum resource](#)” on page 37.
- See “[The vxclus utility](#)” on page 38.

Quorum

The quorum resource maintains the cluster database, as well as critical recovery information, in a recovery log. The quorum resource must be available to all nodes through a SCSI or Fibre Channel bus. With Microsoft clustering alone, the quorum disk must be located on a single physical disk. However, with SFW, the quorum disk can be a mirrored volume that spans multiple disks and cluster nodes.

The quorum resource also determines ownership of the cluster. When a node that is controlling the cluster goes offline, other nodes use a challenge/defense protocol to determine which node can have control of the quorum resource and the cluster.

Cluster ownership of the quorum resource

The Microsoft clustering challenge/defense protocol uses a low-level bus reset of the SCSI buses between the computers to attempt to gain control of the quorum resource.

After a SCSI bus reset, the reservation that each server had been holding on the quorum disk is lost. Each server has about 10 seconds to re-establish that reservation, which would in turn let the other servers know that it is still functioning, even though the other servers would not necessarily be able to communicate with it.

If the active cluster server does not re-establish the SCSI reservation on the quorum resource within the time limit, the applications that were on the server transfer to the server that establishes the SCSI reservation first. The new server servicing the application may now be a bit slower, but clients still get their applications serviced. The IP (Internet Protocol) address and network names move, applications are reconstituted according to the defined dependencies, and clients are still serviced, without any question as to the state of the cluster.

The challenge/defense protocol is more complex when the quorum device is a volume in a Storage Foundation for Windows disk group. For a server to take ownership of the disk group containing the cluster quorum device, SFW on that server must successfully import the disk group, obtaining SCSI reservations on more than half of its disks.

Because a campus cluster configuration has an even number of disks on each site, failover cannot occur automatically. After a site failure, you must use the manual CLI command `vxclus enable` to bring the cluster disk groups online on the secondary node.

The vxclus utility

Storage Foundation for Windows provides the `vxclus` command line utility to allow forcing a failover to the secondary site. The command `vxclus enable` creates an entry in the Registry that enables the cluster disk group to be brought online on a node with a minority of the disks. After you run `vxclus enable`, you can bring the disk group resource online in the Microsoft cluster. After the cluster disk group is brought online, the `vxclus` functionality is disabled.

Warning: When bringing a cluster disk group online with a minority of cluster disks, make sure that a majority of the disk group disks are not online on any other cluster node before (and after) bringing online the disk group. If a majority of disk group disks are online on another node, data corruption can occur.

For more information on the `vxclus` utility, see the *Symantec Storage Foundation for Windows Administrator's Guide*. The `vxclus` utility also provides support for booting from a SAN, but you must have a hardware storage array that supports the capability.

Planning your disaster recovery configuration

After creating a high-availability cluster on a primary site, you can configure a secondary site cluster for disaster recovery.

This disaster recovery solution requires Symantec Storage Foundation Volume Replicator (Volume Replicator).

In a typical clustered Volume Replicator configuration 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. At least two disk groups are necessary—one for the application and one for the quorum resource volume. The quorum volume is not replicated from the primary site to the secondary site. Each site has its own quorum volume.

Figure 3-3 illustrates the cluster configuration on the primary site.

Figure 3-3 DR configuration primary site

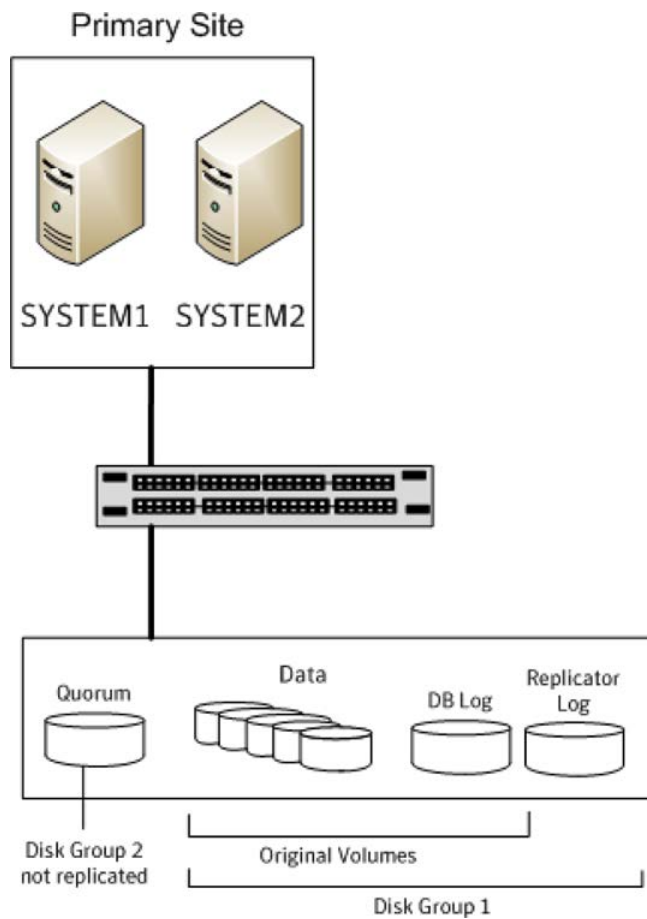
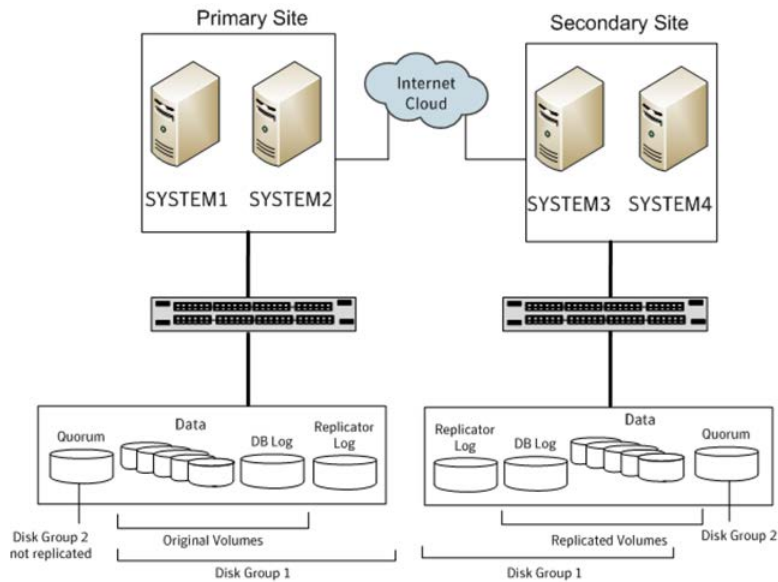


Figure 3-4 shows the primary and secondary site configuration.

Figure 3-4 DR configuration both sites



The quorum disk group is created separately on each site; it does not get replicated because each cluster has its own quorum.

More information is available on disk group and volume configuration.

See [“Planning for SFW cluster disk groups and volumes”](#) on page 48.

[Figure 3-5](#) shows details on the configuration of the Volume Replicator Replicated Volume Group (RVG). The Microsoft Exchange Server application data is stored on the volumes that are under the control of the RVG.

Figure 3-5

Typical Volume Replicator RVG configuration

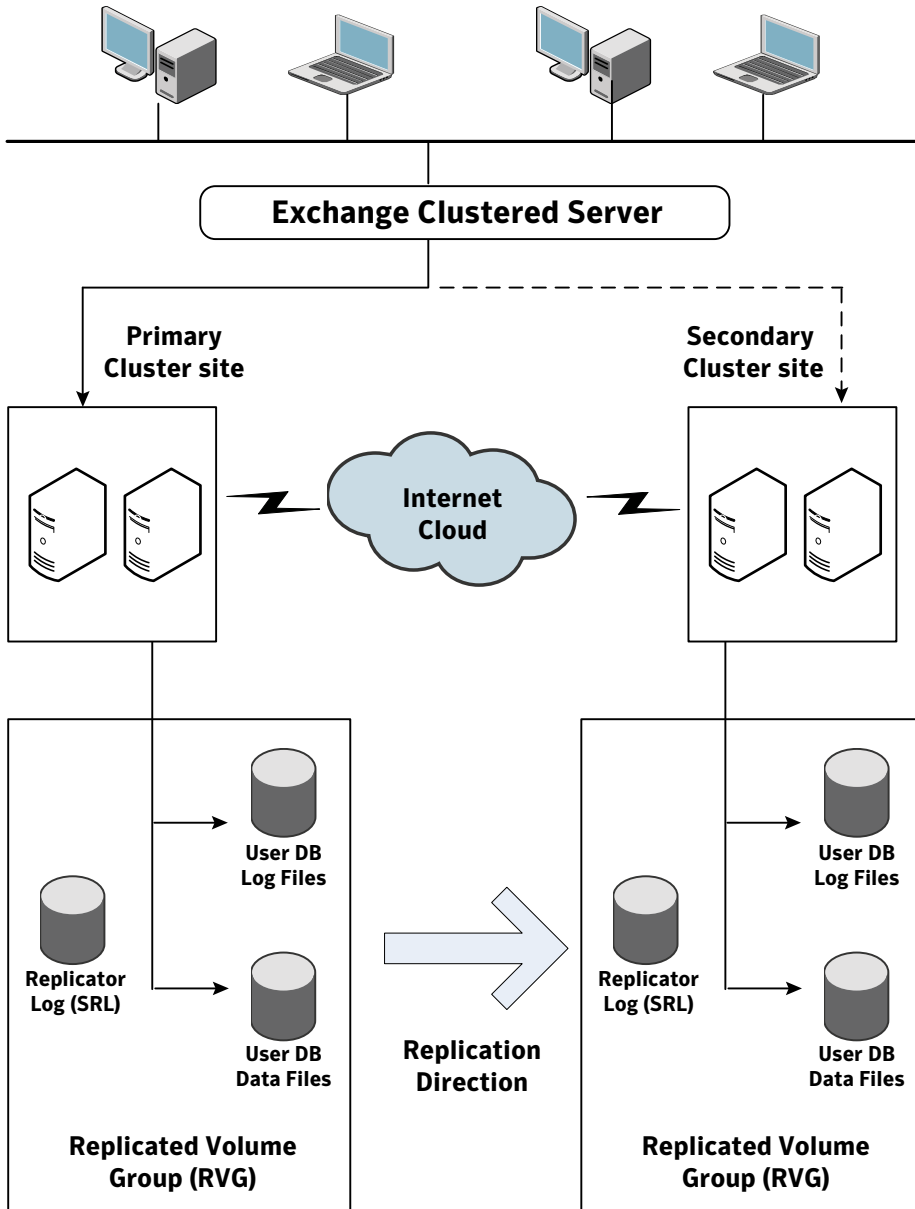
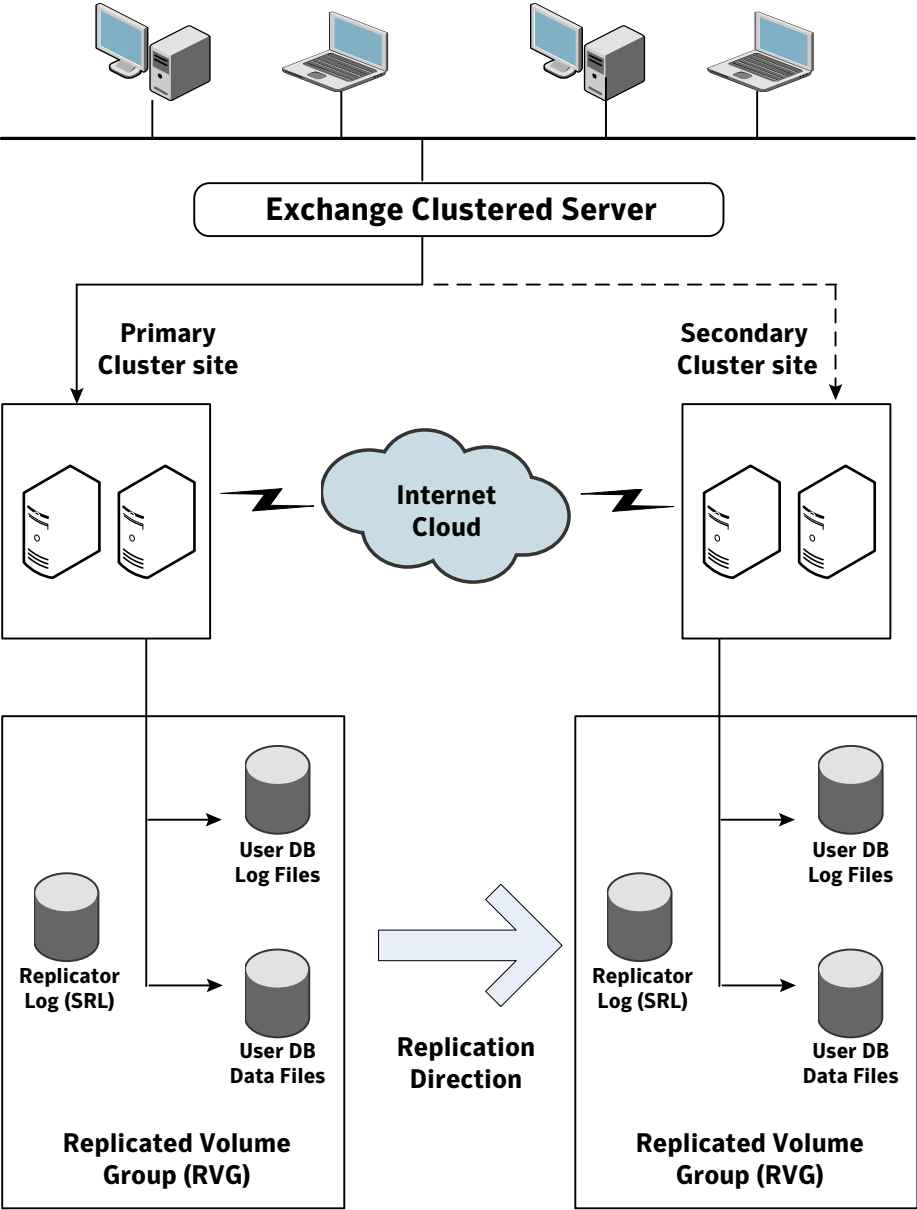


Figure 3-5 Typical Volume Replicator RVG configuration



Installing SFW with Microsoft clustering

This chapter includes the following topics:

- [Tasks for installing and configuring SFW with Microsoft clustering](#)
- [Configuring the storage hardware and network](#)
- [Establishing a Microsoft failover cluster](#)
- [Campus cluster: Connecting the two nodes](#)
- [Installing SFW with Microsoft Failover Cluster option](#)

Tasks for installing and configuring SFW with Microsoft clustering

[Table 4-1](#) shows the tasks to complete before and during SFW installation on a Microsoft cluster.

Table 4-1 Tasks for installing and configuring SFW with Microsoft clustering

Action	Description
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment, ■ Verify the DNS entries and binding order for the systems on which the application will be installed. See “Configuring the storage hardware and network” on page 43.
Establish a Microsoft cluster	Establish the cluster before installing SFW. See “Establishing a Microsoft failover cluster” on page 44.

Table 4-1 Tasks for installing and configuring SFW with Microsoft clustering
(continued)

Action	Description
For a campus cluster, connect the two nodes	For a campus cluster, connect the two nodes after setting up the cluster. See “Campus cluster: Connecting the two nodes” on page 45.
Install SFW with the Cluster Option for Microsoft Failover Cluster	Perform a rolling installation. See “Installing SFW with Microsoft Failover Cluster option” on page 45. Ensure that you select the following options during SFW installation: ■ Select the option to install SFW. ■ On the product options screen, select the option to install Cluster Option for Microsoft Failover Cluster. ■ Leave the client components selected for installation (the default). ■ If you plan to set up replication environment, select the option to install Volume Replicator.

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.

To prevent lost heartbeats on the private networks, and to prevent the Microsoft cluster 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.
- 3 Use independent hubs or switches for the private heartbeats. You can use cross-over Ethernet cables for two-node clusters.
- 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.

Establishing a Microsoft failover cluster

You should establish the Microsoft failover cluster before you install Symantec Storage Foundation.

Refer to the Microsoft documentation for details on establishing a failover cluster. In addition, you should be aware of the following SFW related requirement: Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. In the SFW environment, this means that before you create your SFW cluster disk groups, you must first remove these physical disk resources from the cluster. Otherwise, a reservation conflict occurs. After creating the SFW cluster disk groups, you will add Volume Manager Disk Group resources to the cluster, instead of physical disk resources.

Note: You can install the SFW Cluster Option for Microsoft Failover Cluster on a machine that is not a member of a Microsoft cluster. However, if that machine becomes the first node in a Microsoft cluster, the Volume Manager Disk Group resource type must be manually registered. For more information, see the *Symantec Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Campus cluster: Connecting the two nodes

Make the necessary connections between the two sites after you configure the Microsoft cluster. The cluster is already active on Server A, so Microsoft clustering is now in control of the cluster storage on Server A, and both nodes of the storage cannot be accessed at the same time by the operating system.

To connect the two nodes

- 1 Connect corresponding cables between the three network cards on the two sites.
- 2 Connect the two switches at the two sites through the storage interconnect.
- 3 Test the connectivity between the two sites. Test the IP addresses of all the network adapter cards in the cluster. Bring up the command window and type `ping ipaddress`, where the *ipaddress* is the corresponding network adapter in the other node.

Installing SFW with Microsoft Failover Cluster option

The following information assumes you have already configured a Microsoft cluster and you are installing Storage Foundation for Windows (SFW) on an inactive system that does not own any cluster resources.

Refer to the Microsoft documentation for information on configuring a Microsoft cluster.

Note: You can install the SFW Cluster Option for Microsoft Failover Cluster on a machine that is not a member of a Microsoft cluster. However, if that machine becomes the first node in a Microsoft cluster, the Volume Manager Disk Group resource type must be manually registered. For more information, see the *Symantec Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Symantec recommends a rolling installation to install SFW. For a rolling installation, you must first install SFW on an inactive system. If your resource groups are on

the system where you are installing SFW, you must move the resource groups from the SFW system to another system in the cluster.

After SFW is installed on an inactive system, move the resource groups to this system, and make the other systems inactive. Then install SFW on the other inactive systems in the Microsoft cluster simultaneously.

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

- Select **Storage Foundation for Windows** as the product to install.
- When selecting the available options from the server components, ensure that you select the following:
 - Select the **Cluster Option for Microsoft Failover Cluster** option.
 - If you are planning a disaster recovery configuration using Volume Replicator, select the **Veritas Volume Replicator** option.
- Leave the client components selected (the default).

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

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

For additional details on using the product installer or command line installation, see the *Symantec Storage Foundation and High Availability Solutions Installation and Upgrade Guide*.

Configuring SFW storage

This chapter includes the following topics:

- [Tasks for configuring SFW storage](#)
- [Planning for SFW cluster disk groups and volumes](#)
- [Considerations when creating disk groups and volumes for a campus cluster](#)
- [Considerations when creating volumes for a DR configuration using Volume Replicator replication](#)
- [Viewing the available disk storage](#)
- [Creating dynamic cluster disk groups](#)
- [Adding disks to campus cluster sites](#)
- [Creating dynamic volumes for high availability clusters](#)
- [Creating dynamic volumes for campus clusters](#)
- [Managing disk group and volumes](#)

Tasks for configuring SFW storage

You use SFW to create dynamic cluster disk groups and volumes for a cluster environment.

[Table 5-1](#) shows the tasks for configuring disk groups and volumes.

Table 5-1 Tasks for configuring disk groups and volumes

Action	Description
Plan the disk groups and volumes to create	See “Planning for SFW cluster disk groups and volumes” on page 48. If you are creating a campus cluster or a disaster recovery configuration, review additional information. See “Considerations when creating disk groups and volumes for a campus cluster” on page 51. See “Considerations when creating volumes for a DR configuration using Volume Replicator replication” on page 53.
Configure disk groups	Use the VEA console to create disk groups. See “Creating dynamic cluster disk groups” on page 54. Note: Setting up a Microsoft failover cluster creates physical disk resources for all the basic disks on the shared bus. To use these disks when you create your SFW cluster disk groups, you must first remove the physical disk resources from the cluster. Otherwise, a reservation conflict occurs.
For campus clusters, add disks to sites	To implement site-based allocation for volumes on campus clusters, you add the disks in the disk group to campus cluster sites. See “Adding disks to campus cluster sites” on page 56.
Configure volumes	Use the VEA console to create volumes. See “Creating dynamic volumes for high availability clusters” on page 57. See “Creating dynamic volumes for campus clusters” on page 62.
Understand how to deport and import disk groups and volumes to cluster nodes	When installing the application, you may need to deport and import disk groups and volumes to the different cluster nodes. See “Managing disk group and volumes” on page 69.

Planning for SFW cluster disk groups and volumes

A dynamic cluster disk group is a collection of one or more disks that behave as a single storage repository and which can potentially be accessed by different computers. Within each disk group, you can have dynamic volumes with different layouts.

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

Before creating a disk group, consider the following:

- The type of volume configurations that are required.
- The number of LUNs required for the disk group.
- The implications of backup and restore operations on the disk group setup.
- The size of databases and logs which depend on the traffic load.
- The number of disk groups and volumes that are needed for Exchange. Typically an SFW disk group corresponds to an Exchange storage group, with a separate volume for each database and for the transaction log.
- For campus clusters, consider the following:
 - The disk groups and number of disks on each site
 For campus clusters, each disk group must contain an equal number of disks on each site.
 - Each volume should be a mirrored volume with one plex of the volume on Site A's storage array and the other plex of the volume on Site B's storage array.
- In a Microsoft cluster, plan to include a disk group for the mirrored quorum resource. If possible, use small disks. Microsoft recommends 500 MB for the quorum disk. The number of disks recommended are as follows:
 - In a high-availability configuration, Symantec recommends using at least 3 disks for the mirrored quorum resource.
 - In a campus cluster configuration, because each site must contain an equal number of disks, Symantec recommends a 4-way mirrored quorum, 2 mirrors on each site.

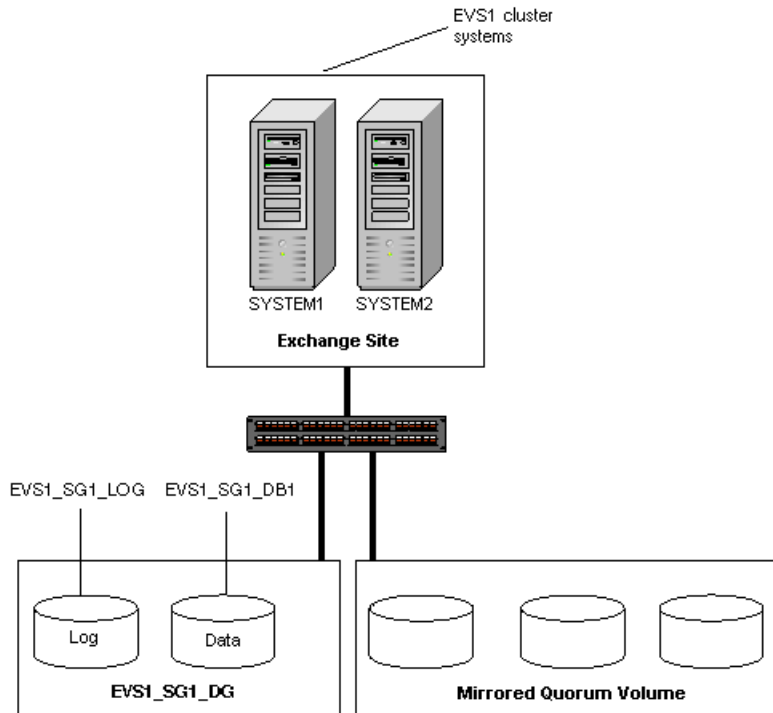
The following topics provide additional guidelines for specific configurations:

- See [“Considerations when creating disk groups and volumes for a campus cluster”](#) on page 51.
- See [“Considerations when creating volumes for a DR configuration using Volume Replicator replication”](#) on page 53.

Sample Exchange Server high availability cluster storage configuration

Figure 5-1 shows a detailed view of the disk groups and volumes for Exchange.

Figure 5-1 SFW disk groups and volumes for Exchange clustered mailbox server EVS1 in Microsoft clustering setup



Exchange disk group EVS1_SG1_DG contains two volumes:

- EVS1_SG1_DB1: Contains the Exchange database. Each database in an Exchange storage group typically resides on a separate volume.
- EVS1_SG1_LOG: Contains the transaction log for the storage group.

The general guidelines for disk group and volume setup for EVS1_SG1_DG also apply to additional storage groups.

This configuration is a simple example. The recommended practice for disk groups and volume layout is dependent on your environment.

Sample campus cluster storage configuration

The campus cluster storage configuration for Exchange Server is similar to the high availability storage configuration.

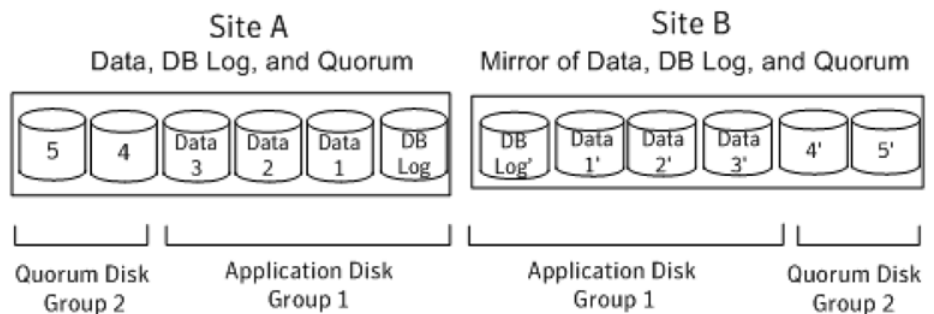
See [“Sample Exchange Server high availability cluster storage configuration”](#) on page 50.

Note that in a campus cluster each disk group spans the storage arrays at both sites. The data and database log on Site A are mirrored to Site B. Each mirrored volume can have more than two disks, but must have an even number, such as four. All the application data could be in one large mirrored volume with multiple disks, but the same number of disks are required on both sites for the mirroring.

A four-way mirror for the quorum volume provides additional redundancy. The minimum configuration would be a two-way mirror. If possible, use small disks for the quorum volume. Microsoft recommends 500 MB for the quorum volume.

[Figure 5-2](#) shows an example campus cluster storage configuration in a Microsoft cluster environment.

Figure 5-2 SFW disk groups and volumes in a Microsoft campus cluster



Considerations when creating disk groups and volumes for a campus cluster

When you create the disk groups for a campus cluster, ensure that each disk group has the same number of disks on each physical site. You create each volume as a mirrored volume with one plex of the volume on Site A's storage array and the other plex of the volume on Site B's storage array.

Symantec recommends using the SFW site-aware allocation feature for campus cluster storage. Site-aware allocation can ensure that site boundary limits are maintained for operations like volume grow, subdisk move, and disk relocation.

Enabling site-aware allocation for campus clusters requires the following steps in the VEA:

- After creating the disk groups, you tag the disks with site names to enable site-aware allocation. This is a separate operation, referred to in the VEA as adding disks to a site.
As an example, say you had a disk group with four disks. Disk1 and Disk2 are physically located on Site A. Disk3 and Disk4 are physically located on Site B. Therefore, you add Disk1 and Disk2 to "site_a" and add Disk3 and Disk4 to "site_b".
- During volume creation, you specify the volume site type as Site Separated. This ensures that the volume is restricted to the disks on the selected site.

Note: The hot relocation operation does not adhere to site boundary restrictions. If hot relocation causes the site boundary to be crossed, then the Site Separated property of the volumes is changed to Siteless. This is done so as not to disable hot relocation. To restore site boundaries later, you can relocate the data that crossed the site boundary back to a disk on the original site and then change back the properties of the affected volumes.

For more information on site-aware allocation, refer to the *Symantec Storage Foundation Administrator's Guide*.

When you create the volumes for a campus cluster, consider the following:

- During disk selection, configure the volume as "Site Separated" and select the two sites of the campus cluster from the site list.
- For volume attributes, select the "mirrored" and "mirrored across enclosures" options.
- Symantec recommends using either simple mirrored (concatenated) or striped mirrored options for the new volumes. Striped mirrored gives you better performance compared to concatenated.
When selecting striped mirrored, select two columns in order to stripe one enclosure that is mirrored to the second enclosure.
- During the volume creation procedure for Site Separated volumes, you can only create as many mirrors as there are sites. However, once volume creation is complete, you can add additional mirrors if desired.
- Choosing "mirrored" and the "mirrored across" option without having two enclosures that meet requirements causes new volume creation to fail.
- You cannot select RAID-5 for mirroring.

- Selecting "stripe across enclosures" is not recommended because then you need four enclosures, instead of two.
- Logging can slow performance.

Considerations when creating volumes for a DR configuration using Volume Replicator replication

Before creating a disk group and volumes for a DR configuration using Volume Replicator replication, consider the following:

- Replicating the system databases is not required or recommended. Make sure that the system databases are not placed on volumes that will be replicated.
- Do not assign a drive letter to the Replicator Log volume. This will limit access to that volume and avoid potential data corruption. You can create the Replicator Log volume while using the wizard for setting up the replicated data set.
- Volume Replicator does not support these types of volumes:
 - Storage Foundation for Windows (software) RAID 5 volumes
 - Volumes with the Dirty Region Log (DRL)
 - Volumes with a comma in their names
 - For the Replicator Log volume, in addition to the above types also make sure that the volume does not have a DCM.

Warning: Do not use volume types that are not supported by Volume Replicator.

Viewing the available disk storage

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

Note: If User Access Control (UAC) is enabled on Windows Server 2008 systems, then you cannot log on to VEA GUI with an account that is not a member of the Administrators group, such as a guest user. This happens because such user does not have the "Write" permission for the "Veritas" folder in the installation directory (typically, C:\Program Files\Veritas). As a workaround, an OS administrator user can set "Write" permission for the guest user using the Security tab of the "Veritas" folder's properties.

To view the available disk storage

- 1 Launch VEA from **Start > Programs > Symantec > Symantec Storage Foundation > Veritas Enterprise Administrator** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

Select a profile if prompted.
- 2 Click **Connect to a Host or Domain**.
- 3 In the Connect dialog box select the host name from the pull-down menu and click **Connect**.

To connect to the local system, select **localhost**. Provide the user name, password, and domain if prompted.
- 4 In the VEA configuration tree, expand **hostname > StorageAgent** and then click **Disks**.

The internal names for the disks which the current system can access for available storage are displayed, with names Harddisk1, Harddisk2, etc. The list includes both disks internal to the local system and any external storage that is available.

Creating dynamic cluster disk groups

Create a dynamic cluster disk group with volumes on shared storage so that they can be shared between nodes in the cluster.

Part of the process of creating a dynamic disk group is assigning it a name. Choose a name that is unique to your environment. Make note of this name, as it will be required later.

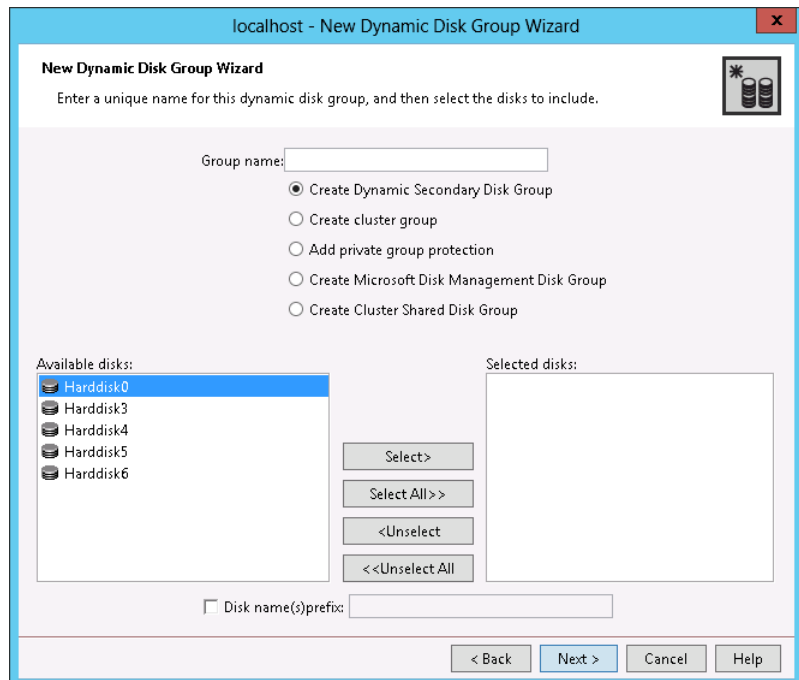
To create dynamic cluster disk groups, use the Veritas Enterprise Administrator (VEA). The VEA can be invoked on one of the servers and can be used to connect to all the other servers. However, VEA can also be launched on client system and can be used to manage all the servers remotely.

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

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

To create a dynamic (cluster) disk group

- 1 Launch VEA from **Start > Programs > Symantec > Symantec Storage Foundation > Veritas Enterprise Administrator** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
 Select a profile if prompted.
- 2 Click **Connect to a Host or Domain**.
- 3 In the Connect dialog box, select the host name from the pull-down menu and click **Connect**. To connect to the local system, select **localhost**. Provide the user name, password, and domain if prompted.
- 4 To start the New Dynamic Disk Group wizard, expand the tree view under the host node, right click the **Disk Groups** icon, and select **New Dynamic Disk Group** from the context menu.
- 5 In the Welcome screen of the New Dynamic Disk Group wizard, click **Next**.
- 6 Provide information about the cluster disk group as follows.



- Enter the name of the disk group (for example, EVS1_SG1_DG).

Note: A dynamic disk group name is limited to 18 ASCII characters. It cannot contain spaces, slash mark (/), backslash (\), exclamation point (!), angle brackets (< >), or equal sign (=). Also, a period cannot be the first character in the name.

- Click the checkbox for **Create cluster group**.
 - Select the appropriate disks in the **Available disks** list, and use the **Add** button to move them to the **Selected disks** list.
 - Optionally, check the **Disk names prefix** checkbox and enter a disk name prefix to give the disks in the disk group a specific identifier. For example, entering TestGroup as the prefix for a disk group that contains three disks creates TestGroup1, TestGroup2, and TestGroup3 as internal names for the disks in the disk group.
 - Windows Disk Management Compatible Dynamic Disk Group creates a type of disk group that is created by Windows Disk Management (LDM).
 - Click **Next**.
- 7 Click **Next** to accept the confirmation screen with the selected disks.
- 8 Click **Finish** to create the new disk group.

Adding disks to campus cluster sites

For campus cluster storage, Symantec recommends using Symantec Storage Foundation for Windows (SFW) site-aware allocation. To enable site-aware allocation, you assign a site name to disks after they are added to a disk group. In the VEA assigning a site name is referred to as adding disks to a site.

For example, Disk1 and Disk2 are physically located on Site A and Disk3 and Disk4 are physically located on Site B. Therefore, you add Disk1 and Disk2 to site_a and add Disk3 and Disk4 to site_b.

To add disks to a site

- 1 From the VEA console, right-click a disk that needs to be added to a site and select **Add Disk to Site**.

Disks must be part of a dynamic disk group in order to add them to a site.

- 2 In the **Add Disk to a Site** screen, choose one of the following:
 - Choose **Select a new site** and specify a new site name.

The site name can include any alphanumeric value and valid characters like the period (.), dash (-), and underscore (_). It cannot exceed 31 characters. Site names are case insensitive; all names are converted to lowercase.

- Choose **Available Sites** and select a site from the list.
- 3 From the **Available Disks** column, select the disk or disks to add to the specified site.
- 4 Click OK.

Creating dynamic volumes for high availability clusters

Use this procedure for creating volumes for a disk group in a high availability cluster. For volumes in a campus cluster, use the following procedure instead:

See [“Creating dynamic volumes for campus clusters”](#) on page 62.

The following topic provides additional guidelines for a DR configuration:

See [“Considerations when creating volumes for a DR configuration using Volume Replicator replication”](#) on page 53.

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

To create dynamic volumes

- 1 Launch VEA from **Start > Programs > Symantec > Symantec Storage Foundation > Veritas Enterprise Administrator** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
 Select a profile if prompted.
- 2 Click **Connect to a Host or Domain**.
- 3 In the Connect dialog box select the host name from the pull-down menu and click **Connect**. To connect to the local system, select **localhost**. Provide the user name, password, and domain if prompted.
- 4 To start the New Volume wizard, expand the tree view under the host node to display all the disk groups. Right click a disk group and select **New Volume** from the context menu.

You can right-click the disk group you have just created, for example EVS1_SG1_DG.

- 5 At the New Volume wizard opening screen, click **Next**.
- 6 Select the disks for the volume as follows:

- Make sure the appropriate disk group name appears in the **Group name** drop-down list.
For example, EVS1_SG1_DG.
 - For Site Preference, leave the setting as **Siteless** (the default).
 - Automatic disk selection is the default setting. To manually select the disks, click **Manually select disks** and use the **Add** and **Remove** buttons to move the appropriate disks to the **Selected disks** list. Manual selection of disks is recommended.
 - You may also check **Disable Track Alignment** to disable track alignment for the volume. Disabling Track Alignment means that the volume does not store blocks of data in alignment with the boundaries of the physical track of the disk.
 - Click **Next**.
- 7 Specify the volume attributes as follows:

localhost - New Volume Wizard

New Volume Wizard
 Select the attributes for this volume.

Volume name: Vol1

Size: 1 GB Max Size

Layout

☒ Concatenated ☐ Striped ☐ RAID-5

Columns: 2

Stripe unit size (Sectors): 128

☐ Stripe across: Port

Mirror Info

☐ Mirrored

Total mirrors: 2

☐ Mirror across: Port

☐ Enable logging

Concatenated: A simple volume with a single copy of data on one or more disks.

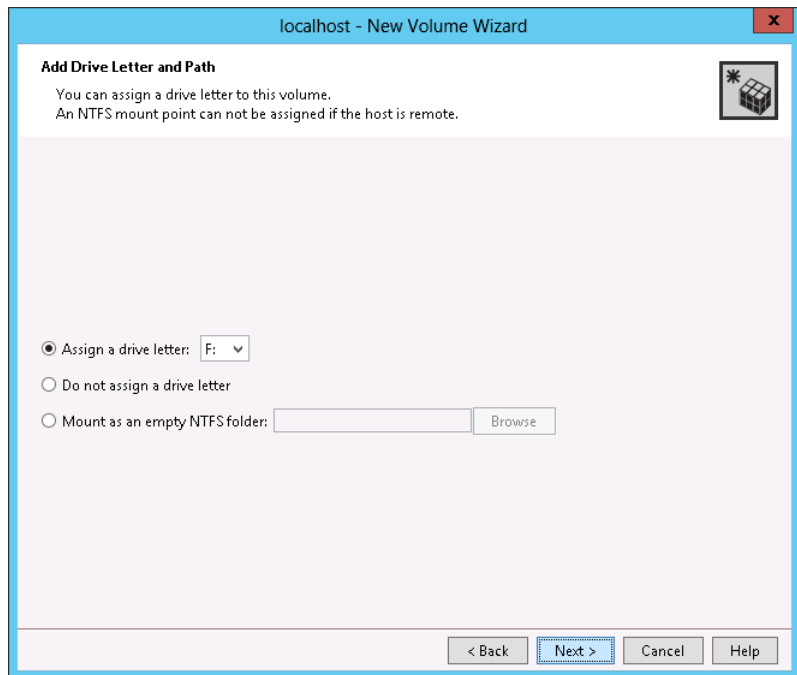
< Back Next > Cancel Help

- Enter a volume name.

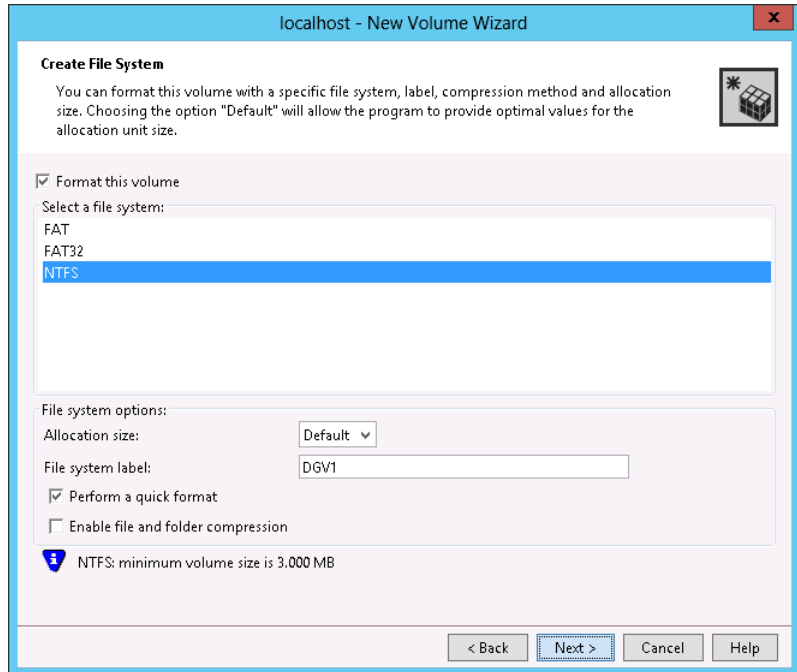
Note: A volume name is limited to 18 ASCII characters. It cannot contain spaces, slash mark (/), backslash (\), exclamation point (!), angle brackets (< >), or equal sign (=). Also, a period cannot be the first character in the name.

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

- Click **Next**.
- 8 Assign a drive letter or mount point to the volume. You must use the same drive letter or mount point on all systems in the cluster. Make sure to verify the availability of the drive letter before assigning it.
- To assign a drive letter, select **Assign a Drive Letter**, and choose a drive letter.
 - To mount the volume as a folder, select **Mount as an empty NTFS folder**, and click **Browse** to locate an empty folder on the shared disk.
 - If creating a Replicator Log volume for Volume Replicator, select **Do not assign a drive letter**.



- 9 Click **Next**.
- 10 Create an NTFS file system as follows.



- Make sure the **Format this volume** checkbox is checked and click **NTFS**.
 - For a Volume Replicator configuration, for the Replicator Log volume only, clear the **Format this volume** check box.
 - Select an allocation size or accept the default.
 - The file system label is optional. SFW makes the volume name the file system label.
 - Select **Perform a quick format** if you want to save time.
 - Select **Enable file and folder compression** to save disk space. Note that compression consumes system resources and performs encryption and decryption, which may result in reduced system performance.
 - Click **Next**.
- 11 Click **Finish** to create the new volume.
 - 12 Repeat these steps to create additional volumes.
- Create the cluster disk group and volumes on the first node of the cluster only.

Creating dynamic volumes for campus clusters

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

For creating volumes for other types of clusters, see the following:

See [“Creating dynamic volumes for high availability clusters”](#) on page 57.

Before you begin, review the following topics:

See [“Considerations when creating disk groups and volumes for a campus cluster”](#) on page 51.

See [“Adding disks to campus cluster sites”](#) on page 56.

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

To create dynamic volumes

- 1 Launch VEA from **Start > Programs > Symantec > Symantec Storage Foundation > Veritas Enterprise Administrator** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
 Select a profile if prompted.
 (Skip to step 4 if VEA is already connected to the appropriate host)
- 2 Click **Connect to a Host or Domain**.
- 3 In the Connect dialog box select the host name from the pull-down menu and click **Connect**. To connect to the local system, select **localhost**. Provide the user name, password, and domain if prompted.
- 4 To start the New Volume wizard, expand the tree view under the host node to display all the disk groups. Right click a disk group and select **New Volume** from the context menu.
 You can right-click the disk group you have just created, for example EVS1_SG1_DG.
- 5 At the New Volume wizard opening screen, click **Next**.
- 6 Select the disks for the volume as follows.

localhost - New Volume Wizard

Assign Disks for Volume

Storage Foundation will automatically select the disks used to create the volume unless you choose to manually specify any of the disks to be used.

Group name: DG1

Site Preference

Siteless

Site Confined

Site Separated

Select site from :

Auto select disks

Manually select disks

Available disks:

Name	PTL	Size	Site
Harddi	P3C0T0L0	1.100 GB	

Select>

Select All>>

<Unselect

<<Unselect All

Selected disks:

Disable Track Alignment

Disable Caching

< Back

Next >

Cancel

Help

Group name

Make sure the appropriate disk group is selected.

Site preference

Select the **Site Separated** option.

Select site from

Select the campus cluster sites. Press **CTRL** to select multiple sites.

Note: If no sites are listed, the disks have not yet been added to a site.

Auto select disks

Automatic disk selection is recommended for campus clusters. SFW automatically selects the disks based on the following criteria:

■ Their port assignment (disks with two different ports are selected). Note that in the list of available disks, the entry after each disk name starts with the port number. For example, the “P3” in the entry P3C0T2L1 refers to port 3.

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

Manually select disks

If you manually select disks, use the **Add** and **Remove** buttons to move the appropriate disks to the **Selected disks** list.

Disable Track Alignment

You may also check Disable Track Alignment to disable track alignment for the volume. Disabling Track Alignment means that the volume does not store blocks of data in alignment with the boundaries of the physical track of the disk.

Click **Next**.

7 Specify the volume attributes as follows.

localhost - New Volume Wizard

New Volume Wizard

Select the attributes for this volume.

Volume name: Vol1

Size: 1 GB Max Size

Layout

☒ Concatenated

Columns: 2

Stripe unit size (Sectors): 128

☐ Stripe across: Port

☐ Striped

☐ RAID-5

Mirror Info

☐ Mirrored

Total mirrors: 2

☐ Mirror across: Port

☐ Enable logging

Concatenated: A simple volume with a single copy of data on one or more disks.

< Back

Next >

Cancel

Help

Volume name

Specify a name for the volume.

Note: A volume name is limited to 18 ASCII characters. It cannot contain spaces, slash mark (/), backslash (\), exclamation point (!), angle brackets (< >), or equal sign (=). Also, a period cannot be the first character in the name.

Size

Specify a size for the volume. If you click **Max Size**, the **Size** box shows the maximum possible volume size for that layout in the dynamic disk group.

Layout

Ensure that the Mirrored checkbox is selected.

Select a layout type as follows:

Select either **Concatenated** or **Striped**.

If you are creating a striped volume, the **Columns** and **Stripe unit** size boxes need to have entries. Defaults are provided. In addition, click the **Stripe across** checkbox and select **Ports** from the drop-down list.

Mirror Info

Click **Mirror across** and select **Enclosures** from the drop-down list.

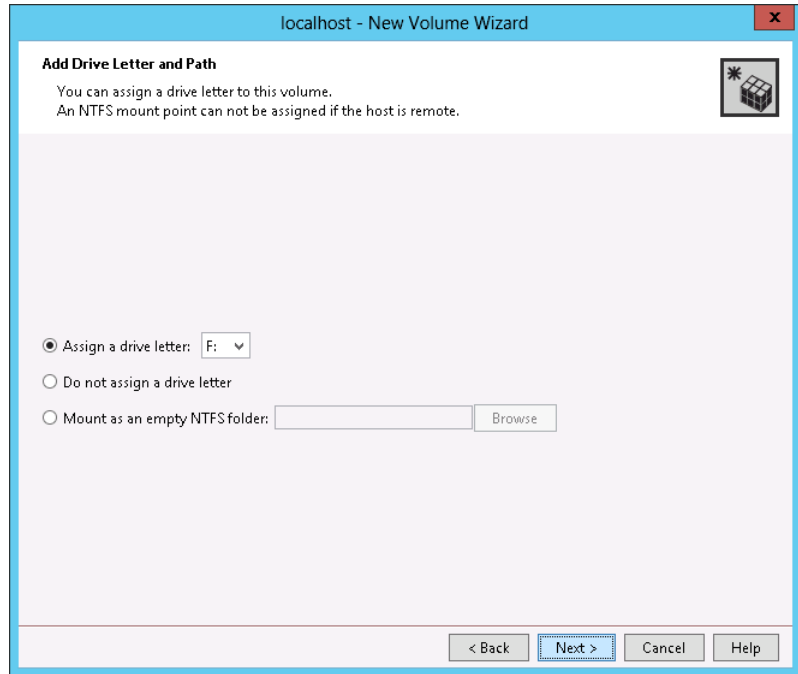
When creating a site separated volume, as required for campus clusters, the number of mirrors must correspond to the number of sites. If needed, you can add more mirrors after creating the volume.

Enable logging

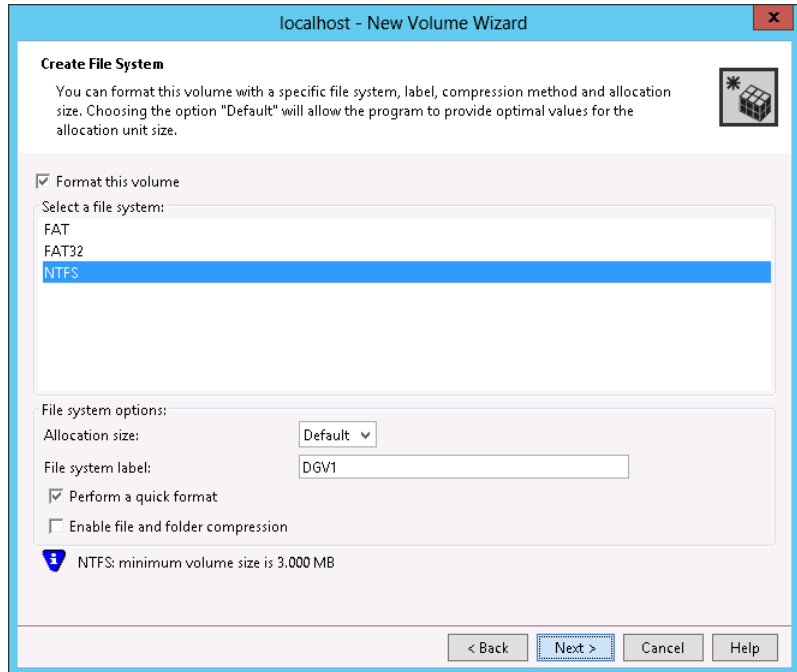
Verify that this option is not selected.

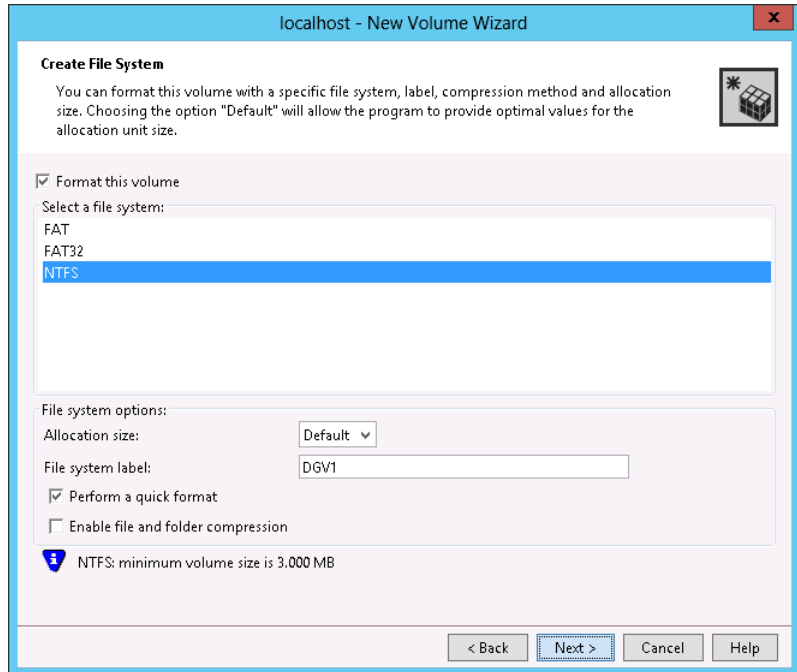
Click **Next**.

- 8 In the Add Drive Letter and Path dialog box, assign a drive letter or mount point to the volume. You must use the same drive letter or mount point on all systems in the cluster. Make sure to verify the availability of the drive letter before assigning it.
 - To assign a drive letter, select **Assign a Drive Letter**, and choose a drive letter.
 - To mount the volume as a folder, select **Mount as an empty NTFS folder**, and click **Browse** to locate an empty folder on the shared disk.



- 9 Click **Next**.
- 10 Create an NTFS file system as follows.





- Make sure the **Format this volume** checkbox is checked and click **NTFS**.
 - Select an allocation size or accept the default.
 - The file system label is optional. SFW makes the volume name the file system label.
 - Select **Perform a quick format** if you want to save time.
 - Select **Enable file and folder compression** to save disk space. Note that compression consumes system resources and performs encryption and decryption, which may result in reduced system performance.
 - Click **Next**.
- 11 Click **Finish** to create the new volume.
 - 12 Repeat these steps to create additional volumes.

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

Managing disk group and volumes

During the process of setting up an SFW environment, refer to the following guidelines for managing disk groups and volumes:

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

Importing a disk group and mounting a volume

Use the VEA Console to import a disk group and mount a volume.

To import a disk group

- 1 From the VEA Console, right-click a disk name in a disk group or the group name in the Groups tab or tree view.
- 2 From the menu, click **Import Dynamic Disk Group**.

To mount a volume

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

Unmounting a volume and deporting a disk group

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

To unmount a volume and deport the dynamic disk group

- 1 From the VEA tree view, right-click the volume, click **File System**, and click **Change Drive Letter and Path**.
- 2 In the Drive Letter and Paths dialog box, click **Remove**. Click **OK** to continue.
- 3 Click **Yes** to confirm.

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

Implementing a dynamic mirrored quorum resource

This chapter includes the following topics:

- [Tasks for implementing a dynamic mirrored quorum resource](#)
- [Creating a dynamic cluster disk group and a mirrored volume for the quorum resource](#)
- [Adding a Volume Manager Disk Group resource for the quorum](#)
- [Changing the quorum resource to a dynamic mirrored quorum resource](#)

Tasks for implementing a dynamic mirrored quorum resource

One of the key advantages of using SFW with Microsoft clustering is the ability to create a mirrored quorum resource that adds fault tolerance to the quorum and protects the cluster.

[Table 6-1](#) shows the tasks for implementing the mirrored quorum resource.

Table 6-1 Tasks for implementing the mirrored quorum resource

Action	Description
Create a dynamic cluster disk group and a mirrored volume for the quorum resource.	Create a dynamic cluster disk group and a mirrored volume for the quorum resource. See “Creating a dynamic cluster disk group and a mirrored volume for the quorum resource” on page 73.

Table 6-1 Tasks for implementing the mirrored quorum resource (continued)

Action	Description
Add a Volume Manager Disk Group resource to the cluster	Add a Volume Manager Disk Group resource for the disk group that you created for the quorum. Create a new quorum group, then add the Volume Manager Disk Group resource for the disk group that you created for the quorum. See “Adding a Volume Manager Disk Group resource for the quorum” on page 74.
Change the cluster quorum resource to the dynamic mirrored quorum resource	Change the cluster quorum properties to use the Volume Manager Disk Group resource. Select either the Node and Disk Majority or No Majority: Disk Only option when configuring the quorum. See “Changing the quorum resource to a dynamic mirrored quorum resource” on page 75.

Creating a dynamic cluster disk group and a mirrored volume for the quorum resource

Use SFW to create a separate cluster disk group for the quorum disks. Microsoft recommends 500 MB for the quorum disk.

Note: If you add other volumes to this disk group, any failures related to their operation can cause disruptive failovers of the quorum volume. If a volume in the group experiences a high level of read/write activity, failovers may result from delayed access to the quorum volume by Microsoft clustering.

Symantec recommends the following configuration for the quorum disk group to create the mirrored quorum volume:

- For a failover cluster, use three small disks; you need a minimum of two disks.
- For a campus cluster, use four small disks.

Use the following guidelines when creating the mirrored volumes:

- Select the **Concatenated** layout.
- Select the **Mirrored** check box.
- For a high-availability failover cluster, specify the three mirrors.
- For a campus cluster, specify the four mirrors.

Detailed procedures are available for creating cluster disk groups and volumes.

See [“Creating dynamic cluster disk groups”](#) on page 54.

See [“Creating dynamic volumes for high availability clusters”](#) on page 57.

Adding a Volume Manager Disk Group resource for the quorum

You add a Volume Manager Disk Group resource corresponding to the disk group that you created for the quorum. You do not set any dependencies for this resource.

You first create a service or application for the quorum resource, name it (for example, `QUORUM`), and add the resource to it.

To add a Volume Manager Disk Group resource for the quorum

- 1 From the **Start** menu (the **Start** screen on Windows 2012 operating systems), click **Administrative Tools**.
- 2 Launch the Failover Cluster Manager snap-in by clicking **Failover Cluster Manager**.
- 3 Verify that the cluster is online on the same node where you created the disk group.
- 4 In the left pane of Failover Cluster Management, right-click **Services and Applications** and select **More Actions > Create Empty Service or Application**.
- 5 Right-click the new group and rename it, for example `QUORUM`.
- 6 Right-click `QUORUM` and select **Add a resource > More resources > Add Volume Manager Disk Group**.
- 7 Right-click **New Volume Manager Disk Group** in the center pane and click **Properties**.
- 8 In the General tab of the Properties dialog box, type a name for the resource in the Resource Name field, for example, `QUORUM_DG_RES`.
- 9 On the Properties tab, in the Disk Group Name field, type the name of the disk group that you previously created for the quorum, and click **OK** to close the dialog box.
- 10 Right-click the Quorum disk group resource (for example, `QUORUM_DG_RES`) in the left pane and select **Bring this resource online**.

The specified disk group resource, `QUORUM_DG_RES` resource, is created under the Quorum group (for example, `QUORUM`).

Changing the quorum resource to a dynamic mirrored quorum resource

After adding a Volume Manager Disk Group resource for the quorum, you change the cluster quorum properties to use that resource. This changes the quorum resource to a dynamic mirrored quorum resource.

Use the following procedure to configure the cluster quorum settings and change the quorum resource to a dynamic mirrored quorum resource.

To change the quorum to a dynamic mirrored quorum resource

- 1 In Failover Cluster Management, right-click the cluster node in the configuration tree, and select **More Actions > Configure Cluster Quorum Settings**.

The Configure Cluster Quorum Wizard opens.

- 2 Review the screen and click **Next**.
- 3 Select either the **Node and Disk Majority** or **No Majority: Disk Only** radio button, and click **Next**.
- 4 Select the storage resource that you want to assign as the disk witness for the quorum and click **Next**.

This is the Volume Manager Disk Group resource that you previously created for the quorum disk group, for example, `QUORUM_DG_RES`.

- 5 Review the information in the Confirmation screen and click **Next**.
- 6 Click **Finish** to close the wizard.

Installing Exchange Server and configuring resources

This chapter includes the following topics:

- [Tasks for installing and configuring Exchange Server](#)
- [Adding a Volume Manager Disk Group resource for Exchange 2007 installation](#)
- [Installing Exchange Server](#)
- [Adding the Volume Manager Disk Group resources to the Exchange group](#)
- [Setting the database dependency on the disk group resource](#)
- [Moving Exchange databases and logs to shared storage](#)
- [Verifying the Exchange Server group in the Microsoft cluster](#)

Tasks for installing and configuring Exchange Server

Table 7-1 show the process for deploying Exchange Server with SFW in a Microsoft failover cluster or campus cluster. If you are installing and configuring Exchange on a secondary site for disaster recovery, see the following topic:

See [“Creating a parallel environment for Exchange Server on the secondary site”](#) on page 85.

Table 7-1 Process for deploying Exchange Server with SFW in a Microsoft failover cluster

Action	Description
Configure disk groups and volumes for Exchange Server	If you have not yet done so, use the VEA console to create disk groups and volumes for Exchange Server. See “Tasks for configuring SFW storage” on page 47.
Add the VMDG resource for the First Storage group to the quorum group	Add the VMDG disk group resource(s) for the First Storage Group. See “Adding a Volume Manager Disk Group resource for Exchange 2007 installation” on page 77.
Install Exchange Server	See “Installing Exchange Server” on page 78.
Add the VMDG resources to the Exchange group	See “Adding the Volume Manager Disk Group resources to the Exchange group” on page 79.
Set the database dependency on the disk group resource	See “Setting the database dependency on the disk group resource” on page 80.
Move Exchange databases and logs to shared storage.	See “Moving Exchange databases and logs to shared storage” on page 80.
Verify the cluster configuration	Move the online Exchange Server cluster group to the second node and back to the first node. See “Verifying the Exchange Server group in the Microsoft cluster” on page 82.

Adding a Volume Manager Disk Group resource for Exchange 2007 installation

Before installing Exchange 2007 in a Microsoft failover cluster with SFW, you add a Volume Manager Disk Group (VMDg) resource for the disk group that you created for the First Storage Group. By doing so, you can install the First Storage Group on a dynamic volume.

You add this resource to the Quorum group temporarily. After installation, you will move it to the Exchange group created by installation and set the appropriate dependencies.

Note: Before creating the resource, start the cluster service on all the nodes in the cluster.

To create a Volume Manager Disk Group resource for the application

- 1 From the **Start** menu (the **Start** screen on Windows 2012 operating systems), click **Administrative Tools**.

Launch the Failover Cluster Manager snap-in by clicking **Failover Cluster Manager**.

Ensure that you are connected to the required cluster.

- 2 In the left pane (tree view) of the Failover Cluster Management tool, right-click the Quorum resource group under **Services and Applications**. Select **Add a resource > More resources > Add Volume Manager Disk Group**.
- 3 In the center panel under Disk Drives, double-click **New Volume Manager Disk Group** to open its Properties dialog box.
- 4 On the **General** tab of the Properties dialog box, type a name for the resource.
For example, type EXCH_DG_RES.
- 5 On the **Properties** tab, in the **Disk Group Name** field, type the name of the disk group you previously created for the First Storage Group (for example, EVS1_SG1_DG), and click **OK** to close the dialog box.
- 6 To bring the resource online, right-click the newly named resource and click **Bring this resource online**.

Installing Exchange Server

Refer to the Microsoft documentation for prerequisites and details on installing a clustered mailbox server. You must install the Active Clustered Mailbox role on the first node and install the Passive Clustered Mailbox role on the failover node.

Make sure that the same drive letter and path are available on all nodes and have adequate space for the installation. For example, if you install the Exchange program files in `C:\Program Files\ExchSrvr` on one node, you must install the files in `C:\Program Files\ExchSrvr` on all the other nodes. Use a drive letter on the local disk of each node in the cluster.

For requirements when installing Exchange Server on a secondary site for disaster recovery, see the following topic:

See [“Creating a parallel environment for Exchange Server on the secondary site”](#) on page 85.

Adding the Volume Manager Disk Group resources to the Exchange group

Exchange 2007 installation creates an application group with resources required by Exchange. You need to move to the Exchange Group the Volume Manager Disk Group (VMDG) resource that you added to the cluster quorum group for the First Storage Group installation.

Also add to the Exchange group the Volume Manager Disk Group resources for any other disk groups that you created for Exchange.

To move the Volume Manager Disk Group resource to the application group

- 1 In the quorum group, right-click the resource you created for the Exchange First Storage Group and select the option to move it to another group.
- 2 Select the Exchange group as the target for the move and click **OK**.

To add Volume Manager Disk Group resources for the application

- 1 In the left pane (tree view) of the Failover Cluster Management tool, right-click the resource group under Services and Applications. Select **Add a resource > More resources > Add Volume Manager Disk Group**. A Volume Manager disk group resource is automatically created.
- 2 In the center panel under Disk Drives, double-click **New Volume Manager Disk Group** (in the center pane) to open the Properties dialog box. You can also right-click **New Volume Manager Disk Group** and select Properties.
- 3 In the **General** tab of the Properties dialog box, type the resource name for the New Volume Manager Disk Group (for example, ExchDG).
- 4 In the **Properties** tab, type the name of the disk group for which you want to add a resource.
- 5 Click **OK** to close the dialog box.
- 6 To bring the resource online, right-click the newly named disk group and click **Bring this resource online**.

Once the Volume Manager Disk Group resources are created, you can set the database dependencies.

See [“Setting the database dependency on the disk group resource”](#) on page 80.

Setting the database dependency on the disk group resource

After adding the Volume Manager Disk Group resources to the Exchange group, you must set the Exchange database resources to be dependent on them.

To set the database resource dependency on the VMDG resource

- 1 In Failover Cluster Management, select the Exchange resource group.
- 2 In the result pane, under **Other Resources**, right-click the appropriate database resource and select **Properties**.
- 3 In the **Dependencies** tab of the Properties dialog box:
 - Click the box **Click here to add a dependency**.
 - Select the appropriate Volume Manager Disk Group resource from the drop-down list of available resources.
 - Click **Insert**.
- 4 Click **OK** to close the Properties dialog box.
- 5 Repeat steps 2 through 4 for each additional database resource that exists in the Exchange group.

Moving Exchange databases and logs to shared storage

During Exchange installation, the First Storage Group is installed to a dynamic volume. You must move the log to a separate volume.

If you created any other Exchange storage groups that were not located on the SFW dynamic volumes, move them to the dynamic volumes.

For each Exchange 2007 storage group, set the log files path and system files path to point to the log volume. For each database, set the database path to point to the appropriate database volume.

You can use either the Exchange Management Console or the Exchange Management Shell cmdlets to specify log and database locations. You can specify locations when creating new storage groups or databases or change the locations for existing storage groups or databases.

Note: You cannot use the Exchange Management Console to change the log file location for remote Mailbox servers.

The following procedures can be used to change paths for existing storage groups and databases.

See the Microsoft Exchange 2007 documentation for additional information on creating new storage groups and databases.

To use the Exchange Management Console to change log file and system file locations for an existing database

- 1 On the server on which the storage group is located, launch Exchange Management Console from **Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Console** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
- 2 In the console tree, expand **Server Configuration**, and then click **Mailbox**.
- 3 In the result pane, click the Mailbox server that contains the storage group for which you want to change the log file location.
- 4 In the work pane, right-click the storage group for which you want to change the log file location and click **Move Storage Group Path**. The Move Storage Group Path wizard appears.
- 5 On the **Introduction** panel, click **Browse**, specify the SFW volume to which to move the log files, and create a folder for the log files. Repeat for the system files. The volume should be the same for both.
- 6 Click **Move**. A warning appears that all databases in the storage group must be temporarily dismounted, which will make them inaccessible to any user. To continue, click **Yes**.
- 7 On the **Completion** panel, confirm whether the path was changed successfully. A status of Completed indicates that the wizard completed the task successfully. A status of Failed indicates that the task was not completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes. Click **Finish** to complete the Move Storage Group Path wizard.

To use the Exchange Management Console to change the database file location for an existing database

- 1 On the server on which the storage group is located, launch Exchange Management Console from **Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Console** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.
- 2 In the console tree, expand **Server Configuration**, and then click **Mailbox**.
- 3 In the result pane, click the Mailbox server that contains the database for which you want to change the database file location.

- 4 In the work pane, right-click the desired database and click **Move Database Path**. The Move Database Path wizard appears.
- 5 On the **Introduction** panel, click **Browse**, specify the SFW volume to which to move the database file, and create a folder for it as needed.
- 6 Click **Move**. A warning appears indicating that the database must be temporarily dismounted, which will make it inaccessible to any user. To continue, click **Yes**.
- 7 On the **Completion** panel, confirm whether the database files were moved successfully. A status of Completed indicates that the wizard completed the task successfully. A status of Failed indicates that the task was not completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes. Click **Finish** to complete the Move Database Path wizard.

Verifying the Exchange Server group in the Microsoft cluster

You can verify your installation by moving the cluster between nodes to see if it fails over properly. The ultimate test of the cluster's failover capability involves shutting down the node that is currently online and bringing it back up after the cluster fails over to the other node.

Refer to the Microsoft documentation for instructions.

Configuring disaster recovery for Exchange Server in a Microsoft cluster

This chapter includes the following topics:

- [Tasks for configuring the secondary site for disaster recovery for Exchange](#)
- [Verifying the primary site configuration](#)
- [Creating a parallel environment for Exchange Server on the secondary site](#)
- [Installing Exchange on the secondary site](#)
- [Setting up the Exchange group on the secondary site](#)
- [Volume Replicator components overview](#)
- [Setting up security for Volume Replicator](#)
- [Creating resources for Volume Replicator](#)
- [Configuring Volume Replicator: Setting up an RDS](#)
- [Creating the RVG resource](#)
- [Setting the Exchange server resource dependency on the RVG resource](#)
- [Normal Volume Replicator operations and recovery procedures](#)

Tasks for configuring the secondary site for disaster recovery for Exchange

After creating a high-availability Microsoft cluster with SFW and Exchange Server on a primary site, you can configure a secondary site for disaster recovery.

This disaster recovery solution requires Symantec Storage Foundation Volume Replicator.

Refer to the *Symantec Storage Foundation Volume Replicator Administrator's Guide* for additional details on Volume Replicator.

[Table 8-1](#) describes the process for configuring the secondary site for disaster recovery.

Table 8-1 Process for configuring the secondary site for disaster recovery

Action	Description
Verify the primary site configuration.	See "Verifying the primary site configuration" on page 85.
Review the prerequisites and planning information	Verify the prerequisites on the secondary site. See "Requirements for deploying Exchange Server with SFW in a Microsoft cluster" on page 26. Note: If the DR site is on a different network segment, ensure that you allocate two IP addresses for the virtual server, one for the primary site and one for the DR site. Understand the DR configuration. See "Planning your disaster recovery configuration" on page 38.
Create the parallel Microsoft cluster configuration with SFW and Exchange 2007 on the secondary site	Many procedures are the same as on the primary site. However, there is a different procedure for installing Exchange and setting up the Exchange resource group. See "Creating a parallel environment for Exchange Server on the secondary site" on page 85.
Understand the Volume Replicator components	See "Volume Replicator components overview" on page 89.
Set up security for Volume Replicator	Set up the security for Volume Replicator on all nodes on both the primary and secondary sites. See "Setting up security for Volume Replicator" on page 90.

Table 8-1 Process for configuring the secondary site for disaster recovery
(continued)

Action	Description
Create the cluster resources for Volume Replicator	■ Create an IP address for the Replicated Volume Group (RVG). ■ Create a Network Name resource for the Replicated Volume Group (RVG). See “Creating resources for Volume Replicator” on page 92.
Set up an RDS	Create a replicated data set (RDS) using the Volume Replicator wizard. See “Configuring Volume Replicator: Setting up an RDS” on page 93.
Create the RVG resource (primary and secondary sites)	Create the RVG resource on both primary and secondary sites. See “Creating the RVG resource” on page 104.
Set up the Exchange Server resource dependencies	Change the Exchange Server resource dependency properties so that it depends on the RVG resource instead of the Volume Manager Disk Group resource. See “Setting the Exchange server resource dependency on the RVG resource” on page 105.

Verifying the primary site configuration

Before you can configure the secondary site, you set up the primary site for high availability.

See [“Workflow for a high availability \(HA\) configuration”](#) on page 16.

Ensure that you install the Volume Replicator option on the primary site. Ensure that you are using static IP addresses as required for Volume Replicator.

Creating a parallel environment for Exchange Server on the secondary site

After setting up an SFW environment with Microsoft failover clustering and Exchange Server 2007 on the primary site, configure a parallel environment for Exchange on the secondary site. Many tasks use the same procedures as on the primary site.

The following procedures are different on the secondary site:

- Install Exchange 2007

See [“Installing Exchange on the secondary site”](#) on page 87.

- Set up the Exchange group on the secondary site
 See [“Setting up the Exchange group on the secondary site”](#) on page 88.

Table 8-2 shows the full list of tasks in the recommended order, with guidelines specific to the secondary site. After completing these tasks you will have a clustered site with SFW and Exchange installed and configured on all the nodes on both the primary and the secondary sites. You can then proceed to configuring the Volume Replicator components for disaster recovery.

Table 8-2 Creating a parallel environment on the secondary site

Action	Description
Configure the storage hardware and network	Use the same procedure as on the primary site. See “Configuring the storage hardware and network” on page 43.
Establish a Microsoft failover cluster	Use the same procedure as on the primary site. See “Establishing a Microsoft failover cluster” on page 44.
Install SFW for a disaster recovery configuration	Use the same procedure as on the primary site. Be sure to select the option to install Volume Replicator. (This must also be installed on the primary site.) See “Installing SFW with Microsoft Failover Cluster option” on page 45.
Configure SFW disk groups and volumes,	Use the same procedure as on the primary site. Make sure the following are exactly the same as the cluster on the primary site: ■ Cluster disk group names ■ Volume names and sizes ■ Drive letters See “Tasks for configuring SFW storage” on page 47.
Implement a dynamic mirrored quorum resource	Use the same procedure as on the primary site. See “Tasks for implementing a dynamic mirrored quorum resource” on page 72.

Table 8-2 Creating a parallel environment on the secondary site (*continued*)

Action	Description
Add Volume Manager Disk Group resources for the Exchange 2007 disk group(s)	Use the same procedure as on the primary site. Unlike on the primary site, the resource will not be used during the Exchange 2007 installation but will be used in the process of recovering the existing database and log information from Active Directory after Exchange installation. See “Adding a Volume Manager Disk Group resource for Exchange 2007 installation” on page 77. If you created any other Exchange storage groups, include resources for those disk groups as well. See “Adding the Volume Manager Disk Group resources to the Exchange group” on page 79.
Install Exchange 2007	See “Installing Exchange on the secondary site” on page 87.
Set up the Exchange group	Unlike on the primary site, Exchange installation does not create the Exchange group and resources. However, after Exchange installation, you can run a command that recovers the resource information from Active Directory. See “Setting up the Exchange group on the secondary site” on page 88.
Move the Volume Manager Disk Group resources to the Exchange group	Use the same procedure as on the primary site. See “Moving Exchange databases and logs to shared storage” on page 80.

Installing Exchange on the secondary site

Review the following requirements for installing Exchange Server 2007 on the secondary site:

- Before you begin installation, make sure to take the Exchange cluster group offline on the primary site; otherwise, the installation on the secondary site will not function properly.

- On the secondary site nodes, do not install the Active Clustered Mailbox role. Instead, install the Passive Clustered Mailbox role on all nodes of the secondary site.
- Make sure that the same drive letter and path are available on all nodes and have adequate space for the installation. For example, if you install the Exchange program files in `C:\Program Files\ExchSrvr` on one node, you must install the files in `C:\Program Files\ExchSrvr` on all the other nodes. Use a drive letter on the local disk of each node in the cluster.

Refer to the Microsoft documentation for additional prerequisites and details on Exchange installation.

Setting up the Exchange group on the secondary site

Installing Exchange 2007 on the secondary site does not create the Exchange group and resources as it does on the primary site. However, after Exchange installation, you can use run the RecoverCMS command to recover the Exchange group and resource information from Active Directory.

To set up the Exchange group on the secondary site

- 1 On the secondary site, ensure that you have set up the cluster disk groups and dynamic volumes to match those on the primary site.
- 2 Ensure that you have created the Volume Manager Disk Group resources that correspond with the Exchange disk groups.
- 3 Ensure that the disk groups are online and volumes mounted on the node where you are going to run the RecoverCMS command.
- 4 Change to the directory where you installed Exchange.
- 5 Run the RecoverCMS command, using the following syntax:

```
Setup.com /recoverCMS /CMSName:<name>/CMSIPAddress:<ip>
```

Where *<name>* is the name you assigned to the Exchange server during installation on the primary site and *<ip>* is the IP assigned during Exchange installation on the primary site.

You may receive an error message due to a Microsoft issue that states the command failed to bring cluster resource Network Name online, and that the group or resource is not in the correct state to perform the requested operation.

In this case, complete the following steps on the secondary site:

- On the secondary site, using the Failover Management console, bring the clustered mailbox server (Network Name) resource online manually.

- After the Network Name resource comes online, take the IP resource offline. (This will also offline the Network Name resource.)
 - Delete the Network Name resource and the IP resource.
 - Run the RecoverCMS command over again. This time it will succeed and all the Exchange resources will be created on the secondary site.
- 6 On the secondary site, bring the Exchange cluster group and its resources offline.
- 7 On the primary site, bring the Exchange cluster group and its resources online.

Volume Replicator components overview

Table 8-3 describes the Volume Replicator components you must configure.

Table 8-3 Volume Replicator components

Component	Description
Replicated Volume Group (RVG)	An RVG is made up of one or more volumes in an SFW disk group. The updates made on the RVG on the primary host are sent to a configured secondary host. Thus, on the secondary host there is a corresponding RVG with a disk group of the same name and volumes with the same names. The data volumes should be the same size. Optionally, to add more redundancy, you can have multiple secondary hosts, all with the same corresponding copy of the RVG. An RVG within a disk group is the container for replication, so if you have multiple disk groups, you will need to create a separate RVG for each disk group. It is possible to have more than one RVG in a disk group; however, the RVG cannot span across disk groups.
Replicated Data Set (RDS)	An RVG on the primary host and any corresponding RVGs on the secondary host or hosts make up a Replicated Data Set (RDS).
Replicator Log volume	Each RVG must have a Replicator Log associated with it. The Replicator Log volume at the primary site holds a copy of any RVG updates that are sent to the secondary site. The Replicator Log on the secondary site is held in reserve so that it can be used if the primary site becomes nonfunctional and the secondary site needs to become the new primary site. The log volumes at the two sites must have the same name. Symantec recommends having Replicator Log volumes of the same size at the primary site and the secondary site.

Setting up security for Volume Replicator

As the first configuration step for Volume Replicator replication, you must configure the VVR Security Service (VxSAS) on all cluster nodes on both the primary and secondary sites. This procedure should not be done until you have installed SFW on all cluster systems. Otherwise, you will get an error message from the VxSAS wizard if you try to select a system without VCS installed.

You can run the VxSAS wizard from any site once SFW is installed on all cluster systems; at that time, you can run the wizard for both the primary and secondary site systems. The Microsoft cluster groups can be either online or offline.

Note the following prerequisites to configure the VxSAS service:

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

For details on this required service, see the *Symantec Storage Foundation Volume Replicator Administrator's Guide*.

To configure the VxSAS service

- 1 Launch the wizard from **Start > Programs > Symantec > Symantec Storage Foundation > Configuration Wizards > VVR Security Service Configuration Wizard** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

Alternatively, run `vxssascfg.exe` from the command prompt to launch the wizard.

Read the information provided on the Welcome page and click **Next**.

- 2 Complete the Account Information panel as follows:

Account name (domain\account)	Enter the administrative account name.
----------------------------------	--

Password	Specify a password
----------	--------------------

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

Click **Next**.

- 3 On the Domain Selection panel, select the domain to which the hosts that you want to configure belong:

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

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

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

Click **Next**.

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

Selecting hosts	The Available hosts pane lists the hosts that are present in the specified domain. Move the appropriate host from the Available hosts list to the Selected hosts list, either by double-clicking it or using the arrow button. Use the Shift key with the up or down arrow keys to select multiple hosts.
Adding a host	If the host name you require is not displayed, click Add host. In the Add Host dialog specify the required host name or IP in the Host Name field. Click Add to add the name to the Selected hosts list.

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

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

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

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

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

Creating resources for Volume Replicator

Create the resources for Volume Replicator replication at the primary and secondary sites using the Failover Cluster Management tool. You create a network name resource and IP address resource to be used for Volume Replicator replication.

A separate valid IP address is necessary for Volume Replicator replication, because on the secondary cluster before a disaster, the application IP must be offline whereas the Volume Replicator IP must be online.

You create the resources for the primary site and then repeat the procedure to create the resources on the secondary site.

To create a Network Name resource and IP address resource for VVR replication

- 1 Right-click on the application group and select **Add a Resource > Client Access Point**.
- 2 In the Client Access Point panel of the New Resource Wizard, specify the following:
 - In the **Name** field, specify a name for the Network Name resource. The default is the name of the group you selected. Specify any name except the node and the virtual server name. The network name you assign when creating the resource for the secondary site must be different from the network name for the primary site.
 - Select the network and specify the IP address.Click **Next**.
- 3 In the Confirmation panel, review the information and click **Next**.
- 4 When configuration is complete, click **Finish**.
- 5 Repeat the same procedure to create the IP and the Network Name resource at the secondary site.
- 6 Bring the resources online.

Configuring Volume Replicator: Setting up an RDS

For each disk group you created for the application, set up a Replicated Data Set (RDS) on the primary and secondary hosts. The Setup Replicated Data Set Wizard enables you to configure an RDS for both sites.

See [“Prerequisites for setting up the RDS”](#) on page 93.

See [“Creating a Replicated Data Set \(RDS\)”](#) on page 94.

Prerequisites for setting up the RDS

Before creating an RDS, check whether your setup meets the following prerequisites:

- Verify that VxSAS has been configured.
- Verify that the intended Primary host is connected to VEA, if you are configuring the RDS from a remote client or from a host that is not the Primary.
- Verify that you set the IP preference, whether Volume Replicator should use IPv4 or IPv6 addresses, before configuring replication. The default setting is IPv4.

When you specify host names while configuring replication, Volume Replicator resolves the host names with the IP addresses associated with them. This setting determines which IP protocol Volume Replicator uses to resolve the host names. Use Veritas Enterprise Administrator (VEA) (Control Panel > VVR Configuration > IP Settings tab) to set the IP preference.

- Verify that the data volumes and Replicator Log volume intended to be a part of the RDS are not of the following types, as Volume Replicator does not support the following types of volumes:
 - Storage Foundation for Windows (software) RAID-5 volumes
 - Volumes with the Dirty Region Log (DRL)
 - Volumes with a comma in their names
 - Secondary volume of a size smaller or greater than that on the Primary
 - Volume that is already being replicated
- For the Replicator Log volume, in addition to the above types, make sure that the volume does not have a DCM.

Creating a Replicated Data Set (RDS)

You can create the Replicated Data Set (RDS) in the following way.

To create the replicated data set

- 1 From the cluster node on the Primary where the cluster disk group is imported, launch the Veritas Enterprise Administrator (VEA).

Launch VEA from **Start > Programs > Symantec > Symantec Storage Foundation > Veritas Enterprise Administrator** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen. Then, connect to the local system.
- 2 In the tree in the left pane, right-click the **Replication Network** node and select **Setup Replicated Data Set**.
- 3 Read the information on the Welcome panel and click **Next**.

- 4 Complete the Enter names for the Replicated Data Set and Replicated Volume Group panel as follows:

Replicated Data Set name	Enter a name for the RDS. For example, specify EVS1_SG1_RDS.
Replicated Volume Group name	Enter a name for the RVG. The same name is used for the Primary and Secondary RVG. For example, specify EVS1_SG1_RVG.
Primary Host	By default the local host is selected. To specify a different host name, make sure that the required host is connected to the VEA console and select it in the Primary Host list. If the required host is not connected to the VEA, it does not appear in the list. In that case, use the VEA console to connect to the host.

Click **Next**.

- 5 Select the dynamic disk group and volumes to be replicated as follows.

Dynamic Disk Group	Select the appropriate dynamic disk group from the list. Multiple disk groups cannot be added in an RDS.
Select Volumes	Choose the required data volumes from the table by selecting the check boxes for the volumes. To select all the volumes, select the check box in the top left corner of the Select Volumes table. To select multiple volumes, press the Shift or Control key while using the Up or Down arrow key. By default, adds DCM logs with mirrored plexes for all selected volumes. If the disk space is inadequate for creating a DCM with mirrored plexes, a single plex is created.

Click **Next**.

- 6 Complete the Select or create a volume for Replicator Log panel by choosing one of the following:
 - To select an existing volume, select the volume in the table and click **Next**. If the volume does not appear in the table, click **Back** and verify that the Replicator Log volume was not selected on the previous page.
 - If you have not created a volume for the Replicator Log or want to create a new one, click **Create Volume**. Complete the information on the Create Volume dialog box as follows:

Name	Enter a name for the volume.
Size	Enter a size for the volume.
Layout	Select the appropriate volume layout.
Disks Selection	If you want Volume Replicator to select the disks for the Replicator Log, choose Select disks automatically. If you want to choose specific disks from the Available disks pane for the Replicator Log, choose Select disks manually. Either double-click on the disks or click Add to move the disks into the Selected disks pane.

Click **OK**. The volume is created and displayed in the Replicator Log panel.
Click **Next**. The summary panel appears.

- 7 Review the information on the summary panel. Click **Back** if you want to change any information.

Click **Create Primary RVG** to create the RVG.

- 8 After the Primary RVG has been created successfully, Volume Replicator displays the following message:

RDS with Primary RVG has been created successfully. Do you want to add Secondary host to this RDS for replication now?

Click **Yes** to add the Secondary host to the Primary RDS now. The Specify Secondary host for replication panel appears.

- 9 On the Specify Secondary host for replication panel, enter the name or IP address of the Secondary host. Click **Next**. If the Secondary host is not connected to VEA, the wizard tries to connect it when you click **Next**. Wait till the connection process is complete and then click **Next** again.
 - If the disk group with the required data volumes and the Replicator Log volume as on the Primary host does not exist on the Secondary, Volume Replicator displays a message. Read the message carefully.
 - The option to automatically create the disk group and the associated volumes on the Secondary host is available only as follows: If the required number of disks of the same type, having the same or a larger amount of space as on the Primary, are available on the Secondary. Otherwise, the wizard enables you to create the disk group and the volumes manually.
 - Click **Yes** to automatically create the disk group, data volumes, and Replicator Log. Any available disks are automatically chosen for creating the disk group on the Secondary host.

- Click **No** to manually create the disk group, data volumes, and Replicator Log. Complete the Create Dynamic Disk Group on Secondary host panel. If the dynamic disk group as on the Primary has already been created on the Secondary, then this panel does not appear. Complete the information on this panel as follows:

Create cluster group	Choose this option only if you need to create clustered disk groups. Select the required disks from the Available disks pane. Either double-click on the disks or click Add to move the disks into the Selected disks pane. To select all the available disks, choose the Add All option.
Create Dynamic Disk Group	Click the Create Dynamic Disk Group button to proceed with creating the disk group. A disk group with the same name as that on the Primary is created and the Next button is enabled.

After the disk group has been created, click **Next**. The Volume Information on connected hosts panel appears.
 Complete this panel as described in step 10.

- If only a disk group, without any data volumes or Replicator Log, as on the Primary host exists on the Secondary, Volume Replicator displays a message. Read the message carefully.
 - The option to automatically create the volumes on the Secondary host is available only as follows: If the disks that are part of the disk group have the same or a larger amount of space as on the Primary and enough space to create volumes with the same layout as on the Primary. Otherwise, the wizard enables you to create the required volumes manually.
 - Click **Yes** to automatically create the data volumes and the Replicator Log. After the configuration has been automatically created on the Secondary, proceed to step 11.
 - Click **No** to create the data volumes and the Replicator Log manually, using the Volume Information on connected hosts panel.
- 10 The Volume Information on connected hosts panel displays information on the availability of volumes on the Secondary nodes, if the Primary and Secondary hosts are connected to the VEA.

This panel does not appear if all the required volumes that are available on the Primary host are also available on the Secondary hosts.

If the required data volumes or the Replicator Log volume have not been created on the Secondary host, the panel displays the appropriate message against the volume name on the Secondary. Create the required volumes as follows:

- For each required volume that is not created, click **Create Volume**.
- The Create Volume dialog verifies the information on the Primary host and displays the volume name and the size.

Complete the information on this panel as follows:

Name	Displays the name specified for the Primary volume.
Size	Displays the size specified for the primary volume.
Layout	Lets you specify the volume layout. Select the appropriate volume layout depending on your requirement.
Disks Selection	Enables you to specify the disk selection method. Select the Select disks automatically option if you want Volume Replicator to select the disks. Select the Select disks manually option to use specific disks from the Available disks pane for creating the volume. Either double-click on it or select Add to move the disks into the Selected disks pane.

Click **OK** to create the required volume.

- Repeat the steps for each of the data volumes and Replicator Log that has not been created.
- After all volumes are created, the volume information panel is updated and the **Next** button is enabled. Click **Next**.

If the required volumes are created but are not eligible for replication, the reason for non-eligibility is indicated against the volume name.

The Volume Information on connected hosts panel enables the appropriate option to convert a non-eligible volume to a Volume Replicator acceptable format.

Complete the information on this panel as follows:

Recreate Volume	This option is enabled if the required data volume is available on the Secondary, but is of a size greater than the Primary volume. Clicking this option displays a message that prompts you to confirm that you want to recreate the volume. Warning: This operation first deletes the volume resulting in loss of the data that already exists on the volumes. Choose Yes to recreate the volume using the Create Volume dialog.
Remove DRL	This option is enabled if the required data volume is available on the Secondary but has a DRL. Clicking this option displays a message that prompts you to confirm that you want to remove the log. Click Yes to confirm the removal of DRL.
Remove DCM	This option is enabled if the required Replicator Log volume is available on the Secondary but has a DCM log. Clicking this option displays a message that prompts you to confirm if you want to remove the log. Click Yes to confirm the removal of the DCM log.
Expand Volume	This option is enabled if the required data volume is available on the Secondary but is of a smaller size than the Primary volume. Clicking this option displays a message that prompts you to confirm that you want to grow the volume. Click Yes to grow the volume to the required size.

After you have converted the non-eligible volumes to a Volume Replicator acceptable format, click **Next**.

If the volume on the Secondary is already a part of another RDS, the wizard does not let you proceed. If you want to use the same volume, you must either remove the corresponding Primary volume from the Primary RVG or delete the other RDS.

- 11 Complete the Edit replication settings panel to specify basic and advanced replication settings for a Secondary host as follows:
 - To modify the default values for the basic settings, select the required value from the drop-down list for each property, as follows:

Primary side IP	Displays the IP address on the Primary that is to be used for replication. If there is more than one IP address available for replication, you can choose the one that you want to use from the drop-down list. If the required IP address is not displayed in the list, edit the field to add the IP address.
-----------------	---

Secondary Side IP	Displays the IP address on the Secondary that is to be used for replication, if the Secondary is connected to VEA. If there is more than one IP address available for replication, you can choose the one that you want to use from the drop-down list. If the required IP address is not displayed in the list, edit the field to add the IP address.
Replication Mode	Select the required mode of replication; Synchronous, Asynchronous, or Synchronous Override. The default is synchronous override. Synchronous Override enables synchronous updates under typical operating conditions. If the Secondary site is disconnected from the Primary site, and write operations occur on the Primary site, the mode of replication temporarily switches to Asynchronous. Synchronous determines updates from the application on the Primary site are completed only after the Secondary site successfully receives the updates. Asynchronous determines updates from the application on the Primary site are completed after VVR updates in the Replicator Log. From there, VVR writes the data to the data volume and replicates the updates to the secondary site asynchronously. Note: If the Secondary is set to the synchronous mode of replication and is disconnected, the Primary data volumes with NTFS file systems may be displayed as MISSING.

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

The **DCM** option enables the Replicator Log protection for the Secondary host when the Replicator Log overflows, and the connection between the Primary and Secondary is lost. This option is available only if all the data volumes under the Primary RVG have a DCM Log associated with them.

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

In the case of the Bunker node. Replicator Log protection is set to Off, by default. Thus, if the Primary RLINK overflows due to the Bunker RLINK, then this RLINK is detached.

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

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

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

Primary RLINK Name This option enables you to specify a Primary RLINK name of your choice. If you do not specify any name, Volume Replicator assigns a default name.

Secondary RLINK Name This option enables you to specify a Secondary RLINK name of your choice. If you do not specify any name, Volume Replicator assigns a default name.

- To proceed without modifying the advanced replication settings, click **Next**. The Start Replication panel appears. Proceed to step [12](#).
- To specify advanced replication settings, click **Advanced**. Complete the Advanced Replication Settings panel as follows:

Latency Protection	By default, latency protection is set to Off. When this option is selected the High Mark Value and the Low Mark Value are disabled. Select the Fail or Override option to enable Latency protection. The Override option behaves like the Off option when the Secondary is disconnected and behaves like the Fail option when the Secondary is connected.
High Mark Value	This option is enabled only when Latency Protection is set to Override or Fail. It specifies the maximum number of pending updates by which the Secondary can be behind the Primary. The default value is 10000, but you can specify the required limit. To ensure that latency protection is most effective the difference between the high and low mark values must not be very large.
Low Mark Value	This option is enabled only when Latency Protection is set to Override or Fail. When the updates in the Replicator Log reach the High Mark Value, then the writes to the Primary continue to be stalled until the number of pending updates on the Replicator Log falls back to the Low Mark Value. The default value is 9950, but you can specify the required limit.
Protocol	UDP/IP is the default replication protocol. Choose TCP/IP or UDP/IP for a regular Secondary. If the storage on the Bunker Secondary is directly accessible from the Primary use the STORAGE protocol, otherwise use TCP/IP or UDP/IP. Note: If the replication protocol for the Bunker Secondary has been set to STORAGE, you can change it only by deleting and recreating the Bunker with the required protocol; UDP/IP or TCP/IP. You cannot change the STORAGE protocol using the Change Replication Settings option.
Packet Size(Bytes)	Default is 1400. Choose the required packet size for data transfer from the drop-down list. The default unit for the packet size is Bytes. You can set the packet size only if the protocol is UDP/IP. Some firewalls do not support packet sizes greater than 1400 bytes. To replicate across such a firewall, use the default packet size to make sure all the Volume Replicator operations function as required. You can also set the packet size to 1300 by selecting from the list. The minimum packet size that you can specify is 1100 bytes. Note: If you need to set a value for packet size different from the value provided in the list, use the command line interface.

Bandwidth	By default, Volume Replicator uses the maximum available bandwidth. To control the bandwidth that is used by Volume Replicator for replication, choose Specify Limit , and then specify the bandwidth limit in the field provided. The default unit is Mega bits per second (Mbps) and the minimum allowed value is 1 Mbps.
Enable Compression	Enable this option if you want to enable compression for the Secondary host.

After completing the Advanced Replication Settings panel, click **OK**. The wizard returns to the Edit Replication Settings panel. Click **Next**. The Start Replication panel appears.

12 Choose the appropriate option from the Start Replication panel as follows:

- To add the Secondary and start replication immediately, select the Start Replication with one of the following options:

Synchronize Automatically	For an initial setup, use this option to synchronize the Secondary and start replication. This setting is the default. When this option is selected, Volume Replicator by default performs intelligent synchronization to replicate only those blocks on a volume that the file system is using. If required, you can disable intelligent synchronization. Note: Intelligent synchronization is applicable only to volumes with the NTFS file systems and not to raw volumes or volumes with FAT/FAT32 file systems.
---------------------------	---

Synchronize from Checkpoint	If you want to use this method, then you must first create a checkpoint. If the Primary data volumes have a considerable amount of data , you may first want to synchronize the Secondary for existing data using the backup-restore method with checkpoint. After the restore is complete, use the Synchronize from Checkpoint option to start replication from checkpoint; this operation synchronizes the Secondary with the writes that happened when backup-restore was in progress.
-----------------------------	--

- To add the Secondary without starting replication, deselect the **Start Replication** option. You can start replication later by using the Start Replication option from the Secondary RVG right-click menu.

Click **Next** to display the Summary panel.

13 Review the information on the Summary panel.

Click **Back** to change any information you had specified or click **Finish** to add the Secondary to the RDS and exit the wizard.

Creating the RVG resource

To enable a disaster recovery setup, once Volume Replicator is configured you create the Replicated Volume Group (RVG) resource on the primary and secondary sites.

You add the RVG resource to the Exchange Server resource group.

You configure the RVG resource to depend on the Volume Replicator IP resource and on the appropriate Volume Manager Disk Group resource.

Since an RVG cannot span disk groups, if you have more than one disk group configured for the application, create a separate RVG resource for each disk group.

To create a Replicated Volume Group (RVG) resource

- 1 In Failover Cluster Management, expand Services and Applications, right-click the Exchange Virtual Server (EVS) group that you have created and select **Add a resource > More resources > Add Replicated Volume Group**.

The New Replicated Volume Group appears in the center panel under Disk Drives.

- 2 Right-click **New Replicated Volume Group** and click **Properties**.
- 3 On the General tab of the Properties dialog box, in the **Resource Name** field, type a name for the RVG resource.
- 4 On the Dependencies tab, add the dependencies for the RVG resource:
 - Click the box **Click here to add a dependency**
 - From the **Resource** drop-down list, select the network name you created for the RVG. Click **Insert**.
 - Click the box **Click here to add a dependency**
 - From the **Resource** drop-down list, select the Volume Manager Disk Group resource created for the application disk group. Click **Insert**.
- 5 On the Properties tab, specify the following:
 - In the **rvgName** field, type the same name that you assigned the RVG on the General tab.

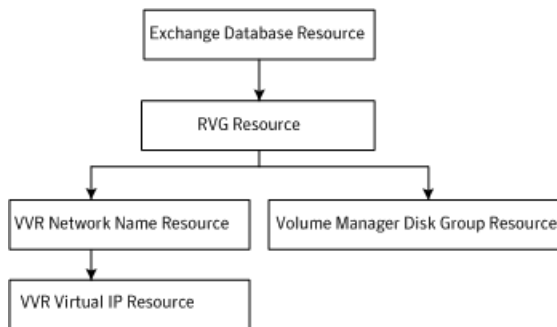
- In the **dgName** field, type the name assigned in the VEA to the application disk group.
- 6 Click **OK** to close the Properties dialog box.
 - 7 Right-click the RVG resource and click **Bring this resource online**.
 - 8 Repeat the same steps to create the RVG resource at the secondary site.

Setting the Exchange server resource dependency on the RVG resource

The Exchange Server resource is set to depend on a Volume Manager Disk Group resource that corresponded to the disk group created for the application. After you add the RVG resource for that disk group, you must change the dependency. You set the database resource to depend on the RVG resource instead.

You must set the dependency on the RVG resource on both primary and secondary sites.

Figure 8-1 Dependency graph for Exchange Server



To set the database resource dependency on the RVG resource

- 1 Make sure the application resource is offline before attempting to modify the dependencies. Right-click the resource and click **Take this resource offline**.
- 2 In Failover Cluster Management, select the Exchange resource group.
- 3 In the result pane, under **Other Resources**, right-click the appropriate database resource and select **Properties**.
- 4 In the **Dependencies** tab of the Properties dialog box:
 - Click the box **Click here to add a dependency**.

- Select the Replicated Volume Group resource from the drop-down list of available resources.
 - Select the Volume Manager Disk Group (VMDG) resource from the dependencies list and click **Delete**.
- 5 Click **OK** to close the Properties dialog box.
- 6 Repeat these steps for any additional database resources.

The cluster configuration is now complete. Bring online the entire application group on the primary cluster.

Normal Volume Replicator operations and recovery procedures

You perform normal Volume Replicator operations and recovery as described in the following topics:

- [Monitoring the status of the replication](#)
- [Performing planned migration](#)
- [Replication recovery procedures](#)

Monitoring the status of the replication

Under normal operating conditions you can monitor the status of the replication using the following:

- VEA GUI
- Command Line Interface (CLI)
- Performance Monitor (perfmon)
- Alerts

For details, refer to the *Symantec Storage Foundation Volume Replicator Administrator's Guide*.

Performing planned migration

You may want to migrate the application to the Secondary host for maintenance purposes and for testing the readiness of the Secondary host. The following procedure describes the generic set of tasks.

To migrate the application to the Secondary

- 1 Detach the user database. See the Microsoft documentation for instructions.
 Note that the `master`, `model`, and `tempdb`, databases cannot be detached.
- 2 Bring the RVG resource offline on both clusters.
- 3 Transfer the Primary role to the secondary using the Migrate option as follows:
 - From the VEA screen, right-click the Primary RVG and select **Migrate**.
 - Select the Secondary host and click **OK**. The replication role is migrated to the Secondary host.
- 4 Assign drive letters to the volumes on the new Primary. Ensure that these drive letters are the same as that of the original Primary.
- 5 Bring the RVG resource online on both the clusters.
- 6 Bring the Exchange group online on the new Primary.
- 7 Attach the databases. See the Microsoft documentation for instructions.

You can now verify that the application runs fine on the new Primary with the replicated data. After verifying, you can revert back the roles to its original state using the same set of tasks described above.

Any changes that you make to the data on the new Primary will get replicated to the original Primary, which is now the Secondary.

Replication recovery procedures

In the event of a disaster you must bring up an Exchange server on the secondary host.

Once the original primary host is functioning again, you can revert the Primary role back to the original primary host.

Bringing up the application on the secondary host

Use the following procedure to bring up Exchange Server on the secondary host if a disaster recovery scenario occurs on the primary host.

To bring up the application on the secondary host

- 1 From the left-pane in the VEA GUI console on the Secondary host, right-click on the desired secondary RVG node inside the replication network.
- 2 Select **Takeover** and follow the instructions in the wizard to perform the takeover operation.

You can choose to perform takeover with the following options:

- Perform the **Takeover with fast-fallback** option to restore the original Primary easily once it becomes available again. When performing Takeover with fast-fallback, make sure that you do not select the **Synchronize Automatically** option.
- Perform the **Takeover without fast-fallback** option. In this case, you need to perform a complete synchronization of the original Primary with the new Primary. This may take quite a while depending on the size of the data volume. Only after the synchronization is complete can you migrate the Primary role back to the original Primary.

After takeover, the existing Secondary becomes the new Primary.

- 3 Assign drive letters to the volumes on the new Primary. Ensure that these drive letters are the same as that of the original Primary.
- 4 Bring the Exchange group online.
- 5 Attach the databases. See the Microsoft documentation for instructions.

Now you can start using the application on the new Primary.

Restoring the primary host

After a disaster, if the original Primary becomes available again you may want to revert the role of the Primary back to this host.

To restore the Primary role to the original Primary host

- 1 Detach the user database. See the Microsoft documentation for instructions.
 Note that the `master`, `model`, and `tempdb`, databases cannot be detached.
- 2 Take the RVG resource offline on both the clusters.
- 3 Depending on whether you performed Takeover with or without fast-fallback option, do one of the following:

- For Takeover with the Fast-fallback option, the original Primary, after it has recovered, will be in the `Acting as Secondary` state. If the original Primary is not in the `Acting as Secondary` state, verify whether your network connection has been restored.

To synchronize this original Primary and the new Primary, use the **Resynchronize Secondaries** option from the right-click menu of the new Primary.

- For Takeover without the Fast-fallback option, after you have performed this operation, you must convert the original Primary to a Secondary using the **Make Secondary** option.

Before performing the **Make Secondary** operation, the original Primary's RVG and the new Primary's RVG will be shown in separate RDSs. However, after this operation they will be merged under a single RDS.

After the **Make Secondary** operation, the original Primary will be converted to a secondary. Right-click this secondary RVG and select **Start Replication** with **Synchronize Automatically** option.

- 4 After the synchronization is complete, perform a migrate operation to transfer the Primary role back to the original Primary. To do this, right-click the Primary RVG and select **Migrate** from the menu.
- 5 Ensure that the volumes have retained the same drive letters that existed before the disaster.
- 6 Bring the RVG resource online on the Secondary.
- 7 Bring the Exchange group online on the original Primary.
- 8 Attach the databases on the original Primary. See the Microsoft documentation for instructions.

Index

C

- campus cluster
 - connecting the nodes 45
 - disk groups 51
 - overview 12
 - sample configuration 51
 - volumes 51
 - Vxclus 38
 - workflow 18
- creating RDS
 - procedure 94

D

- dependency
 - setting on disk group resource 80
- disaster recovery
 - overview 13
 - volumes for Volume Replicator 53
 - workflow 22
- disk group resource
 - adding for Exchange Server installation 77
 - adding for quorum 74
- Disk groups
 - creating 54
- disk groups
 - campus cluster 51
 - planning 48
 - quorum 73
- disk space requirements 28
- DNS settings 43

E

- Exchange installation 78
- Exchange Server
 - verifying the cluster 82

F

- failover verification 82

H

- high availability
 - overview 11
 - workflow 16

I

- installation
 - SFW installation on cluster 45
- IP address resource for Volume Replicator 92

M

- mirrored volume for quorum 73
- moving Exchange databases and logs to shared storage 80

N

- Network Name resource
 - RVG 92
- network settings 43

Q

- quorum
 - adding resource for disk group 74
 - arbitration settings 45
 - changing to dynamic mirrored quorum resource 74
 - cluster ownership concepts 37
 - concepts 37
 - disk group 73
 - implementing dynamic mirrored 72
 - recommended device configuration 31
 - volume 73

R

- replicated data set 93
- replication
 - creating a Replicated Volume Group (RVG) resource 104
 - setting up RDS 93

- requirements
 - SFW installation 29
 - software 26
 - system 28
- resource
 - adding for quorum 74
 - Exchange Server resource group 77
 - quorum 72
 - RVG 104
- rolling installation 45
- RVG Network Name resource 92

S

- sample configurations
 - campus cluster 51
 - high availability 30
- security for Volume Replicator 90
- setting bandwidth
 - using RDS wizard 94
- SFW
 - installing on Microsoft cluster 45
- software requirements 26
- storage hardware 43
- supported OS
 - server components 27
- system requirements 28

V

- Volume Manager Disk Group resource 77
 - adding for quorum 74
- Volume Manager Disk Group resources
 - adding to the Exchange group 79
- Volume Replicator
 - creating RVG resource 104
 - IP address resource 92
 - Network Name resource 92
 - setting up RDS 93
 - volumes 53
 - VxSAS service 90
- volumes
 - campus cluster 51
 - considerations for Volume Replicator 53
 - creating 57
 - planning 48
 - quorum 73
- Vxclus utility 38
- VxSAS service 90