Storage Foundation and High Availability 7.4 Solutions Microsoft Clustering Solutions Guide for Microsoft SQL Server - Windows

VERITAS™

Last updated: 2018-05-31

Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas 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. Refer to the third-party legal notices document accompanying this Veritas product or available at:

https://www.veritas.com/about/legal/license-agreements

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 Veritas Technologies LLC 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. VERITAS TECHNOLOGIES LLC 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas 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.

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

doc.feedback@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 Introducing SFW solutions for a Microsoft cluster 7

About Microsoft clustering solutions with SFW 7
Advantages of using SFW in a Microsoft cluster 8
About high availability clusters 8
About campus clusters 9
About disaster recovery clusters 10

Chapter 2 Planning for deploying SQL Server with SFW in a Microsoft cluster 13

InfoScale requirements for Microsoft clustering solutions 13
Planning your SQL Server high availability configuration 15
Sample high availability configuration for SQL Server with SFW 16
Configuring the quorum device for high availability 17
Planning your campus cluster configuration 17
Microsoft campus cluster failure scenarios 20
Microsoft cluster quorum and quorum arbitration 22
Planning your disaster recovery configuration 24
Sample disaster recovery configuration for SQL Server with SFW and Volume Replicator 27

Chapter 3 Workflows for deploying SQL Server with SFW in a Microsoft cluster 29

Workflow for a high availability (HA) configuration 29
Workflow for a campus cluster configuration 31
Campus cluster: Connecting the two nodes 34
Workflow for a disaster recovery configuration 34
Using the Solutions Configuration Center workflow 38
Configuring the storage hardware and network 38

Chapter 4 Configuring SFW storage 40

Tasks for configuring InfoScale Storage 40
Planning for SFW cluster disk groups and volumes 41
Sample SQL Server high-availability cluster storage configuration 43
Sample campus cluster storage configuration 45
Sample SQL Server disaster recovery storage configuration 45
Considerations when creating disk groups and volumes for a campus cluster 47
Considerations when creating volumes for a DR configuration using Volume Replicator replication 48
Viewing the available disk storage 49
Creating dynamic cluster disk groups 49
Adding disks to campus cluster sites 52
Creating dynamic volumes for high availability clusters 52
Creating dynamic volumes for campus clusters 57

Chapter 5 Implementing a dynamic mirrored quorum resource 63

Tasks for implementing a dynamic mirrored quorum resource 63
Creating a dynamic cluster disk group and a mirrored volume for the quorum resource 64
Adding a Volume Manager Disk Group resource for the quorum 65
Changing the quorum resource to a dynamic mirrored quorum resource 65

Chapter 6 Installing SQL Server and configuring resources 67

Tasks for installing and configuring SQL Server 67
Creating the resource group for the SQL Server instance 68
Prerequisites for installing SQL Server 69
Installing SQL Server in an InfoScale Storage environment 70
Dependency graph for SQL Server 71
Verifying the SQL Server group in the Microsoft cluster 72

Chapter 7 Configuring disaster recovery 73

Tasks for configuring the secondary site for disaster recovery for SQL Server 73
Verifying the primary site configuration 75

Creating a parallel environment for SQL Server on the secondary site 75
Volume Replicator components overview 76
Setting up security for Volume Replicator 77
Creating resources for Volume Replicator 79
Configuring Volume Replicator: Setting up an RDS 79
Prerequisites for setting up the RDS 80
Creating a Replicated Data Set (RDS) 80
Creating the RVG resource 91
Setting the SQL server resource dependency on the RVG resource 92
Normal Volume Replicator operations and recovery procedures 93
Monitoring the status of the replication 93
Performing planned migration 93
Replication recovery procedures 94

Appendix A Configure InfoScale Storage in an existing Microsoft Failover Cluster 97

Configuring InfoScale Storage in an existing Microsoft Failover Cluster 97

Chapter 1

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 Microsoft clustering solutions with SFW

Microsoft clustering may be used with 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 *Dynamic Multi-Pathing Administrator's 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.

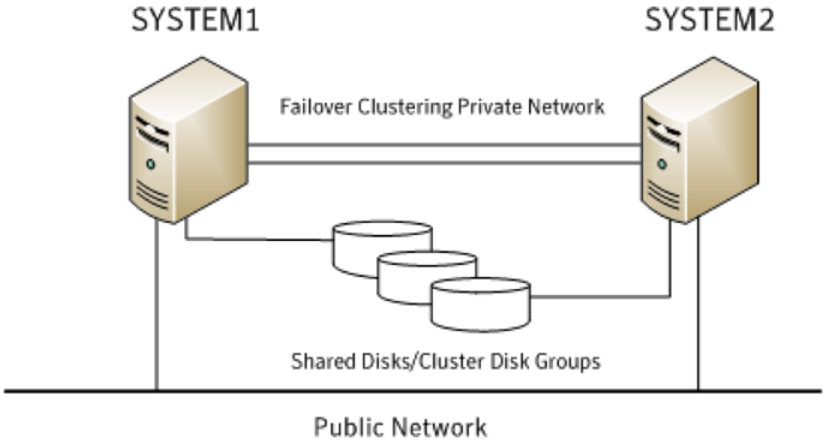
A cluster is a group of independent computers working together as a single system to ensure that mission-critical applications and resources are highly available. The cluster is managed as a single system, shares a common namespace, and is specifically designed to tolerate component failures and to support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

The following figure 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.

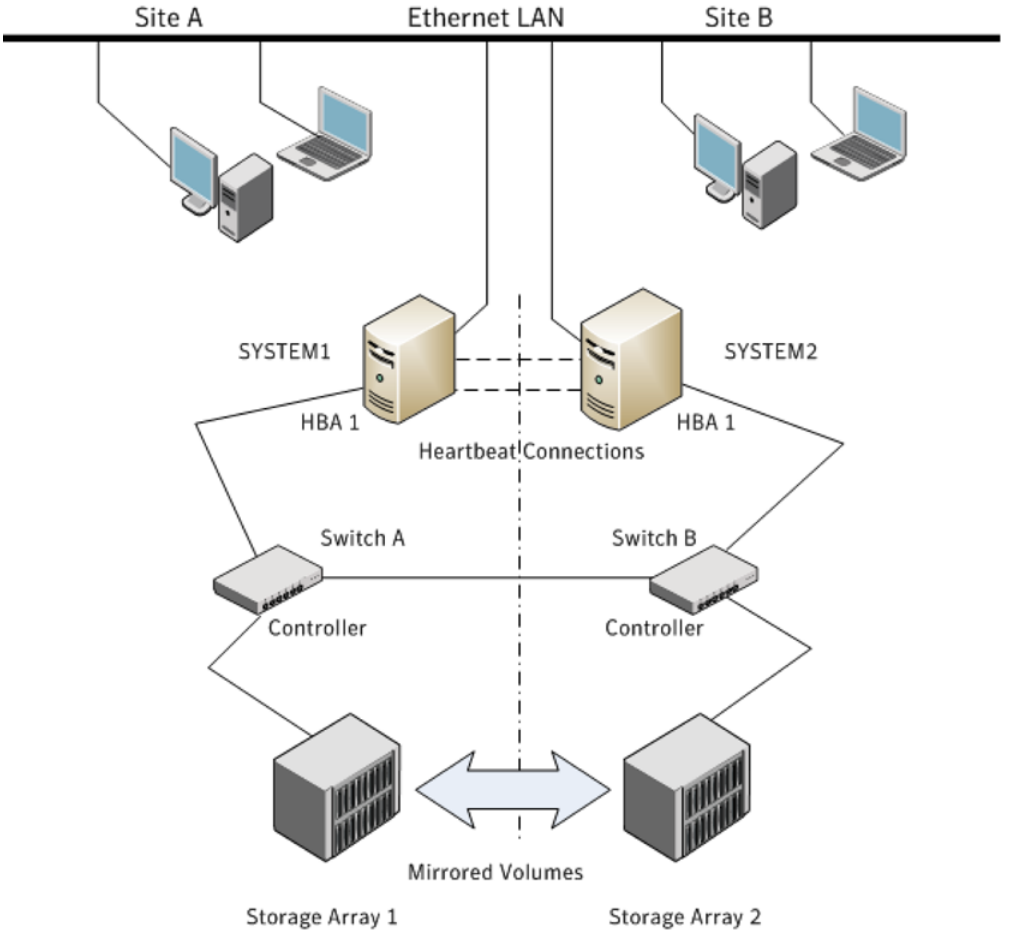
Typical campus clusters involve two sites; you can use more than two sites for additional redundancy.

This environment also provides a simpler solution for disaster recovery than a more elaborate InfoScale 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.

The following figure 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.

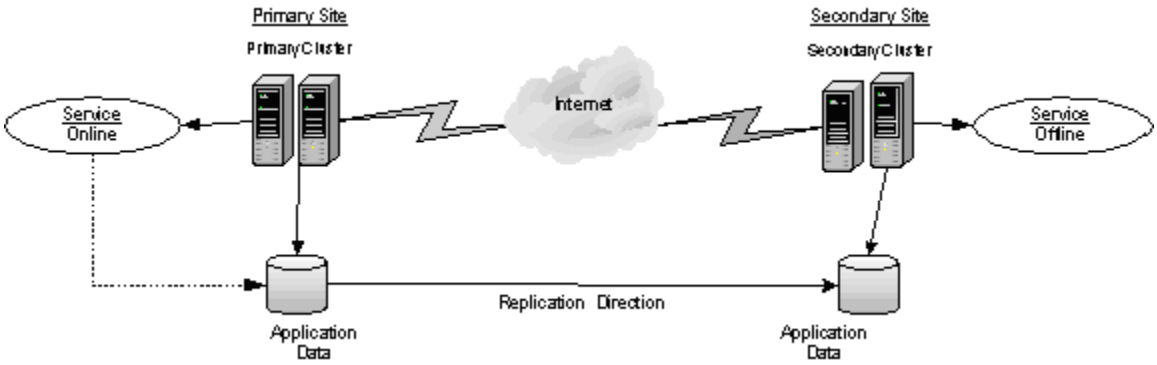
Using Volume Replicator with Microsoft clustering provides a replicated backup of your application data, which can be used for recovery after an outage or disaster. However, this solution does not provide the automated failover capability for disaster recovery that can be achieved using Volume Replicator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

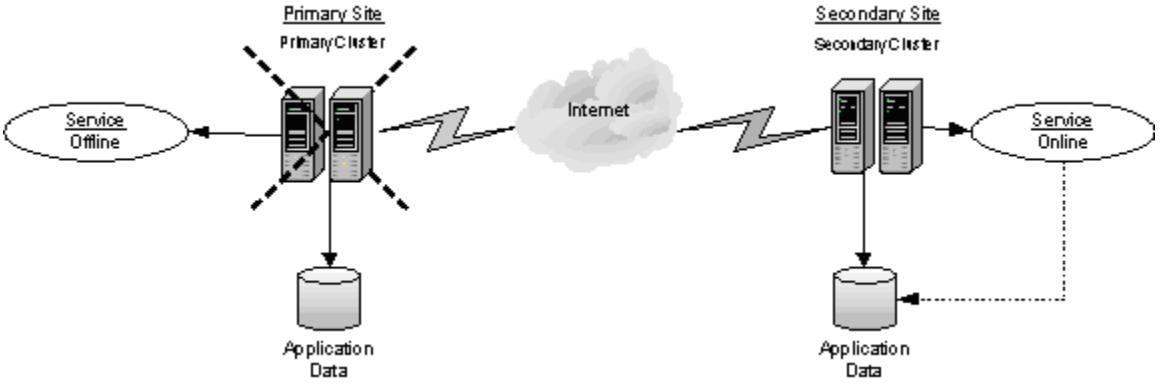
The following figure shows an example disaster recovery configuration before a failure.

Figure 1-3 Disaster recovery configuration



The following figure shows an example disaster recovery configuration after a failure.

Figure 1-4 Disaster recovery after a failure



Chapter 2

Planning for deploying SQL Server with SFW in a Microsoft cluster

This chapter includes the following topics:

- InfoScale requirements for Microsoft clustering solutions
- Planning your SQL Server high availability configuration
- Planning your campus cluster configuration
- Planning your disaster recovery configuration

InfoScale requirements for Microsoft clustering solutions

Refer to Microsoft documentation for Microsoft cluster requirements.

Use the following requirements as a guideline for InfoScale Storage with Microsoft SQL Server in a Microsoft cluster:

- One CD-ROM drive accessible to the system on which you are installing InfoScale Storage.
- Each system requires 1 GB of RAM for SFW.
- The storage disks must be shared between the cluster nodes.

Note: In a Microsoft Azure environment you cannot configure shared storage. Microsoft Azure does not support provisioning of shared disks. Due to this Microsoft limitation, in an Azure environment, InfoScale Storage cannot be used in cluster configurations that require shared storage.

- 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). Veritas 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.
- Microsoft clustering requires at least two disks for SQL, one for SQL database files and one for SQL 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.
- InfoScale Storage requires administrator privileges to install the software.
- Installing InfoScale Storage requires a reboot, but a reboot on the active cluster node causes it to fail over. Therefore, use a "rolling install" procedure to install InfoScale Storage first on the inactive cluster node. Then move the cluster resources to the other node and install on the now inactive node.
- 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, corresponding Volume Manager Disk Group (VMDg) resources are added to the cluster, under the available storage. The VMDg resource name corresponds to the cluster disk group name. You can then assign any of these resources to an application service group.

Note: You can install the Microsoft Failover Cluster option 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 *Veritas InfoScale Installation and Upgrade Guide*.

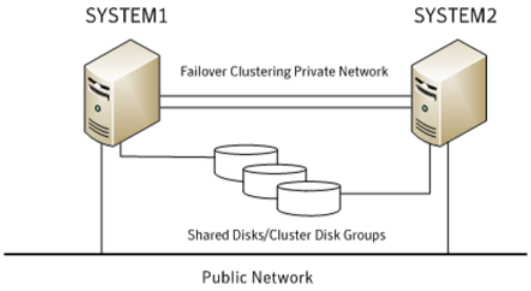
Planning your SQL Server high availability configuration

You can configure InfoScale Storage and SQL Server in a Microsoft cluster for high availability on a single site.

In the example high availability configuration, you create a virtual server in an active/passive SQL Server configuration on a Microsoft cluster. The active node of the cluster hosts the virtual server. The second node is a dedicated redundant server able to take over and host the virtual server in the event of a failure on the active node. In a high availability configuration both nodes are located on the same site.

The following figure illustrates a typical two-node active/passive configuration.

Figure 2-1 High availability active/passive configuration



The following are some key points about the configuration:

- The SQL virtual server is configured on the active node (SYSTEM1). If SYSTEM1 fails, SYSTEM2 becomes the active node and the SQL virtual server comes online on SYSTEM2.
- One or more application virtual 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 SQL databases are configured on the shared storage on volumes contained in one or more cluster disk groups.
- InfoScale Storage enables you to create a dynamic mirrored quorum. If the quorum resource fails, the mirror takes over for the resource.
  In this configuration, Veritas 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.
- InfoScale Storage enables you to add fault-tolerance to data volumes. Veritas 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
- SQL virtual server IP address, which should be the same on all nodes

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

Sample high availability configuration for SQL Server with SFW

The example configuration includes the dynamic mirrored quorum and requires setting up two or more dynamic cluster disk groups in SFW—one or more cluster disk groups for the application and data and one for the dynamic mirrored quorum.

The following names describe the objects created and used during the installation and configuration.

Name	Object
SYSTEM1 & SYSTEM2	server names
SQL_GROUP	Microsoft SQL Server resource group
SQLCLUST	Microsoft cluster for SQL Server high availability
SQLVS	Microsoft SQL Server virtual server
INST1	Microsoft SQL Server instance name

INST1_DG	disk group for Microsoft SQL Server volumes
INST1_SYS_FILES	volume for Microsoft SQL Server system data files
INST1_DB1_VOL	volume for storing a Microsoft SQL Server user-defined database
INST1_DB1_LOG	volume for storing a Microsoft SQL Server user-defined database log file
QUORUM_DG	disk group for quorum volume
SQL_QRM	volume for storing the Microsoft cluster quorum

More information is available on disk group and volume configuration.

See "Planning for SFW cluster disk groups and volumes" on page 41.

Configuring the quorum device for high availability

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

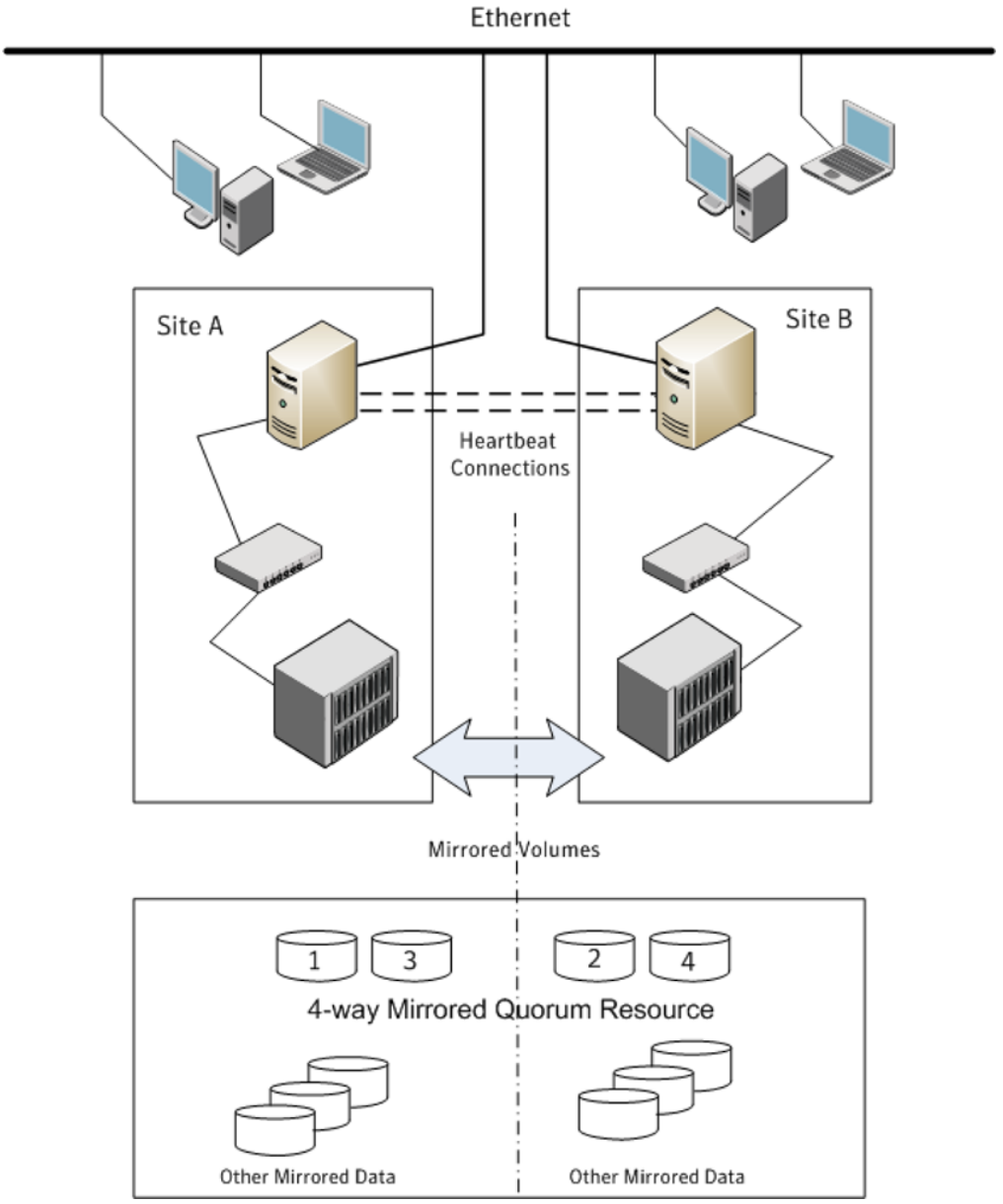
See "Planning for SFW cluster disk groups and volumes" on page 41.

Although a campus cluster setup with Microsoft clustering can work without InfoScale Storage, InfoScale Storage 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.

The following figure shows a Microsoft 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 2-2 Typical campus clustering configuration



Microsoft campus cluster failure scenarios

Different failure and recovery scenarios can occur with a Microsoft campus cluster and InfoScale Storage 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 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 22.

The following table lists failure situations and the outcomes that occur.

Table 2-1 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 2-1 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 2-1 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 23.

- See "Cluster ownership of the quorum resource" on page 23.
- See "The vxclus utility" on page 24.

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 Internet Protocol (IP) 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 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 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 *Storage Foundation 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

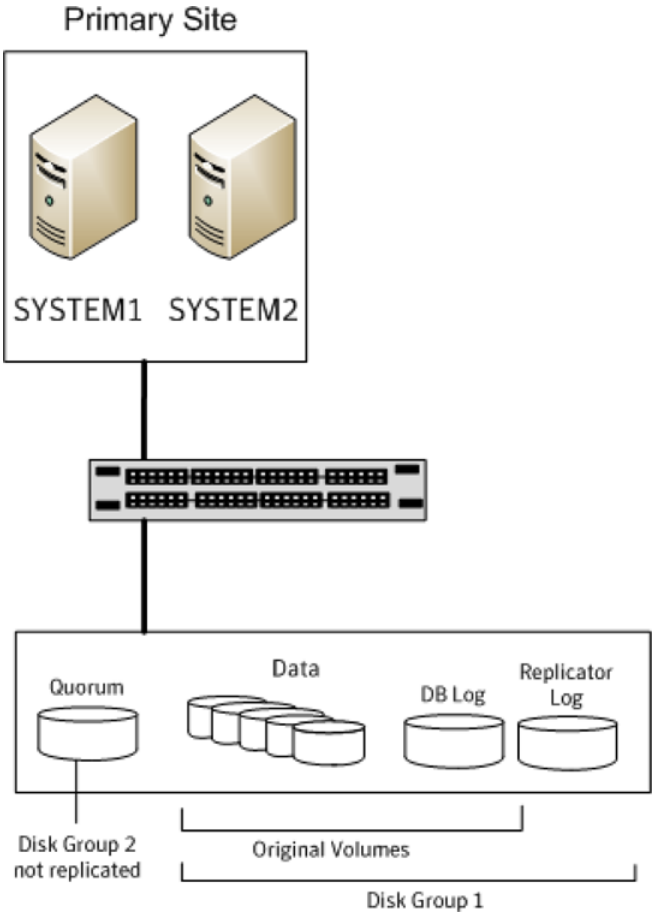
After creating a high-availability cluster on a primary site, you can configure a secondary site cluster for disaster recovery.

This disaster recovery solution requires 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.

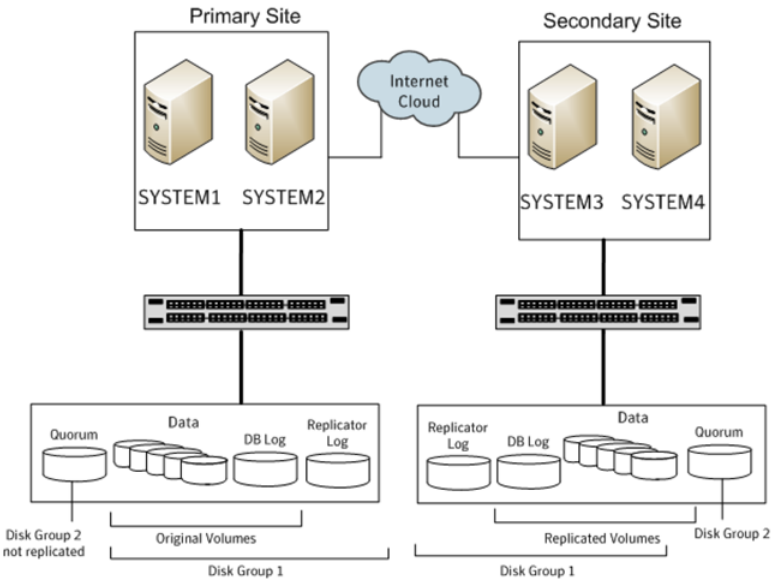
The following figure illustrates the cluster configuration on the primary site.

Figure 2-3 DR configuration primary site



The following figure shows the primary and secondary site configuration.

Figure 2-4 DR configuration both sites



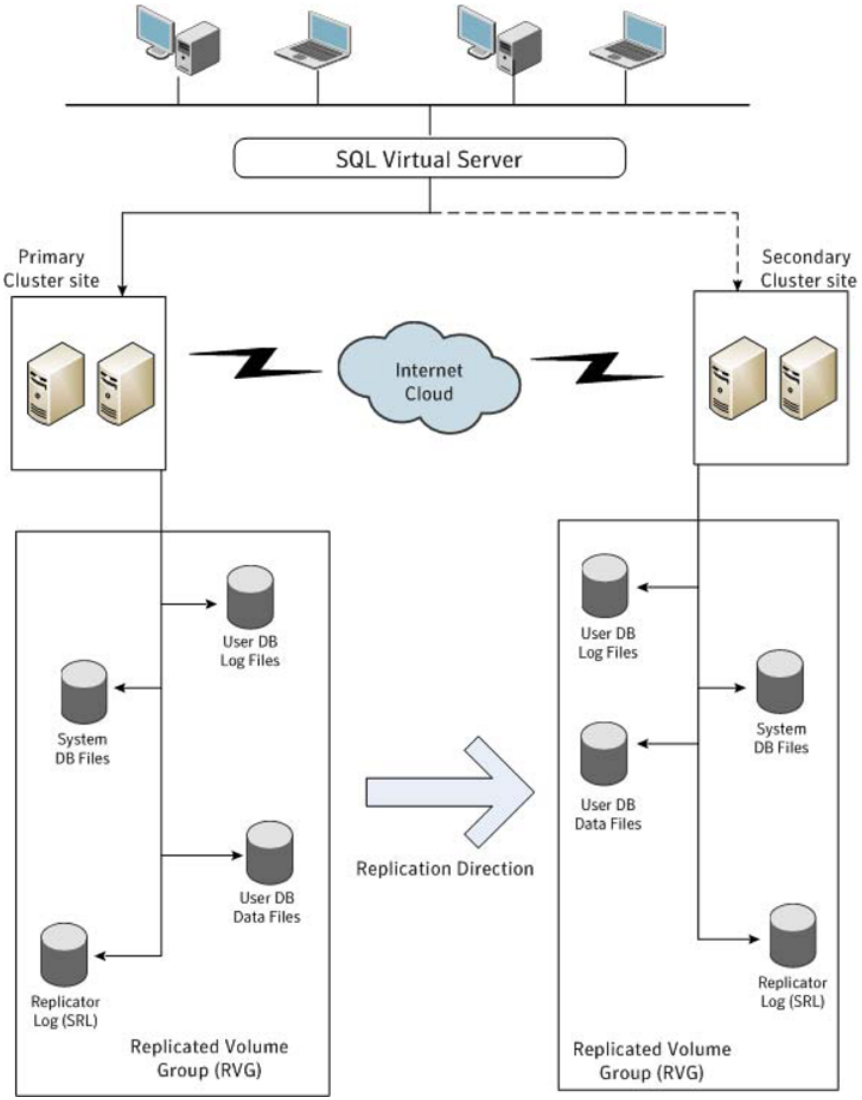
The quorum disk group is created separately on each site; it does not get replicated because each cluster has its own quorum.

More information is available on disk group and volume configuration.

See "Planning for SFW cluster disk groups and volumes" on page 41.

The following figure shows details on the configuration of the Volume Replicator Replicated Volume Group. The Microsoft SQL Server application data is stored on the volumes that are under the control of the RVG.

Figure 2-5 Typical Volume Replicator RVG configuration



Sample disaster recovery configuration for SQL Server with SFW and Volume Replicator

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

The following names describe the objects created and used when configuring two sites for disaster recovery with SFW and Volume Replicator on a Microsoft cluster.

Primary Site	
SYSTEM1 & SYSTEM2	server names
SQL_GROUP	Microsoft SQL Server virtual server group
SQLCLUST	Microsoft cluster
SQLVS	Microsoft SQL Server virtual server
SQL_IP	Microsoft SQL virtual server IP address resource
INST1	Microsoft SQL Server instance name
INST1_DG	disk group for Microsoft SQL volumes
INST1_SYS_FILES	volume for Microsoft SQL Server system data files
INST1_DB1_VOL	volume for storing a Microsoft SQL Server user-defined database
INST1_DB1_LOG	volume for storing a Microsoft SQL Server user-defined database log file
QUORUM_DG	quorum volume disk group for mirroring the quorum
SQL_QRM	volume for storing the Microsoft cluster quorum
Secondary Site	
SYSTEM3 & SYSTEM4	first and second nodes of the secondary site
All the other parameters are the same as on the primary site.	
DR Components	
INST1_RDS	Volume Replicator Replicated Data Set (RDS) name
INST1_RVG	Volume Replicator Replicated Volume Group (RVG) name
INST1_REPLOG	Volume Replicator Replicator log volume
INST1_RVG_RES	Replicated Volume Group Resource name
VVR_IP	SQL RVG IP address resource

Chapter 3

Workflows for deploying SQL 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
- Configuring the storage hardware and network

Workflow for a high availability (HA) configuration

You can install and configure InfoScale Storage and SQL Server in a Microsoft cluster for high availability on a single site.

Table 3-1 Process for deploying SQL Server with InfoScale Storage in a Microsoft high-availability cluster

Action	Description
Understand the configuration	See "Planning your SQL Server high availability configuration" on page 15.

Table 3-1 Process for deploying SQL Server with InfoScale Storage 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 SQL will be installed. See "Configuring the storage hardware and network" on page 38.
Establish a Microsoft cluster	Establish the cluster before installing InfoScale Storage.
Install InfoScale Storage with the Microsoft Failover Cluster option	Refer to the *Veritas InfoScale Installation and Upgrade Guide*.
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 InfoScale Storage" on page 40. **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. ■ Verify that a Volume Manager Disk Group (VMDG) resource is created for the quorum disk group. See "Tasks for implementing a dynamic mirrored quorum resource" on page 63.
Create the SQL virtual server resource group	■ Create a SQL Server resource group in the cluster. ■ Add the VMDG disk group resource(s). See "Creating the resource group for the SQL Server instance" on page 68.

Table 3-1 Process for deploying SQL Server with InfoScale Storage in a Microsoft high-availability cluster *(continued)*

Action	Description
Install SQL Server	■ Mount the disk group and volumes created for the data files on the node where you install. ■ Install the software. Ensure that you install the data files to the path of the dynamic volume on shared storage. See "Installing SQL Server in an InfoScale Storage environment" on page 70. ■ Verify the resource dependencies. See "Dependency graph for SQL Server" on page 71.
Verify the cluster configuration	Move the online SQL Server cluster group to the second node and back to the first node. See "Verifying the SQL Server group in the Microsoft cluster" on page 72.

Workflow for a campus cluster configuration

You can install and configure InfoScale Storage and SQL 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 3-2 Process for deploying SQL Server with InfoScale Storage in a Microsoft campus cluster

Action	Description
Understand the configuration	See "Planning your campus cluster configuration" on page 17.
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment. ■ Verify the DNS entries for the systems on which SQL will be installed. See "Configuring the storage hardware and network" on page 38.
Establish a Microsoft cluster	Connect the two campus cluster nodes after setting up the Microsoft cluster. See "Campus cluster: Connecting the two nodes" on page 34.
Install InfoScale Storage with the Microsoft Failover Cluster option	Refer to the *Veritas InfoScale Installation and Upgrade Guide*.
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 InfoScale Storage" on page 40. 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 47. 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 52. **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 3-2 Process for deploying SQL Server with InfoScale Storage in a Microsoft campus 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 63.
Create the SQL virtual server group	■ Create a SQL Server cluster group. ■ Add the VMDG disk group resource(s). See "Creating the resource group for the SQL Server instance" on page 68.
Install SQL Server	■ Mount the disk group and volumes created for the data files on the node where you install. ■ Install the software. Ensure that you install the data files to the path of the dynamic volume on shared storage. See "Installing SQL Server in an InfoScale Storage environment" on page 70. ■ Verify the resource dependencies. See "Dependency graph for SQL Server" on page 71.
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.

Table 3-2 Process for deploying SQL Server with InfoScale Storage in a Microsoft campus cluster *(continued)*

Action	Description
Verify the cluster configuration	Move the online SQL Server cluster group to the second node and back to the first node. See "Verifying the SQL Server group in the Microsoft cluster" on page 72.

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.

Workflow for a disaster recovery configuration

After creating a high-availability cluster on a primary site, you can install and configure InfoScale Storage and SQL Server on a secondary site cluster for disaster recovery.

This disaster recovery solution requires Volume Replicator.

Table 3-3 Process for deploying SQL 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 29.
Review the prerequisites and planning information	Verify the prerequisites on the secondary site. See "InfoScale requirements for Microsoft clustering solutions" on page 13. **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 24.
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 SQL Server resource group, and SQL Server installation. See "Creating a parallel environment for SQL Server on the secondary site" on page 75.
Configure the storage hardware and network	■ Set up the storage hardware for a cluster environment. ■ Verify the DNS entries for the systems on which SQL will be installed. See "Configuring the storage hardware and network" on page 38.
Establish a Microsoft cluster	Establish the cluster before installing InfoScale Storage.
Install InfoScale Storage with the Microsoft Failover Cluster option	Refer to the *Veritas InfoScale Installation and Upgrade Guide*.

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

Action	Description
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 InfoScale Storage" on page 40. **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 63.
Create the SQL virtual server group	■ Create a SQL Server cluster group. Ensure that it has the same name as on the primary site. ■ Add the VMDG disk group resource(s). See "Creating the resource group for the SQL Server instance" on page 68.

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

Action	Description
Install SQL Server	Before starting the SQL installation on the secondary site, note the following requirements: ■ Make sure that you take the SQL Server Network Name resource offline on the primary site. This will also offline the dependent resources. ■ Mount the disk group and volumes created for the data files on the node where you install. ■ During installation, specify the same name for the SQL virtual server as that on the primary site. ■ Ensure that you install the data files to the path of the dynamic volume on shared storage. See "Installing SQL Server in an InfoScale Storage environment" on page 70.
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 77.
Understand the Volume Replicator components	See "Volume Replicator components overview" on page 76.
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 79.
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 79.
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 91.
Set up the SQL Server resource dependencies	Change the SQL Server resource properties so that it depends on the RVG resource instead of the Volume Manager Disk Group resource. See "Setting the SQL server resource dependency on the RVG resource" on page 92.

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** > **All Programs** > **Veritas** > **Veritas 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 SQL Server.
3. Click to expand the Microsoft Campus Cluster workflow.

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, Veritas 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.

Chapter 4

Configuring SFW storage

This chapter includes the following topics:

- Tasks for configuring InfoScale 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

Tasks for configuring InfoScale Storage

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

The following table lists the tasks for configuring disk groups and volumes.

Table 4-1 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 41. 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 47. See "Considerations when creating volumes for a DR configuration using Volume Replicator replication" on page 48.
Configure disk groups	Use the VEA console to create disk groups. See "Creating dynamic cluster disk groups" on page 49. **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 52.
Configure volumes	Use the VEA console to create volumes. See "Creating dynamic volumes for high availability clusters" on page 52. See "Creating dynamic volumes for campus clusters" on page 57.
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.

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, Veritas 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, Veritas 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 47.

- See "Considerations when creating volumes for a DR configuration using Volume Replicator replication" on page 48.

Sample SQL Server high-availability cluster storage configuration

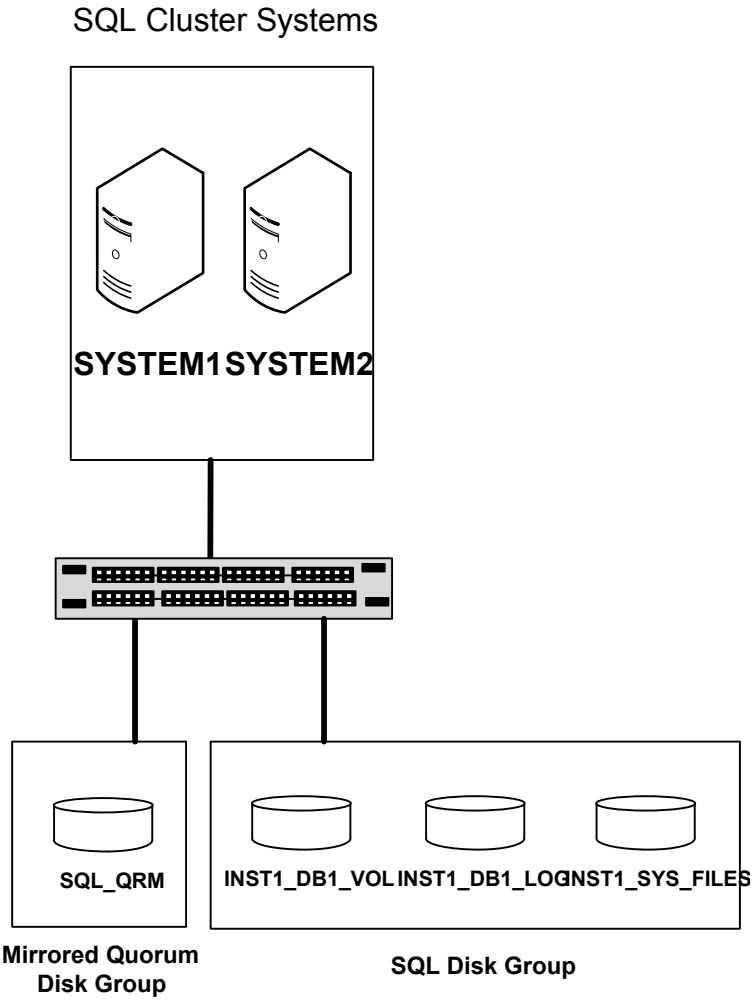
The number of disk groups for SQL Server depends on the planned organization of the data. The application program files need to be installed on the local drive of the server. Data files and other related files, such as logs, or FILESTREAM filegroups (if implemented), are placed on the shared storage in a cluster disk group.

Veritas recommends that you place database files, log files, and FILESTREAM filegroups on separate volumes.

You create at least one disk group for the system data files. You may want to create additional disk groups for user databases.

The following figure shows an example configuration of the disk groups and volumes for SQL Server in a Microsoft cluster environment.

Figure 4-1 SFW disk groups and volumes for SQL in a Microsoft high-availability cluster



SQL disk group INST1_DG contains the following volumes:

- INST1_DB1_VOL contains the SQL database. Each database typically resides on a separate volume.
- INST1_DB1_LOG contains the transaction log.
- INST1_SYS_FILES contains the volume for Microsoft SQL Server system data files.

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

Note: If FILESTREAM is implemented, the configuration should also contain a separate volume for the FILESTREAM filegroup.

Sample campus cluster storage configuration

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

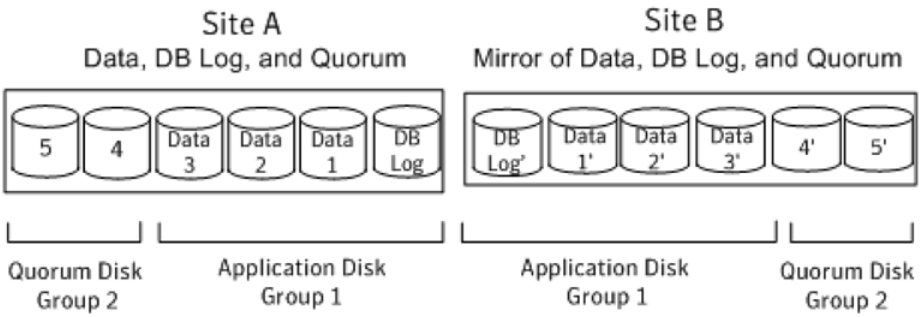
See "Sample SQL Server high-availability cluster storage configuration" on page 43.

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.

The following figure shows an example campus cluster storage configuration in a Microsoft cluster environment.

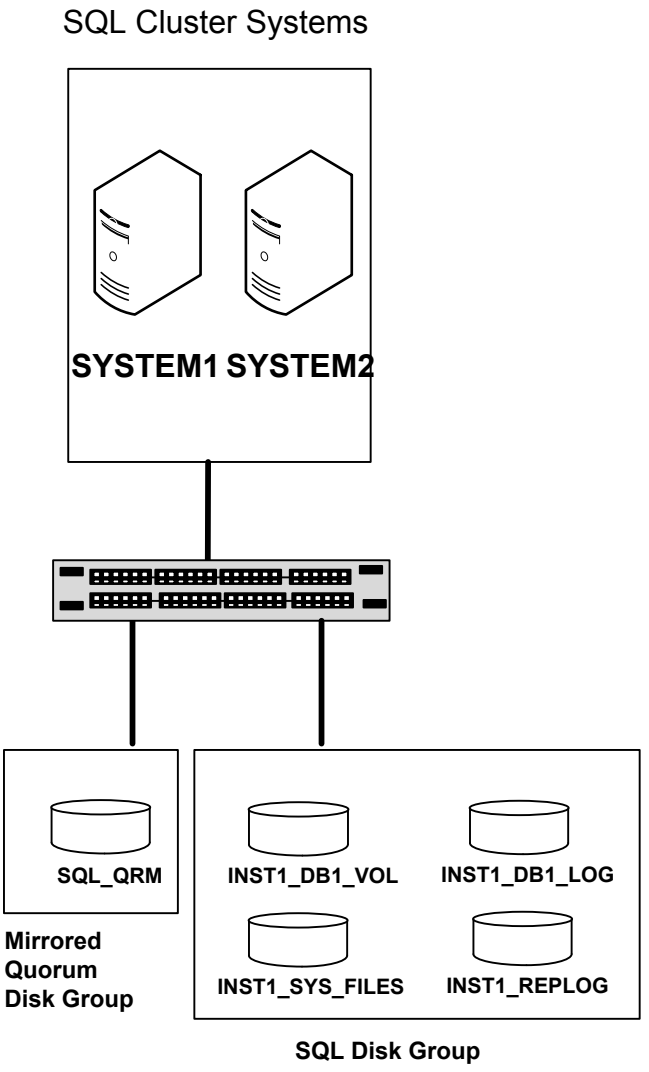
Figure 4-2 SFW disk groups and volumes in a Microsoft campus cluster



Sample SQL Server disaster recovery storage configuration

The following figure shows an example configuration of the disk groups and volumes for SQL Server on the primary site of a Microsoft cluster disaster recovery configuration.

Figure 4-3 SFW disk groups and volumes for SQL virtual server in a Microsoft disaster recovery configuration



Warning: When configuring the disk groups and volumes on the secondary site, be sure to use the same disk group and volume names as on the primary site.

SQL disk group INST1_DG contains at least the following volumes:

- INST1_DB1_VOL contains the SQL database. Each database typically resides on a separate volume.
- INST1_DB1_LOG contains the transaction log.
- INST1_SYS_FILES contains the volume for Microsoft SQL Server system data files.
- INST1_REPLOG contains the replicator log for Volume Replicator.

If FILESTREAM is implemented, the configuration should also contain a separate volume for the FILESTREAM filegroup.

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.

Veritas 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 *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.
- Veritas 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 (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.

To view the available disk storage

1. Launch VEA from **Start** > **All Programs** > **Veritas** > **Veritas 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, corresponding Volume Manager Disk Group (VMDg) resources are added to the cluster, under the available storage. The VMDg resource name corresponds to the cluster disk group name. You can then assign any of these resources to an application service group..

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** > **All Programs** > **Veritas** > **Veritas Storage Foundation** > **Veritas Enterprise Administrator** or, on Windows 2012 operating systems, from the **Apps** menu in the **Start** screen.

   Select a profile if prompted.

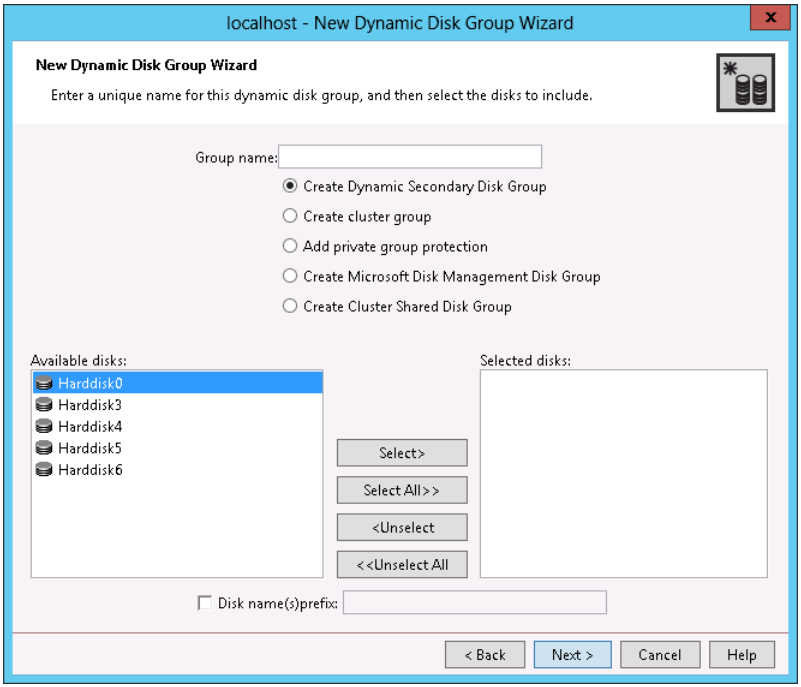
2. Click **Connect to a Host or Domain**.

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.



- In the Group name field, enter a name for the disk group (for example, INST1_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, Veritas recommends using 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 57.

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 48.

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** > **All Programs** > **Veritas** > **Veritas 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**.

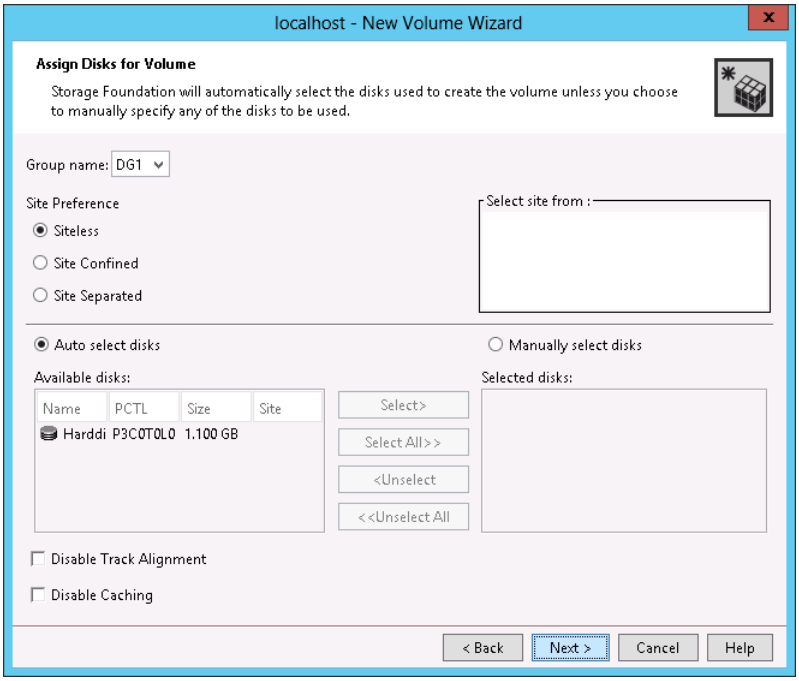
3. In the Connect dialog box select the host name from the pull-down menu and click **Connect**. To connect to the local system, select **localhost**. Provide the user name, password, and domain if prompted.

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 INST1_DG.

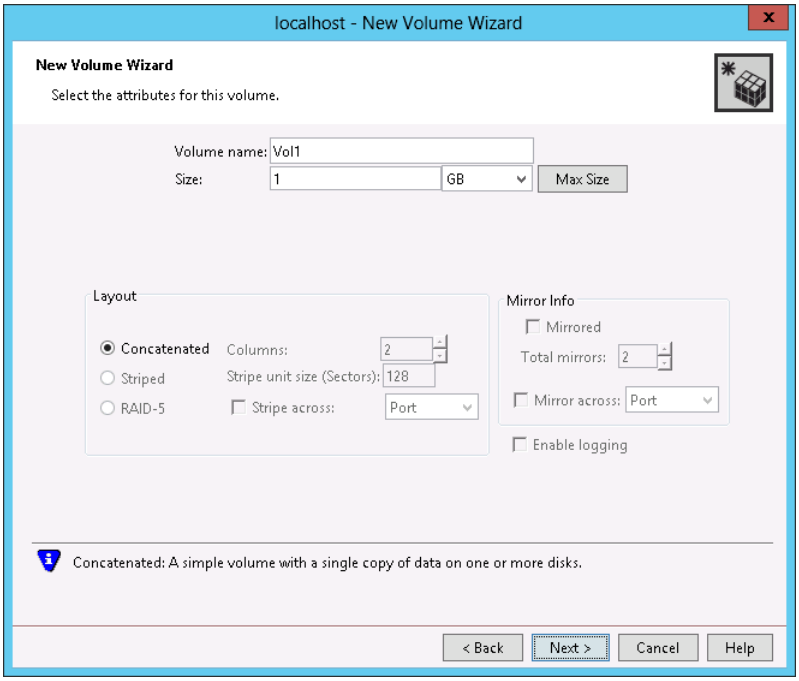
5. At the New Volume wizard opening screen, click **Next**.

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, INST1_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:



- 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.

     Note: If you plan to use this volume to install SQL Server, do not select the Enable file and folder compression checkbox. The SQL Server installation cannot copy files on a compressed or encrypted folder.

   - 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 52.

Before you begin, review the following topics:

See "Considerations when creating disk groups and volumes for a campus cluster" on page 47.

See "Adding disks to campus cluster sites" on page 52.

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** > **All Programs** > **Veritas** > **Veritas 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**.

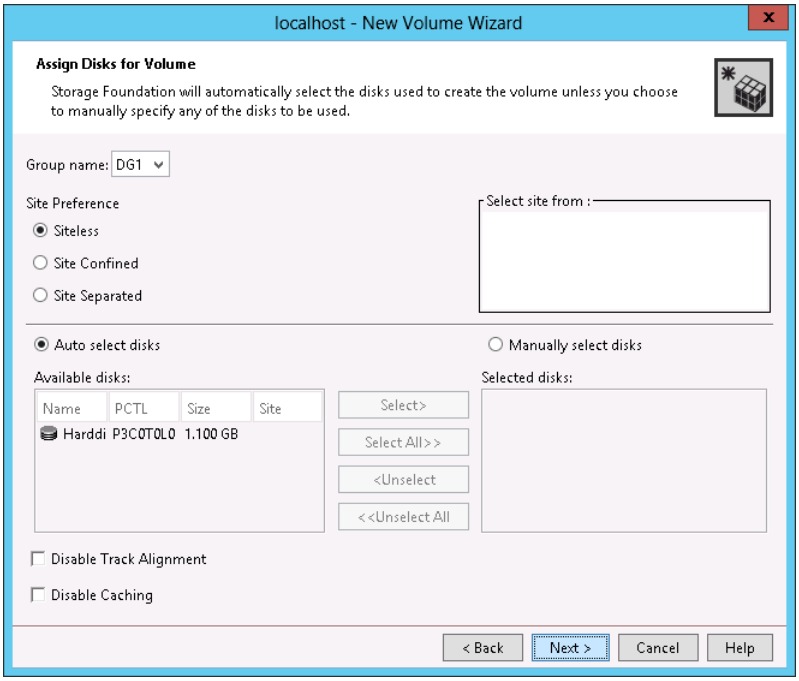
3. In the Connect dialog box select the host name from the pull-down menu and click **Connect**. To connect to the local system, select **localhost**. Provide the user name, password, and domain if prompted.

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 INST1_DG.

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

6. Select the disks for the volume as follows.

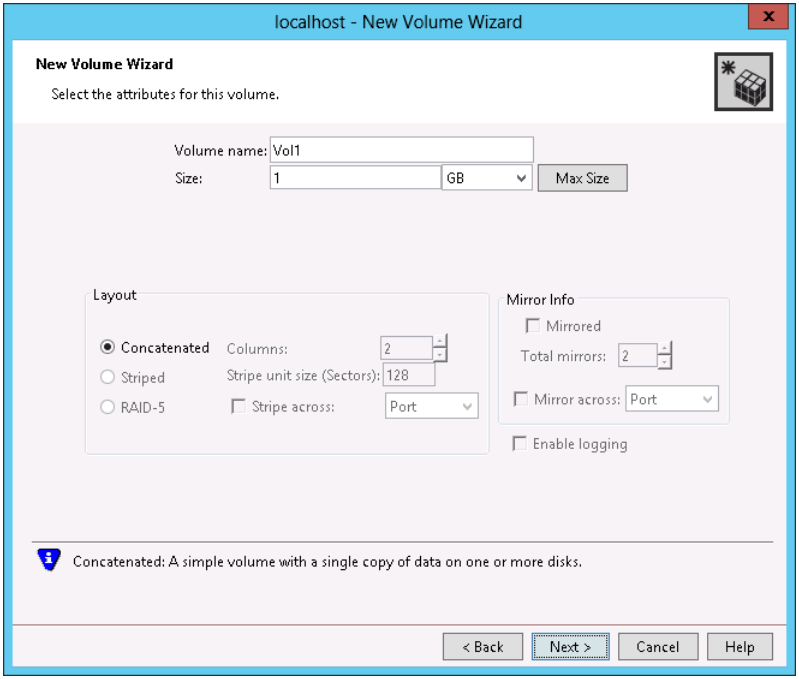


Group name	Make sure the appropriate disk group is selected.
Site preference	Select the **Site Separated** option.
Select site from	Select the campus cluster sites. Press **CTRL** to select multiple sites. **Note:** If no sites are listed, the disks have not yet been added to a site.
Auto select disks	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.



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.

Chapter 5

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.

The following table lists the tasks for implementing the mirrored quorum resource.

Table 5-1 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 64.

Table 5-1 Tasks for implementing the mirrored quorum resource *(continued)*

Action	Description
Verify that the Volume Manager Disk Group resource is added to the cluster	Verify that a resource for the disk group created is added to the Failover Cluster. Create a new quorum group and move the Volume Manager Disk Group resource that is created in step 1. See "Adding a Volume Manager Disk Group resource for the quorum" on page 65.
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 65.

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.

Veritas 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 49.

See "Creating dynamic volumes for high availability clusters" on page 52.

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. Move the clustered disk group resource from the **Available Storage** to **Quorum Group**.
7. Right-click the clustered disk group resource, and in the General tab of the Properties dialog box, change the name of the resource in the Resource Name field, for example, `QUORUM_DG_RES`.

Changing the quorum resource to a dynamic mirrored quorum resource

After a Volume Manager Disk Group resource is added 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 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.

Chapter 6

Installing SQL Server and configuring resources

This chapter includes the following topics:

- Tasks for installing and configuring SQL Server
- Creating the resource group for the SQL Server instance
- Prerequisites for installing SQL Server
- Installing SQL Server in an InfoScale Storage environment
- Dependency graph for SQL Server
- Verifying the SQL Server group in the Microsoft cluster

Tasks for installing and configuring SQL Server

The following table lists the process for deploying SQL Server with SFW in a Microsoft failover cluster.

Table 6-1 Tasks for installing and configuring SQL Server in a Microsoft failover cluster

Action	Description
Configure disk groups and volumes for SQL Server	■ If you have not yet done so, use the VEA console to configure disk groups and volumes for SQL Server See "Tasks for configuring InfoScale Storage" on page 40.

Table 6-1 Tasks for installing and configuring SQL Server in a Microsoft failover cluster *(continued)*

Action	Description
Create the SQL virtual server resource group	■ Create a SQL Server resource group in the cluster. ■ Add the VMDG disk group resource(s). See "Creating the resource group for the SQL Server instance" on page 68.
Install SQL Server	■ Review the prerequisites for installation See " Prerequisites for installing SQL Server" on page 69. ■ Mount the disk group and volumes created for the data files on the node where you install. ■ Install the software. Ensure that you install the data files to the path of the dynamic volume on shared storage. See "Installing SQL Server in an InfoScale Storage environment" on page 70.
Verify the resource dependencies.	See "Dependency graph for SQL Server" on page 71.
Verify the cluster configuration	Move the online SQL Server cluster group to the second node and back to the first node. See "Verifying the SQL Server group in the Microsoft cluster" on page 72.

Creating the resource group for the SQL Server instance

Before installing SQL Server you must:

- Create the SQL Server resource group .
- Add the resource for the SFW disk group that you created for SQL Server.

SQL virtual server installation requires a separate volume on which the system database files will be placed. Before installation, you create a Volume Manager Disk Group resource for the disk group that contains this volume. Creating this resource will enable SQL to monitor the system database files.

If you created additional SFW disk groups for SQL Server, for example, for user databases, you add Volume Manager Disk Group resources for those as well.

SQL Server installation adds the required SQL Server resources to the resource group and sets the appropriate dependencies for them.

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

To create the SQL Server resource group and add a disk group resource

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 you are connected to the required cluster.

2. In the left pane, right-click **Services and Applications** and select **More Actions > Create Empty Service or Application**. An empty group named New service or application is created. Right-click it and rename it, for example, SQL_GROUP.

3. In the left pane, right-click the group you created and select **Add a resource > More resources > Add Volume Manager Disk Group**.

4. In the center panel under Disk Drives, double-click **New Volume Manager Disk Group** to open its Properties dialog box.

5. On the General tab of the Properties dialog box, type a name for the resource.

   For example, type SQL_DG_RES.

6. On the Properties tab, in the **Disk Group Name** field, type the exact name of the disk group you previously created for the application (for example, INST1_DG), and click **OK** to close the dialog box.

7. Right-click the newly named resource and select **Bring this resource online**.

Prerequisites for installing SQL Server

Before you begin installing SQL Server, note the following prerequisites for installing in the SFW environment:

- Make sure that you have created the SFW disk groups and volumes for SQL Server.
  See "Tasks for configuring InfoScale Storage" on page 40.
- Make sure that you have created the SQL Server resource group and added the resource for the SQL Server disk group.
  See "Creating the resource group for the SQL Server instance" on page 68.
- Make sure that the SFW cluster disk group for SQL Server is imported to the first node and the volumes are mounted.

- Make sure that each node has a local drive letter in common with all the other nodes in the cluster to enable installation of the binaries in exactly the same path on each cluster node.
- If you are installing on a secondary site for a disaster recovery configuration, make sure that you take the SQL Network Name resource offline on the primary site before you begin installation on the secondary site. This will also offline the dependent resources. If the sites are on the same subnet and therefore use the same SQL IP address, ensure that the IP Address resource is offline on the primary site before beginning installation on the secondary site.
  See "Creating a parallel environment for SQL Server on the secondary site" on page 75.
- Ensure that the [NT AUTHORITY\SYSTEM] account is granted the sysadmin server role (from SQL Management Studio Console) on each node.

Installing SQL Server in an InfoScale Storage environment

Review the prerequisites for installation before you begin.

See " Prerequisites for installing SQL Server" on page 69.

During a Microsoft SQL Server installation, you install the first (active) node and additional nodes separately.

Refer to the Microsoft documentation for detailed installation information. As you progress through the installation, use the following guidelines to create an installation that will function properly in a Microsoft Failover Clustering environment with SFW:

- Ensure that the Volume Manager Disk Group resource is added to the Failover Cluster and the resource is online on the node where you plan to begin the SQL installation.
- Ensure that you set the installation path for the data files to the drive letter and location of the SFW volume created for the SQL Server system data files (for example, `INST1_SYS_FILES`). Allow the rest of the path (`Program Files\Microsoft SQL Server`) to remain. This must be the same path on all nodes.
  The installation program installs the system databases on the specified cluster (shared) disk. System databases must be on a clustered disk so that they can be shared between the nodes (and failed over when necessary), because these databases contain specific user login and database object information that must be the same for each node. The virtual server name will allow users access to the online node.

- If you are installing multiple instances, specify an instance name; only one default instance is allowed per cluster. Specify the same instance name when installing this instance on all cluster nodes.
- You must assign a unique virtual server name, for example, SQLVS, during installation. Specify the same virtual server name when installing this SQL instance on all cluster nodes.
  For a disaster recovery configuration, when installing on a secondary site, you must specify the same name for the SQL virtual server as that on the primary site.
- When configuring the virtual server, specify the IP address for the SQL virtual server.
- For the cluster group, specify the SQL Server resource group that you configured earlier.
  See "Creating the resource group for the SQL Server instance" on page 68.
- After installation, verify that SQL Server installed correctly according to Microsoft instructions. Check that the SQL virtual server group has the correct dependencies.

Note: If you select the checkbox to enable FILESTREAM for file I/O streaming access, the installation creates a resource SQL Server FILESTREAM share of type File Share. It is created with the appropriate dependencies set on the Volume Manager Disk Group, SQL Server, and SQL Server Network Name resource.

See "Dependency graph for SQL Server" on page 71.

- After the installation on the first node is complete, proceed to install SQL Server on the additional cluster nodes. To install SQL Server on additional nodes, launch the "Add node to a SQL Server failover cluster" wizard. The wizard identifies the existing cluster and accordingly proceeds with the installation.
- Using the same guidelines, install SQL Server on additional passive nodes. Make sure that you install the binaries on the same local drive on each node.

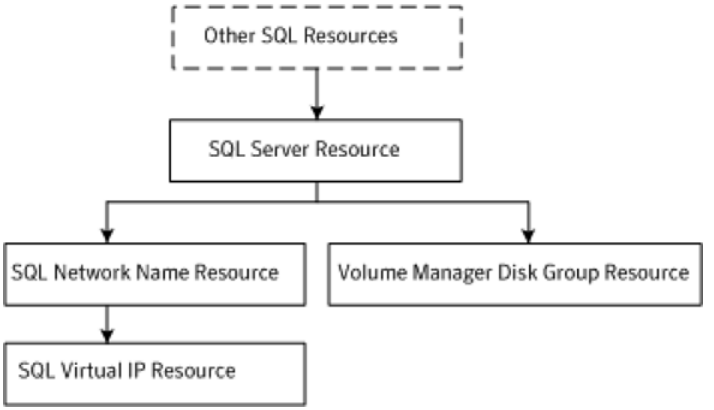
Dependency graph for SQL Server

Once Microsoft SQL Server is installed, the SQL Server Resource with dependencies on the SQL Network Name and the Volume Manager Disk Group resource is created.

Note: If you enabled the FILESTREAM file I/O streaming functionality during a SQL Server installation, a FILESTREAM resource is created with a dependency on the SQL Network Name resource, the SQL Server resource, and the Volume Manager Disk Group Resource.

The following figure indicates the dependencies that are established.

Figure 6-1 Dependency graph after the SQL installation is completed



Verifying the SQL 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.

Chapter 7

Configuring disaster recovery

This chapter includes the following topics:

- Tasks for configuring the secondary site for disaster recovery for SQL Server
- Verifying the primary site configuration
- Creating a parallel environment for SQL Server 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 SQL server resource dependency on the RVG resource
- Normal Volume Replicator operations and recovery procedures

Tasks for configuring the secondary site for disaster recovery for SQL Server

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

This disaster recovery solution requires Volume Replicator.

Refer to the *Volume Replicator Administrator's Guide* for additional details.

The following table describes the process for configuring the secondary site for disaster recovery.

Table 7-1 Process for configuring the secondary site for disaster recovery

Action	Description
Verify the primary site configuration.	See "Verifying the primary site configuration" on page 75.
Review the prerequisites and planning information	Verify the prerequisites on the secondary site. See "InfoScale requirements for Microsoft clustering solutions" on page 13. **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 24.
Create the parallel configuration on the secondary site	Ensure that you follow the secondary site requirements and guidelines for IP addresses, disk groups and volumes, the SQL Server resource group, and SQL Server installation. See "Creating a parallel environment for SQL Server on the secondary site" on page 75.
Understand the Volume Replicator components	See "Volume Replicator components overview" on page 76.
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 77.
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 79.
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 79.
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 91.

Table 7-1 Process for configuring the secondary site for disaster recovery *(continued)*

Action	Description
Set up the SQL Server resource dependencies	Change the SQL Server resource dependency properties so that it depends on the RVG resource instead of the Volume Manager Disk Group resource. See "Setting the SQL server resource dependency on the RVG resource" on page 92.

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 29.

Creating a parallel environment for SQL Server on the secondary site

After setting up an SFW environment with Microsoft clustering on the primary site, complete the same tasks on the secondary site before the SQL installation.

See "Workflow for a high availability (HA) configuration" on page 29.

However, note the following guidelines and exceptions:

- 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.
- During the creation of disk groups and volumes for the secondary site, make sure the following is exactly the same as the cluster on the primary site:
  - Cluster disk group name
  - Volume names and sizes
  - Drive letters
- Specify the same name for the SQL Server resource group as the name on the primary site.
- Before starting the SQL installation make sure you take the SQL Server Network Name resource offline on the primary site. This will also offline the dependent

SQL resources. In addition, if the secondary is in the same subnet, take the IP Address resource offline on the primary site.

- During installation, specify the same name for the SQL virtual server as the name on the primary site.

Do not begin Volume Replicator configuration until you have completed all the steps for setting up the parallel configuration on the secondary site, including the following:

- Disk groups and volumes configured
- SQL Server installed on all the nodes

Volume Replicator components overview

The following table describes the Volume Replicator components you must configure.

Table 7-2 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. Veritas 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 Volume Replicator Security Service (VxSAS) on all cluster nodes on both the primary and secondary sites.

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 *Volume Replicator Administrator's Guide*.

To configure the VxSAS service

1. Launch the wizard from **Start** > **All Programs** > **Veritas** > **Veritas 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 `vxsascfg.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 Volume Replicator 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 80.

See “Creating a Replicated Data Set (RDS)” on page 80.

Prerequisites for setting up the RDS

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

- Verify that the disk groups and volumes for the SQL user database files and log files have been created. You can create the Replicator Log volume while you run the wizard if not created earlier.
- Verify that VxSAS has been configured.
- Verify that the SQL virtual server Network Name resource is offline on the secondary site. This would also bring all the dependent SQL resources offline. If on the same subnet, ensure that the SQL IP address resource is also offline.
- Verify that the intended Primary host is connected to VEA, if you configure the RDS from a remote client or from a host that is not the Primary.
- Verify whether the IP version preference is set before you configure replication. If you specify host names when you configure replication, Volume Replicator resolves the host names with the IP addresses associated with them. This setting determines which IP version Volume Replicator uses to resolve the host names.

  Use one of the following methods to set the IP preference:

  - Veritas Enterprise Administrator (VEA) GUI—select the appropriate options on the Control Panel > VVR Configuration > IP Settings tab.
  - Run the `vxtune ip_mode [ipv4 | ipv6]` command at the primary site as well as the secondary site.
- Verify that the data volumes and Replicator Log volume that 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 (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 under replication
    For the Replicator Log volume, in addition to these 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** > **All Programs** > **Veritas** > **Veritas 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 about 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 INST1_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 INST1_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**. For example, select INST1_REPLOG.
  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 about 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 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 **Create Dynamic Disk Group** to proceed with creating the disk group. A disk group with the same name as that on the Primary is created.

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 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 about 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 about the Primary host and displays the volume name and the size.
  Complete the information on this panel as follows:

Name	Displays the name that is specified for the Primary volume.
Size	Displays the size that is 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. 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 Volume Replicator updates in the Replicator Log. From there, Volume Replicator 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 or ReFS 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 that is provided in the list, use the command line interface.

Bandwidth	By default, Volume Replicator uses the maximum available bandwidth. To control the bandwidth thatVolume Replicator uses for replication, choose **Specify Limit**, and then specify the bandwidth limit in the field provided. The default unit is Megabits 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 the 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 uses. If required, you can disable intelligent synchronization. **Note:** Intelligent synchronization is applicable only to volumes with the NTFS and ReFS file systems and not to raw volumes or volumes with FAT 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 SQL 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 SQL Server virtual server 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.

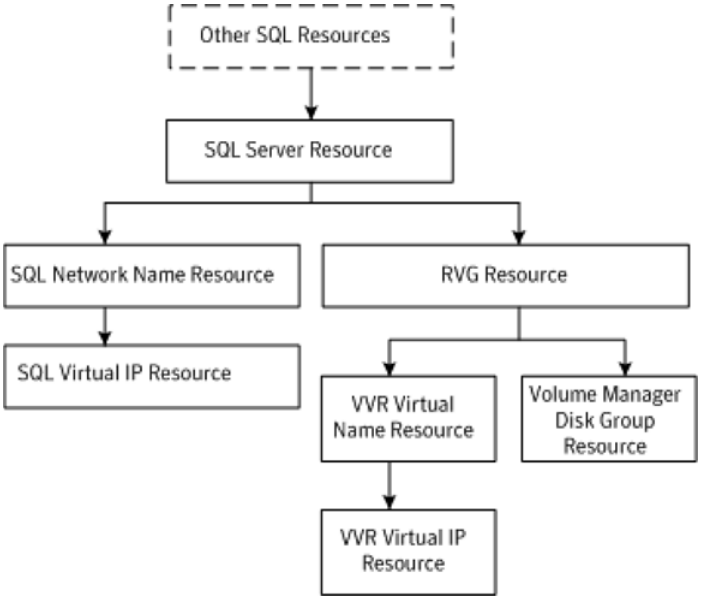
Setting the SQL server resource dependency on the RVG resource

The SQL Server resource was earlier 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.

The following figure indicates the dependencies required.

Figure 7-1 Dependency graph for SQL Server



To change the SQL Server resource dependency properties

1. Ensure that the SQL Server resource is offline.
2. Right-click the SQL Server resource and select **Properties**.
3. On the Properties dialog box, select the Dependencies tab.
4. Make the appropriate selections on the Dependencies tab to:
   - Add the Replicated Volume Group resource to the dependencies.
   - Delete the Volume Manager Disk Group resource from the dependencies.
5. The cluster configuration is now complete. Online the entire SQL_GROUP group on the primary cluster.

Normal Volume Replicator operations and recovery procedures

The following topics describe the normal Volume Replicator operations and recovery.

- See "Monitoring the status of the replication" on page 93.
- See "Performing planned migration" on page 93.
- See "Replication recovery procedures" on page 94.

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 *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 SQL 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 a SQL 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 SQL 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-failback** option to restore the original Primary easily once it becomes available again. When performing Takeover with fast-failback, make sure that you do not select the **Synchronize Automatically** option.
- Perform the **Takeover without fast-failback** 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 SQL 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-failback option, do one of the following:

- For Takeover with the Fast-failback 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-failback 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 SQL group online on the original Primary.
8. Attach the databases on the original Primary. See the Microsoft documentation for instructions.

Appendix A

Configure InfoScale Storage in an existing Microsoft Failover Cluster

This appendix includes the following topics:

- Configuring InfoScale Storage in an existing Microsoft Failover Cluster

Configuring InfoScale Storage in an existing Microsoft Failover Cluster

After you have configured an application for high availability, in a Microsoft Failover Cluster, you may want to move the application data from the existing disks to the InfoScale Storage -controlled storage disks. This task involves installing InfoScale Storage on all the cluster systems, converting the already configured basic disks to dynamic disks, and then adding the dynamic disk group resource to the application role.

Notes:

- You are required to reboot the systems to successfully install InfoScale Storage. Also, you need take the application role offline before you begin to convert the basic disks to dynamic disks. These procedures result in application down-time.
- For the steps performed using the Failover Cluster Manager, refer to the Microsoft documentation for details. For the steps performed using VEA, refer to the SFW administrator's guide for the details about Disk and Volume tasks.

To configure InfoScale Storage in an existing Microsoft Failover Cluster, perform the following steps:

1. Install InfoScale Storage on all the cluster systems. You must select the Microsoft Failover Cluster option during the installation.

   Note: At the end of the installation process you are required to reboot the system. To ensure less down-time, you can first install InfoScale Storage on the cluster systems other than the one where the application role is online. After you complete the installation on all these systems initiate the installation on the system where the application role is online.

   ---

2. After the cluster systems have restarted, using the Failover Cluster Manager, stop the application role to bring the resources offline.
3. Check the resource dependencies to note the storage resource dependencies.
4. Remove the existing basic disk storage resource from the application role.
5. Remove the basic disk from the available storage.

   This step removes the basic disk resource from the application role and takes the disk offline.
6. Using VEA, bring the basic disk online.
7. Create a new clustered dynamic disk group using the basic disk that is brought online in step 6. Before you create a dynamic disk group, ensure that minimum 16MB free space is available in the disk. This space is required to upgrade a basic disk to a dynamic disk.
8. Using Failover Cluster Manager, move the clustered disk group resource that is created in step 7. You must move this resource from the **Available Storage** to the Application Role.
9. Set the resource dependencies as noted in step 3.

   All the earlier storage resource dependencies must now be replaced with the Volume Manager Disk Group resource.
10. Bring the application role online.