Veritas™ Cluster Server Implementation Guide for Microsoft SQL

Windows Server 2003

5.1
Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

VCS is a licensed product. See the *Veritas Cluster Server Install and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit http://www.symantec.com/business/support/index.jsp and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.
## Chapter 1  Introducing the VCS agents for SQL and NetApp

- About the VCS agents for SQL and NetApp .......................................................... 12
- About VCS hardware replication agent for NetApp ............................................ 13
  - NetApp Filer agent .................................................................................. 13
  - NetApp SnapDrive agent ........................................................................... 14
  - NetApp SnapMirror agent ........................................................................... 15
- About the VCS database agent for Microsoft SQL Server ..................................... 16
- About the SQL Server 2000 agents ..................................................................... 17
  - Agent for SQL Server 2000 ......................................................................... 17
  - Agent for MSSearch service ....................................................................... 17
- About the SQL Server 2005 agents ..................................................................... 18
  - Agent for SQL Server 2005 ......................................................................... 18
  - Agent for SQL Server 2005 agent service ................................................. 18
  - Agent for SQL Server 2005 analysis service ............................................ 19
- About the agent for MSDTC service .................................................................. 19
- About SQL Server services ................................................................................. 20
  - MSSearch service ......................................................................................... 20
  - Microsoft Data Transaction Coordinator (MSDTC) service ..................... 20
- Monitoring options .............................................................................................. 21
- How the agents make SQL Server highly available ........................................... 21
  - Local cluster configuration ........................................................................ 21
  - Disaster recovery configuration ................................................................... 22
- Running SQL Server in an active-active clustered environment ....................... 22
- Typical SQL Server 2000 configuration in a VCS cluster .................................. 23
- Typical SQL Server 2005 configuration in a VCS cluster .................................. 25
- Typical disaster recovery configuration ............................................................. 27

## Chapter 2  Installing the VCS database agent for SQL

- About installing the VCS agent for SQL ............................................................. 30
- Before installing the agent ................................................................................ 30
- Installing the agent ........................................................................................... 30
- Configuring the cluster ....................................................................................... 31
  - Configuring Web console .............................................................................. 43
  - Configuring notification ............................................................................... 44
  - Configuring Wide-Area Connector process for global clusters ................. 47
Chapter 3 Installing and configuring SQL Server

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About installing and configuring SQL</td>
<td>50</td>
</tr>
<tr>
<td>Before installing SQL</td>
<td>50</td>
</tr>
<tr>
<td>Privileges requirements</td>
<td>51</td>
</tr>
<tr>
<td>Configuring Microsoft iSCSI Initiator</td>
<td>51</td>
</tr>
<tr>
<td>Managing storage using Network Appliance filer</td>
<td>52</td>
</tr>
<tr>
<td>Connecting virtual disks to the cluster node</td>
<td>53</td>
</tr>
<tr>
<td>Disconnecting virtual disks from the cluster nodes</td>
<td>54</td>
</tr>
<tr>
<td>Configuring Microsoft iSCSI Initiator</td>
<td>51</td>
</tr>
<tr>
<td>About LDM support</td>
<td>55</td>
</tr>
<tr>
<td>Reserving disks (if you use Windows LDM)</td>
<td>56</td>
</tr>
<tr>
<td>Creating volumes (if you use Windows LDM)</td>
<td>56</td>
</tr>
<tr>
<td>Mounting volumes (if you use Windows LDM)</td>
<td>56</td>
</tr>
<tr>
<td>Unassigning a drive letter</td>
<td>57</td>
</tr>
<tr>
<td>Releasing disks (if you use Windows LDM)</td>
<td>57</td>
</tr>
<tr>
<td>Installing SQL Server 2000 on the first node</td>
<td>58</td>
</tr>
<tr>
<td>Preparing to install SQL Server 2000 on the second node</td>
<td>60</td>
</tr>
<tr>
<td>Stopping the SQL Server 2000 Service</td>
<td>61</td>
</tr>
<tr>
<td>Disconnecting virtual disks from the first node</td>
<td>61</td>
</tr>
<tr>
<td>Releasing disks from the first node (if you use Windows LDM)</td>
<td>61</td>
</tr>
<tr>
<td>Connecting virtual disks to the second node</td>
<td>61</td>
</tr>
<tr>
<td>Mounting volumes on the second node (if you use Windows LDM)</td>
<td>61</td>
</tr>
<tr>
<td>Renaming shared SQL Server 2000 files</td>
<td>62</td>
</tr>
<tr>
<td>Installing SQL Server 2000 on the second node</td>
<td>62</td>
</tr>
<tr>
<td>Installing SQL Server 2000 on the second node</td>
<td>62</td>
</tr>
<tr>
<td>Setting the internal name of the clustered instance</td>
<td>63</td>
</tr>
<tr>
<td>Installing SQL Server 2005 on the first node</td>
<td>66</td>
</tr>
<tr>
<td>Preparing to install SQL Server 2005 on the second node</td>
<td>69</td>
</tr>
<tr>
<td>Stopping the SQL Server 2005 service</td>
<td>69</td>
</tr>
<tr>
<td>Disconnecting virtual disks from the first node</td>
<td>69</td>
</tr>
<tr>
<td>Releasing disks from the first node (if you use Windows LDM)</td>
<td>69</td>
</tr>
<tr>
<td>Connecting virtual disks to the second node</td>
<td>69</td>
</tr>
<tr>
<td>Mounting volumes on the second node (if you use Windows LDM)</td>
<td>69</td>
</tr>
<tr>
<td>Renaming shared SQL Server 2005 files</td>
<td>70</td>
</tr>
<tr>
<td>Installing SQL Server 2005 on the second node</td>
<td>70</td>
</tr>
<tr>
<td>Removing shared SQL Server 2005 files</td>
<td>70</td>
</tr>
<tr>
<td>Setting the internal name of the clustered instance</td>
<td>71</td>
</tr>
<tr>
<td>Assigning ports for multiple SQL Server instances</td>
<td>74</td>
</tr>
</tbody>
</table>
Chapter 4 Configuring the SQL service group

About configuring the SQL service group ..........................................................76
Before configuring the SQL service group .......................................................76
Configuring a SQL Server service group .......................................................77
Running SnapManager for SQL .....................................................................82
Creating a SQL Server user-defined database .................................................82
Creating new volumes or LUNs .....................................................................83
Creating a new SQL Server database ..........................................................83
Adding storage agent resources to the SQL service group .............................84
Verifying the service group configuration ......................................................86
Bringing the service group online ..................................................................86
Taking the service group offline ....................................................................86
Switching the service group ..........................................................................87
Administering a SQL Server service group .....................................................88
Modifying a SQL service group configuration ...............................................88
Deleting a SQL service group ........................................................................89

Chapter 5 Configuring an MSDTC service group for high availability

About configuring the MSDTC service group ..................................................92
Before configuring the MSDTC service group ................................................92
Reviewing the configuration ..........................................................................93
Creating an MSDTC service group ..................................................................95
Creating an MSDTC client .............................................................................97
Verifying the installation ..............................................................................98

Chapter 6 Making a standalone SQL server highly available

About making a standalone SQL server highly available ................................100
Reviewing the configuration ..........................................................................101
Sample configuration ....................................................................................102
Configuring the storage hardware and network ..........................................103
Preparing the standalone SQL Server ............................................................104
Backing up existing SQL data ........................................................................104
Setting SQL Server services to manual start ..............................................105
Installing and configuring VCS on the standalone SQL server ....................106
Installing and configuring SQL Server on additional nodes .......................106
Moving the existing SQL Server data files and user databases ....................107
Configuring the VCS SQL Server service group ..........................................107
Creating a SQL Server user-defined database ..............................................108
Verifying the installation ..............................................................................108
Chapter 7  Active-Active configuration

About active-active configuration ......................................................... 110
Reviewing the configuration .............................................................. 110
   Sample configuration .................................................................. 111
   Configuring the storage hardware and network ......................... 113
Installing VCS and configuring the cluster ................................... 114
Configuring volumes or virtual disks for SQL Server ................. 114
Installing and configuring the first instance of SQL Server .......... 115
Configuring the VCS service group for the first SQL Server instance ...... 116
Creating a SQL Server user-defined database ............................... 116
Repeating SQL Server installation for additional instances ............ 116
Verifying the configuration ............................................................. 117

Chapter 8  Disaster recovery configuration

About disaster recovery configuration .............................................. 120
What is a disaster recovery solution? ............................................. 120
   Why implement a disaster recovery solution? ......................... 120
   Understanding replication ....................................................... 121
What needs to be protected in a SQL Server environment? ............ 121
Typical disaster recovery configuration ......................................... 122
Disaster recovery: New SQL Server 2000 installation .................. 123
   Reviewing the configuration .................................................... 123
   Installing VCS and configure the cluster ................................. 125
   Configuring volumes or LUNs on the shared storage .................. 125
   Installing and configuring SQL Server 2000 at the primary site ...... 125
   Configuring the VCS SQL service group .................................. 125
Creating a parallel environment on the secondary site ............... 126
Configuring DR components on the primary and secondary sites .... 127
Disaster recovery: New SQL Server 2005 installation .................. 128
   Reviewing the configuration .................................................... 128
   Installing VCS and configuring the cluster ................................. 129
   Configuring volumes or LUNs on the shared storage .................. 130
   Installing and configuring SQL Server 2005 at the primary site ...... 130
   Configuring the VCS SQL service group .................................. 131
Creating a parallel environment on the secondary site ............... 132
Installing DR components on the primary and secondary sites .... 132
Configuring DR components ......................................................... 133
Configuring replication using Network Appliance SnapMirror ........ 133
Configuring SnapMirror resources at the primary site .................. 134
Configuring the Global Cluster Option for wide-area failover ........ 135
   Prerequisites ........................................................................... 135
   Linking clusters: Adding a remote cluster to a local cluster ....... 136
Appendix B Sample configurations

About sample configurations .............................................................. 190
Sample configuration for a SQL Server 2000 cluster .............................. 190
Sample configuration for a SQL Server 2005 cluster .............................. 194

Index 199
Introducing the VCS agents for SQL and NetApp

This chapter contains the following topics:

- “About the VCS agents for SQL and NetApp” on page 12
- “About VCS hardware replication agent for NetApp” on page 13
- “About the VCS database agent for Microsoft SQL Server” on page 16
- “About the SQL Server 2000 agents” on page 17
- “About the SQL Server 2005 agents” on page 18
- “About the agent for MSDTC service” on page 19
- “About SQL Server services” on page 20
- “Monitoring options” on page 21
- “How the agents make SQL Server highly available” on page 21
- “Running SQL Server in an active-active clustered environment” on page 22
- “Typical SQL Server 2000 configuration in a VCS cluster” on page 23
- “Typical SQL Server 2005 configuration in a VCS cluster” on page 25
- “Typical disaster recovery configuration” on page 27
About the VCS agents for SQL and NetApp

The VCS database agent for Microsoft SQL Server provides high availability to SQL Server. The VCS hardware replication agent for Network Appliance SnapMirror enables configuring Network Appliance filers over an iSCSI or Fibre Channel (FC) connection in a VCS cluster environment. Both the agents work together to provide high availability and disaster recovery to SQL Server in environments that use Network Appliance filers for shared storage. The agents also support disaster recovery configurations set up using the VCS Global Cluster Option and Network Appliance SnapMirror for data replication.

In a typical configuration, the agents are installed on each node in the cluster. The nodes are connected to the NetApp filers through a dedicated (private) storage network. VCS nodes are physically attached to the Network Appliance filer via an ethernet cable supporting iSCSI or FC as the transport protocol.

![Figure 1-1 Typical VCS configuration in a NetApp storage environment](image)

This chapter provides an overview of the agents. For more information about the agents, including their VCS resource type definitions and attribute definitions, see “Resource type definitions” on page 167.
About VCS hardware replication agent for NetApp

The VCS hardware replication agent for Network Appliance provides failover support and recovery in environments employing Network Appliance filers for storage and SnapMirror for replication. The agent monitors and manages the state of replicated filer devices and ensures that at a time only one system has safe and exclusive access to the configured devices.

The agent can be used in local clusters, single VCS replicated data clusters, and multi-cluster environments set up using the VCS Global Cluster Option. The package contains three agents; each agent is described in subsequent sections:

- **NetAppFiler agent**—Monitors the state of the filer.
- **NetAppSnapDrive agent**—Connects and disconnects virtual disks (LUNs) using the iSCSI or FC protocol.
- **NetAppSnapMirror agent**—Determines the role of the filer volumes with respect to replication and promotes a read-only snapmirrored volume to a read-write source volume during a wide-area failover.

**NetApp Filer agent**

The NetApp Filer agent monitors the state of the filer device. The agent is represented by the NetAppFiler resource type in VCS. NetAppFiler resources are persistent, meaning that they are not brought online or taken offline.

**Agent operation**

- **Monitor**—Verifies the state of the filer attached to the host by sending an ICMP ping command to the filer. If the filer does not respond, the agent reports the state of the filer as faulted.
NetApp SnapDrive agent

The NetApp SnapDrive agent monitors, connects, and disconnects filer volumes. The agent can be configured to use the iSCSI or the FC protocol.

Agent operations

- **Online**—Connects a virtual disk (LUN) using an iSCSI or an FC Initiator. The agent presents the LUN as a locally-attached drive to the host. The agent also removes LUN-host mappings made before the online operation.
- **Offline**— Disconnects the virtual disk (LUN) from the host.
- **Monitor**—Verifies that the specified virtual disk (LUN) is connected to the host.
- **Open**—Verifies that there is connectivity to the filer. It also checks that the VCS Helper service is running with the same privileges as the SnapDrive service.
- **Clean**—Attempts to forcibly disconnect a virtual disk (LUN).
NetApp SnapMirror agent

The NetApp SnapMirror agent monitors the replication state of filer devices. When a failover occurs, the agent reverses the direction of replication.

Agent operations

- **Online**—If the state of the local filer device is **SOURCE**, the agent creates a lock file to indicate that the resource can come online. This effectively makes the devices writable for the application.
  
  If the state of the local filer is **SNAPMIRRORED**, the agent attempts to reverse the direction of replication by changing the state of the local filer to **SOURCE** and that of the original source to **SNAPMIRRORED**.
  
  If the original source filer is down, the agent performs a mirror breakoff to enable local write access, if the filer is not already broken off.
  
  If the original source returns to life, you must re-synchronize the data manually. The Online entry point touches a lock file if Read Write access is enabled successfully.

- **Offline**—Removes the lock file. The agent does not perform any filer operations because an offline entry point does not necessarily indicate an intention to give up the devices.

- **Monitor**—Verifies the lock file exists. If the lock file exists, the monitor entry point reports the status of the resource as online. If the lock file does not exist, the monitor entry point reports the status of the resource as offline.

- **Open**—Removes the lock file, thereby preventing potential concurrency violation if the group fails over to another node.

  **Note:** The agent does not remove the lock file if the agent was started after an hastop -force command.

- **Clean**—Removes the lock file. No filer operations are performed since offlineing this resource is no indication of a pending role swap.
About the VCS database agent for Microsoft SQL Server

The VCS database agent for Microsoft SQL Server provides high availability for Microsoft SQL Server 2000 and Microsoft SQL Server 2005 in a VCS cluster. The agent monitors Microsoft SQL Server RDBMS and its services on a VCS cluster to ensure high availability. The database agent also provides “active-active” support for SQL Server. VCS provides separate agents for SQL Server 2000 and SQL Server 2005.

Agents for SQL Server 2000

- Agent for SQL Server 2000 service. The agent provides high availability for SQL Server 2000 service.
- Agent for MSSSearch service. The agent provides high availability for full-text search indices with a clustered SQL instance.

Agents for SQL Server 2005

- Agent for SQL Server 2005 Analysis service. The agent provides high availability for SQL Server 2005 Analysis service.

The VCS database agent for Microsoft SQL Server also includes an MSDTC agent, which provides high availability for MSDTC service used in distributed transactions. The agent provides high availability for MSDTC service for SQL Server 2000 and SQL Server 2005.
About the SQL Server 2000 agents

The agents for SQL Server 2000 monitor specific resources within an enterprise application, determine the status of these resources, brings them online, and takes them offline.

Agent for SQL Server 2000

The agent brings the SQL Server 2000 service online, monitors the status, and takes it offline. The agent provides high availability for SQL Server 2000 in a clustered environment. The SQL Server 2000 agent monitors the SQL Server service and the SQL agent service. Specific agent operations include:

- **Online**—Brings the SQL Server 2000 service online.
- **Offline**—Takes the SQL Server 2000 service offline.
- **Monitor**—Queries the Service Control Manager (SCM) for the status of SQL Server 2000 services. See “Monitoring options” on page 21 for more information.
- **Clean**—Forcibly stops the SQL Server service.

Agent for MSSearch service

The agent brings the full-text search for a particular SQL instance online, monitors the status, and takes it offline. The agent provides high availability for full-text search index in a clustered environment. Specific agent operations include:

- **Online**—Brings the full-text search service for a particular instance online.
- **Offline**—Takes the full-text search service for a particular instance offline.
- **Monitor**—Monitors the full-text search service for a particular instance.
- **Clean**—Forcibly stops the MSSearch service for a particular instance.

**Note:** The MSSearch agent requires the SQL Server agent to be configured. Hence, you must configure MSSearch agent only on those cluster nodes that have SQL Server agent configured.
About the SQL Server 2005 agents

The agents for SQL Server 2005 monitor specific resources within an enterprise application, determines the status of these resources, brings them online, and takes them offline.

Agent for SQL Server 2005

The agent brings the SQL Server 2005 service online, monitors the status, and takes it offline. The agent provides high availability for SQL Server 2005 in a clustered environment. The SQL Server 2005 agent monitors the SQL Server service. Specific agent operations include:

- Online—Brings the SQL Server 2005 service online.
- Offline—Takes the SQL Server 2005 service offline.
- Monitor—Queries the Service Control Manager (SCM) for the status of SQL Server 2005 services.
  See “Monitoring options” on page 21 for more information.
- Clean—Forcibly stops the SQL Server service.

Agent for SQL Server 2005 agent service

The agent brings the SQL Server 2005 agent service online, monitors the status, and takes it offline. The agent provides high availability for SQL Server 2005 agent in a clustered environment. Specific agent operations include:

- Online—Brings the SQL Server 2005 agent service online.
- Offline—Takes the SQL Server 2005 agent service offline.
- Monitor—Monitors the SQL Server 2005 agent service.
- Clean—Forcibly stops the SQL Server 2005 agent service.
Agent for SQL Server 2005 analysis service

The agent brings SQL Server 2005 analysis service online, monitors the status, and takes it offline. The agent provides high availability for SQL Server 2005 analysis service in a clustered environment. Specific agent operations include:

- **Online**—Brings the SQL Server 2005 agent service online.
- **Offline**—Takes the SQL Server 2005 agent service offline.
- **Monitor**—Monitors the SQL Server 2005 agent service.
- **Clean**—Forcibly stops the SQL Server 2005 agent service.

**Note:** The VCS database agent for Microsoft SQL Server does not provide an agent for monitoring SQL Server 2005 MSSearch service. Instead, the SQL Server 2005 MSSearch service is monitored using a GenericService resource. Refer to *Veritas Cluster Server Bundled Agents Reference Guide* for more information about GenericService agent.

About the agent for MSDTC service

The MSDTC agent comprises two parts; MSDTC client and MSDTC server. The MSDTC client and the MSDTC server must not be configured on the same cluster node.

The MSDTC agent brings the MSDTC service online, monitors its status, and takes it offline. The agent provides high availability for an MSDTC service in a clustered environment. Specific agent operations include:

- **Online**—Brings the MSDTC service online.
- **Offline**—Takes the MSDTC service offline.
- **Monitor**—Monitors the MSDTC service.
- **Clean**—Forcibly stops the MSDTC service.
About SQL Server services

The VCS database agent for Microsoft SQL Server provides high availability for following services, MSSearch and MSDTC.

MSSearch service

SQL Server 2000 provides a full-text search index using the Microsoft Search (MSSearch) service. MSSearch is an indexing service that creates and manages full-text indices on specified columns within a database table. Full-text search creates an index entry for each word in the textual data for a specified column. Because each word in the textual data is indexed, queries looking for particular words become extremely fast.

Microsoft Data Transaction Coordinator (MSDTC) service

Microsoft Data Transaction Coordinator or the MSDTC service enables you to perform distributed transactions. A distributed transaction updates data on more than one computer in a network. The MSDTC service ensures that a transaction is successfully committed on each computer. A failure to commit on a single system aborts the transaction on all systems in the network.

If a transaction spans across more than one computer in the network, you must ensure that the MSDTC service is running on all the computers. Also, all the computers must be able to communicate with each other.
Monitoring options

The VCS database agent for Microsoft SQL Server provides two levels of application monitoring: basic and detail. Basic monitoring queries the SCM to verify whether the SQL Server services are continuously active. Detail monitoring updates a temporary table in the SQL Server database to verify the availability of the database instance.

If you start the SQL server services from outside VCS, then the SQL resource will go in an UNKNOWN state, because the VCS database agent for Microsoft SQL monitors the computer context of the services. If the SQL service is not started in the virtual server context the resource goes in an UNKNOWN state. You must ensure that you start all the SQL related services from within VCS.

Note: Detail monitoring can be configured only for the SQL Server 2000 and SQL Server 2005 agents.

How the agents make SQL Server highly available

The VCS database agent for Microsoft SQL Server detects an application failure if a configured virtual server becomes unavailable. The NetApp agents ensure consistent data access to the node on which SQL Server instances are running. This section describes how the agents migrate SQL Server to another node in local clusters and in global disaster recovery configurations.

Local cluster configuration

When the VCS database agent for Microsoft SQL Server detects an application failure, the SQL Server service group is failed over to the next available system in the service group's system list. The configured SQL services and virtual server are started on the new system. The NetApp agents connect the virtual disks (LUNs) that contain the SQL Server data to the new node; thus ensuring continuous availability to SQL data.
Disaster recovery configuration

In a disaster recovery configuration, VCS first attempts to fail over the application to a node in the local cluster. If all nodes in the local cluster are unavailable, or if a disaster strikes the site, VCS attempts to fail over the application to the remote site. This involves the following steps:

- Connecting the virtual disks (LUNs) to the target hosts (using the NetAppSnapDrive agent)
- Performing a mirror break, which enables write access to the target (using the NetAppSnapMirror agent)
- Reversing the direction of replication by demoting the original source to a target, and begin replicating from the new source (using the NetAppSnapMirror agent)
- Starting the SQL services on the remote node (using the VCS database agent for SQL Server)

Running SQL Server in an active-active clustered environment

SQL Server allows up to 16 independent instances of SQL Server to run on a single machine. Using this feature, the VCS database agent for Microsoft SQL Server supports SQL Server in an active-active environment by allowing a node to run up to 16 instances. A SQL Server instance can fail over to any of the other configured nodes on its system list.

You can choose an active-active SQL Server configuration where several instances are intended to run on a single node. However, remember that you must configure failover nodes such that a single node can never host more than 16 instances.
Typical SQL Server 2000 configuration in a VCS cluster

A typical SQL Server 2000 configuration in a VCS cluster involves two cluster nodes accessing a shared storage. The SQL Server binaries are installed on the cluster nodes. The shared storage is used to store SQL Server data files and the MSDTC log files. The cluster nodes access the shared storage. The shared storage can be managed using Network Appliance suite of products.

The cluster nodes are configured to host the SQL Server 2000 and SQL Server 2000 MSSearch resource. The MSDTC resource can be configured on the same cluster nodes. You need not configure an MSDTC client if the MSDTC resource is configured on the same nodes that have SQL Server 2000 resource configured. However, if the MSDTC resource is configured on other nodes, you must configure an MSDTC client to point to the virtual server name of the MSDTC resource.
The following illustration depicts a two node cluster hosting a SQL Server service group with MSSearch service configured. MSDTC resource is also configured on the same nodes.

**Figure 1-2**  Typical SQL 2000 configuration in a VCS cluster
Typical SQL Server 2005 configuration in a VCS cluster

A typical SQL Server 2005 configuration in a VCS cluster involves two cluster nodes accessing a shared storage. The SQL Server binaries are installed on the cluster nodes. The shared storage is used to store SQL Server data files and the MSDTC log files. The cluster nodes access the shared storage. The shared storage can be managed using Network Appliance suite of products.

The cluster nodes are configured to host the SQL Server 2005 resource, the SQL Server 2005 agent service resource, the SQL Server 2005 MSSearch service resource, and the SQL Server 2005 analysis service resource. The MSDTC resource can be configured on the same cluster nodes. You need not configure an MSDTC client if the MSDTC resource is configured on the same nodes that have SQL Server 2005 resource configured. However, if the MSDTC resource is configured on other nodes, you must configure an MSDTC client to point to the virtual server name of the MSDTC resource.
The following illustration depicts a two node cluster hosting a SQL Server service group with the different services configured. MSDTC resource is also configured on the same nodes.

**Figure 1-3  Typical SQL Server 2005 configuration in a VCS cluster**
Typical disaster recovery configuration

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

Figure 1-4  Typical DR configuration in a VCS cluster

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

Filer1 in the cluster on the primary site replicates to Filer2 in the cluster on the secondary site. Replication between the filers is set up using NetApp SnapMirror for SQL. Refer to NetApp documentation for more information on replication using NetApp filers.

If the Microsoft SQL Server server on System1 fails, SQL Server comes online on node System2 and begins servicing requests. From the user’s perspective there might be a small delay as the backup node comes online, but the interruption in effective service is minimal.

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

Typical disaster recovery configuration
Installing the VCS database agent for SQL

This chapter contains the following topics:

■ “About installing the VCS agent for SQL” on page 30
■ “Before installing the agent” on page 30
■ “Installing the agent” on page 30
■ “Configuring the cluster” on page 31
About installing the VCS agent for SQL

This chapter describes how to install the VCS database agent for SQL and then configure the cluster. Follow these instructions if you did not install the agent while installing VCS.

Before installing the agent

- Verify that you have VCS installed on all cluster nodes. Refer to the *Veritas Cluster Server Installation and Upgrade Guide* for instructions.
- Verify that you have Local Administrator privileges on the node where you are installing the agent.

Installing the agent

Complete these steps to install the VCS database agent for SQL on a system. Repeat these steps on all systems on which you wish to configure SQL with VCS.

To install the agent

1. Start the installer for VCS. In the Add/Remove Programs window, click **VCS for Windows** and click **Change**.
2. In the VCS for Windows dialog box, choose the **Add or Remove** option and click **Next**.
3. In the VCS product options dialog box, click **Next**.
4. Check the **Veritas Cluster Server Database Agent for SQL** check box and click **Next**.
   The disk space required for the installation is displayed toward the bottom of the screen. When you add or remove an option, the total space changes.
5. The installer validates the system for prerequisites. After the system is accepted, click **Next**.
   If a system is rejected, the Comments column displays the cause for rejecting the system. Highlight the system to view a detailed information about the failure in the Details box. Resolve the error, highlight the system from the list, and click **Validate Again**.
6. Review the summary of your selections and click **Update** to start the installation. The installer displays the status of installation.
7. After the installation is complete, review the installation report and click **Next**.
8 Click **Finish**.
After the agent is successfully installed, proceed to configuring the cluster.

**Configuring the cluster**

After installing the VCS database agent for SQL using the product installer, set up the components required to run a cluster. The VCS Cluster Configuration Wizard (VCW) sets up the cluster infrastructure, including LLT and GAB, and configures Symantec Product Authentication Service in the cluster. The wizard also configures the ClusterService group, which contains resources for the Cluster Management Console (Single Cluster Mode), also referred to as the Web Console, notification, and global clusters.

- If you plan to set up a disaster recovery environment, configure the wide-area connector process for global clusters.
- If you plan to create a new user account for the VCS Helper service, you must have Domain Administrator privileges or belong to the Domain Account Operators group.
- When configuring a user account for the VCS Helper service, make sure that the user account is a domain user. The VCS HAD, which runs in the context of the local system built-in account, uses the VCS Helper service user context to access the network. This account does not require domain admin privileges.
- Make sure the VCS Helper service domain user account has “Add workstations to domain” privilege enabled in the Active Directory.
- In case of NetApp, the user account for the VCS Helper service must have administrative privileges on the NetApp filer.

**To configure a VCS cluster**

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

2. Read the information on the Welcome panel and click **Next**.

3. On the Configuration Options panel, click **Cluster Operations** and click **Next**.
4 On the Domain Selection panel, select or type the name of the domain in which the cluster resides and select the discovery options.

To discover information about all systems and users in the domain:

- Clear the **Specify systems and users manually** check box.
- Click **Next**.
  
  Proceed to step 8 on page 34.

To specify systems and user names manually (recommended for large domains):

- Check the **Specify systems and users manually** check box.
- Additionally, you may instruct the wizard to retrieve a list of systems and users in the domain by selecting appropriate check boxes.
- Click **Next**.
  
  If you chose to retrieve the list of systems, proceed to step 6 on page 33. Otherwise, proceed to the next step.
5. On the System Selection panel, type the name of each system to be added, click **Add**, and then click **Next**. Do not specify systems that are part of another cluster.

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

Proceed to step 8 on page 34.
Enter the name of the system and click **Add** to add the system to the **Selected Systems** list, or click to select the system in the Domain Systems list and then click the > (right-arrow) button.

7. The System Report panel displays the validation status, whether **Accepted** or **Rejected**, of all the systems you specified earlier.
   
   A system can be rejected for any of the following reasons:
   - System is not pingable.
   - WMI access is disabled on the system.
   - Wizard is unable to retrieve the system architecture or operating system.
   - VCS is either not installed on the system or the version of VCS is different from what is installed on the system on which you are running the wizard.

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

   Click **Next** to proceed.

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

9. On the Cluster Details panel, specify the details for the cluster and then click **Next**.
The wizard validates the selected systems for cluster membership. After the systems are validated, click **Next**.

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

If you chose to configure a private link heartbeat in step 9 on page 34, proceed to the next step. Otherwise, proceed to step 12 on page 38.

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

Do one of the following:
To configure the VCS private network over Ethernet

- Select the check boxes next to the two NICs to be assigned to the private network.
  Symantec recommends reserving two NICs exclusively for the private network. However, you could lower the priority of one NIC and use the low-priority NIC for public and private communication.

- If you have only two NICs on a selected system, it is recommended that you lower the priority of at least one NIC that will be used for private as well as public network communication. To lower the priority of a NIC, right-click the NIC and select **Low Priority** from the pop-up menu.

- If your configuration contains teamed NICs, the wizard groups them as "NIC Group #N" where "N" is a number assigned to the teamed NIC. A teamed NIC is a logical NIC, formed by grouping several physical NICs together. All NICs in a team have an identical MAC address. Symantec recommends that you do not select teamed NICs for the private network.

The wizard will configure the LLT service (over Ethernet) on the selected network adapters.
To configure the VCS private network over the User Datagram Protocol (UDP) layer:

- Check the **Configure LLT over UDP** check box.
- Specify a unique UDP port in the **Port number for Link1** and **Port number for Link2** fields. You can use ports in the range 49152 to 65535. The default ports numbers are 50000 and 50001 respectively.
- Select the check boxes next to the two NICs to be assigned to the private network. Symantec recommends reserving two NICs exclusively for the VCS private network.
- For each selected NIC, verify the displayed IP address. If a selected NIC has multiple IP addresses assigned, double-click the field and choose the desired IP address from the drop-down list. Each IP address can be in a different subnet. The IP address is used for the VCS private communication over the specified UDP port.
- For each selected NIC, double-click the respective field in the Link column and choose a link from the drop-down list. Specify a different link (Link1 or Link2) for each NIC. Each link is associated with a UDP port that you specified earlier.

The wizard will configure the LLT service (over UDP) on the selected network adapters. The specified UDP ports will be used for the private network communication.
12 On the VCS Helper Service User Account panel, specify the name of a domain user for the VCS Helper service. The VCS HAD, which runs in the context of the local system built-in account, uses the VCS Helper service user context to access the network. This account does not require domain admin privileges.

To specify an existing user, do one of the following:
- Click Existing user and select a user name from the drop-down list,
- If you chose not to retrieve the list of users in step 4 on page 32, type the user name in the Specify User field, and then click Next.
- To specify a new user, click New user and type a valid user name in the Create New User field, and then click Next.

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

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

Do one of the following:
To use the single sign-on feature

Click **Use Single Sign-on**. In this mode, VCS uses SSL encryption and platform-based authentication. The VCS engine (HAD) and Veritas Command Server run in secure mode.

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

If you know the name of the system that will serve as the root broker, click **Specify root broker system**, type the system name, and then click **Next**.

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

If you specify a system outside of the cluster, make sure that the system is configured as a root broker; the wizard configures all nodes in the cluster as authentication brokers.

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

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

Table 2-1 contains some more examples of search criteria.

<table>
<thead>
<tr>
<th>1st drop-down list value</th>
<th>2nd drop-down list value</th>
<th>Adjacent field entry</th>
<th>Search result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>*system</td>
<td>*system</td>
<td>Displays all systems with names that end with <em>system</em>.</td>
</tr>
<tr>
<td>Name</td>
<td><em>vcsnode</em></td>
<td></td>
<td>Displays all systems with names that contain <em>vcsnode</em>.</td>
</tr>
<tr>
<td>Operating System</td>
<td><em>2003</em></td>
<td></td>
<td>Displays all Windows Server 2003 systems.</td>
</tr>
<tr>
<td>Operating System Version</td>
<td>5.*</td>
<td></td>
<td>Displays all systems whose operating system version is 5.x, where x could be 0, 1, 2, etc.</td>
</tr>
</tbody>
</table>

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

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

If the root broker is a cluster node, the wizard configures the other cluster nodes as authentication brokers. If the root broker is outside the cluster, the wizard configures all the cluster nodes as authentication brokers.
To use VCS user privilege:

- Click **Use VCS User Privileges**.
  
The default user name for the VCS administrator is *admin* and the default password is *password*. Both are case-sensitive. You can accept the default user name and password for the VCS administrator account or type a new name and password. It is recommended that you specify a new user name and password. Use this account to log on to VCS using Cluster Management Console (Single Cluster Mode) or Web Console, when VCS is not running in secure mode.

- Click **Next**.

14 Review the summary information on the Summary panel, and click **Configure**. The wizard configures the VCS private network.

If the selected systems have LLT or GAB configuration files, the wizard displays an informational dialog box before overwriting the files. In the dialog box, click **OK** to overwrite the files. Otherwise, click **Cancel**, exit the wizard, move the existing files to a different location, and rerun the wizard. The wizard starts running commands to configure VCS services. If an operation fails, click **View configuration log file** to see the log.

15 On the Completing Cluster Configuration panel, click **Next** to configure the ClusterService service group; this group is required to set up components for the Cluster Management Console (Single Cluster Mode) or Web Console, notification, and for global clusters.
To configure the ClusterService group later, click **Finish**.

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

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

You are not required to configure the Cluster Management Console (Single Cluster Mode) or Web Console, for this HA environment. Refer to the *Veritas Cluster Server Administrator’s Guide* for complete details on VCS Cluster Management Console (Single Cluster Mode), and the Notification resource.

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

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

- Check the **Web Console** checkbox to configure the Cluster Management Console (Single Cluster Mode), also referred to as the Web Console. See “Configuring Web console” on page 43.
Check the **Notifier Option** checkbox to configure notification of important events to designated recipients. See “Configuring notification” on page 44.

**Configuring Web console**

This section describes steps to configure the VCS Cluster Management Console (Single Cluster Mode), also referred to as the Web Console.

**To configure the Web console**

1. On the Web Console Network Selection panel, specify the network information for the Web Console resources and click **Next**.

   ![Web Console Network Selection Panel]

   - If the cluster has a ClusterService service group configured, you can use the IP address configured in the service group or configure a new IP address for the Web console.
   - If you choose to configure a new IP address, type the IP address and associated subnet mask.
   - Select a network adapter for each node in the cluster. Note that the wizard lists the public network adapters along with the adapters that were assigned a low priority.

2. Review the summary information and choose whether you want to bring the Web Console resources online when VCS is started, and click **Configure**.

3. If you chose to configure a Notifier resource, proceed to: “Configuring notification” on page 44. Otherwise, click **Finish** to exit the wizard.
Configuring notification

This section describes steps to configure notification.

To configure notification

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

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

2. If you chose to configure SNMP, specify information about the SNMP console and click Next.
- Click a field in the SNMP Console column and type the name or IP address of the console. The specified SNMP console must be MIB 2.0 compliant.
- Click the corresponding field in the Severity column and select a severity level for the console.
- Click ‘+’ to add a field; click ‘-’ to remove a field.
- Enter an SNMP trap port. The default value is “162”.

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

- Type the name of the SMTP server.
- Click a field in the Recipients column and enter a recipient for notification. Enter recipients as admin@example.com.
- Click the corresponding field in the Severity column and select a severity level for the recipient. VCS sends messages of an equal or higher severity to the recipient.
- Click ‘+’ to add fields; click ‘-’ to remove a field.
4. On the Notifier Network Card Selection panel, specify the network information and click **Next**.

![Notifier Network Card Selection panel](image)

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

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

6. Click **Configure**.

7. Click **Finish** to exit the wizard.
Configuring Wide-Area Connector process for global clusters

Configure the wide-area connector process only if you are configuring a disaster recovery environment.

To configure the wide-area connector process for global clusters

1. On the GCO Network Selection panel, specify the network information and click **Next**.

   - If the cluster has a ClusterService service group configured, you can use the IP address configured in the service group or configure a new IP address.
   - If you choose to configure a new IP address, enter the IP address and associated subnet mask. Make sure that the specified IP address has a DNS entry.
   - Select a network adapter for each node in the cluster. The wizard lists the public network adapters along with the adapters that were assigned a low priority.

2. Review the summary information and choose whether you want to bring the resources online when VCS starts and click **Configure**.

3. Click **Finish** to exit the wizard.
Installing the VCS database agent for SQL
Configuring the cluster
Installing and configuring SQL Server

This chapter contains the following topics:

- “About installing and configuring SQL” on page 50
- “Before installing SQL” on page 50
- “Managing storage using Network Appliance filer” on page 52
- “Managing storage using Windows Logical Disk Manager” on page 55
- “Installing SQL Server 2000 on the first node” on page 58
- “Preparing to install SQL Server 2000 on the second node” on page 60
- “Installing SQL Server 2000 on the second node” on page 62
- “Installing SQL Server 2005 on the first node” on page 66
- “Preparing to install SQL Server 2005 on the second node” on page 69
- “Installing SQL Server 2005 on the second node” on page 70
- “Assigning ports for multiple SQL Server instances” on page 74
About installing and configuring SQL

This chapter provides information for installing and configuring SQL Server. This environment uses an active-passive configuration with one to one failover capabilities.

To configure MSDTC service groups, see “Configuring an MSDTC service group for high availability” on page 91.

If you already have an existing SQL Server deployment, and you wish to make it highly available using VCS, see “Making a standalone SQL Server highly available” on page 99.

If you are planning to deploy an active-active configuration with multiple SQL instances, see “Active-Active configuration” on page 109.

Before installing SQL

- Verify that VCS is installed on all the nodes in the cluster.
- Verify that you have configured a VCS cluster using VCS Cluster Configuration Wizard (VCW).
  See “Configuring the cluster” on page 31.
- Verify that all nodes have adequate resources to run SQL Server 2000 or SQL Server 2005, and VCS.
- If using iSCSI, verify that the Microsoft iSCSI Initiator is configured to establish a persistent connection between the Network Appliance filer and the cluster nodes. See the Microsoft documentation for instructions.
- Make sure that you have an external, basic disk to create volumes or LUNs (virtual disk).
  Symantec recommends that you create volumes for the following:
  - SQL Server data
  - Registry replication
  - User defined database
  - User defined database logs
  See “Managing storage using Network Appliance filer” on page 52.
  See “Managing storage using Windows Logical Disk Manager” on page 55.
- If your cluster has an Exchange service group configured, make sure to install SQL Server on a node that is not in the SystemList attribute for the Exchange service group.
Privileges requirements

- You must be a domain user. The domain user must have administrator privileges.
- You must be a member of the Local Administrators group on all nodes on which Microsoft SQL will be installed.
- You must have write permissions for the Active Directory objects corresponding to these nodes.
- You must have write permissions on the DNS server to perform DNS updates.

Configuring Microsoft iSCSI Initiator

The Microsoft iSCSI initiator enables communication between Windows systems and Network Appliance Filers. The initiator uses the iSCSI protocol to present the filer volume as a local block device to the system.

**To configure Microsoft iSCSI initiator**

1. Make sure the Microsoft iSCSI Initiator software version 2.0 is installed on all cluster nodes. Refer to Microsoft documentation for further information.
2. Start the Microsoft iSCSI initiator. Double-click the Microsoft iSCSI Initiator icon from the desktop.
3. Click the **Target Portals** tab, if not already selected.
4. Click **Add**.
5. In the Add Target Portals dialog box, specify the IP address or the DNS name for the Network Appliance Filer and click **OK**.
6. Click the **Available Targets** tab and click **Log On**.
7. In the Log On to Target dialog box, verify the target portal name and select the **Automatically restore this connection when the system reboots** check box.
8. Click **OK**.
9. Click the **Persistent Target** tab to verify that the newly added target portal is listed under the **Select a target** box.
10. Click **OK**.
Managing storage using Network Appliance filer

Network Appliance manages data by creating volumes on physical disks. These volumes can further be divided into Logical Unit Numbers (LUNs). The LUNs are accessible from the cluster nodes, provided the nodes have Microsoft iSCSI Initiator and Network Appliance SnapDrive installed. If you plan to use Fibre Channel (FC) for connecting the LUNs, ensure that you install the FCP Attach Kit or Windows Host Utilities on all the cluster nodes. Refer to the NetApp documentation for more information.

**Note:** Symantec does not support volumes created using qtree.

**Figure 3-1** VCS cluster in a NetApp storage environment

The VCS database agent for Microsoft SQL requires two LUNs to be created on the Network Appliance filer, one for SQL Server data and the other for the registry replication information.

If you will be configuring an MSDTC service group, create additional volumes for MSDTC log, and MSDTC registry replication. These LUNs must be accessible from all cluster nodes.

For example, you could create the following volumes to manage your SQL Server database and logs:

- **INST1_DATA_FILES**: contains the SQL Server system data files (including the master, model, msdb, and tempdb databases)
■ INST1_REGREP_VOL: contains the list of registry keys that must be replicated among cluster systems for the SQL Service. Create a 100 MB (minimum recommended size) volume for this purpose.

■ INST1_DB1_VOL: contains the user database files

■ INST1_DB1_LOG: contains the user database log files

Perform the following tasks to create LUNs on the NetApp Filer and to make them accessible from cluster nodes:

■ Create volumes on the NetApp Filer.

■ Share the volumes.

■ Create LUNs on the shared volumes.

Refer to Network Appliance documentation for instructions on performing these tasks.

Connecting virtual disks to the cluster node

Once the virtual disks are created on the Network Appliance filer, they must be connected (if not connected already) to the cluster nodes using Network Appliance SnapDrive.

To connect virtual disks to the cluster node

1. Start the Computer Management MMC on the cluster node where you want to connect the LUN. Click Start > All Programs > Administrative Tools > Computer Management.

2. From the left pane, expand Storage and double-click SnapDrive.

3. Right-click Disks and then click Connect Disk... to launch the Connect Disk wizard.

4. Click Next on the Welcome page.

5. Specify the path of the virtual disk that you wish to connect to the cluster node and then click Next.

6. Select Dedicated as the Virtual Disk Type and then click Next.

7. Click Assign a Drive Letter and then choose a drive letter from the drop-down list.

8. On the Select Initiator panel, specify the initiator(s) for the virtual disk and then click Next.

9. On the igroup Management Type panel, choose the option that allows SnapDrive to perform igroup management automatically and then click Next.
10 Click **Finish** to begin connecting the specified virtual disk to the cluster node.

### Disconnecting virtual disks from the cluster nodes

**To disconnect virtual disks**

1. Start the Computer Management MMC on the cluster node where you want to disconnect the LUN. Click **Start > All Programs > Administrative Tools > Computer Management.**
2. From the left pane, expand **Storage** and double-click **SnapDrive.**
3. Double-click **Disks** to see the LUNs that are connected to the node.
4. Right-click the LUN you want to disconnect and then click **Disconnect Disk...**
5. In the Disconnect Disk alert box, click **OK.**
Managing storage using Windows Logical Disk Manager

If your configuration uses shared disks and volumes managed using Windows Logical Disk Manager (LDM), use the VCS DiskReservation (DiskRes) and Mount agents. Before configuring shared storage, review the resource types and attribute definitions of the Disk Reservation and Mount agents described in the Veritas Cluster Server Bundled Agents Reference Guide.

Symantec recommends that you create two volumes on the shared disk, one for SQL Server data and the other for the registry replication information.

If you will be configuring an MSDTC service group, create additional volumes for MSDTC log, and MSDTC registry replication. These LUNs must be accessible from all cluster nodes.

For example, you could create the following volumes to manage your SQL Server database and logs:

- INST1_DATA_FILES: contains the SQL Server system data files (including the master, model, msdb, and tempdb databases)
- INST1_REGREP_VOL: contains the list of registry keys that must be replicated among cluster systems for the SQL Service. Create a 100 MB (minimum recommended size) volume for this purpose.
- INST1_DB1_VOL: contains the user database files
- INST1_DB1_LOG: contains the user database log files

Perform the following tasks to create volumes and make them accessible from server farm nodes:

- Reserve disks. See “Reserving disks (if you use Windows LDM)” on page 56.
- Create volumes. See “Creating volumes (if you use Windows LDM)” on page 56.
- Mount volumes. See “Mounting volumes (if you use Windows LDM)” on page 56.

About LDM support

The following restrictions apply in this release:

- Disk Reservation and Mount agents are supported on VCS for Windows only. These agents are not supported in an SFW storage environment.
- LDM support is available on Windows Server 2003 only.
For using LDM, your storage devices must be configured to use SCSI-2 disk reservations. SCSI-3 is not supported.

LDM support is not applicable for Disaster Recovery configurations. Currently only HA configurations are supported.

Reserving disks (if you use Windows LDM)

Complete the following steps to reserve the disks on the node on which you are going to install SQL.

To reserve the disks

1. To display all the disks, type the following on the command line:
   
   C:\>havol -scsitest /l

   You will see a table that lists all the disks that are visible from the current system. Make a note of the disk numbers (Disk# column in the table). You will need it in the next step.

2. To reserve a disk, type the following on the command line:
   
   C:\>havol -scsitest /RES:<disk #>

   For example, to reserve disk #4, type:
   
   C:\>havol -scsitest /RES:4

   Make a note of the disk number and the corresponding signature. You will require these details to identify and reserve the disks while installing SQL, and configuring the SQL service group, on additional nodes in the cluster.

Creating volumes (if you use Windows LDM)

Use the Windows Disk Management tool to verify that the disks are visible on the cluster nodes, and then create volumes on the reserved disks. After creating the required volumes on a node, rescan the disks on all the remaining nodes in the cluster.

Refer to Microsoft Windows documentation for more information about the Disk Management tool.

Mounting volumes (if you use Windows LDM)

Use the Windows Disk Management tool to mount the volumes that you created earlier. After mounting the volumes on a cluster node, run the CHKDSK command and verify that there are no errors on the mounted volumes.

Make a note of the drive letters that you assign to the mounted volumes. Use the same drive letters while mounting these volumes on the remaining cluster nodes.
Refer to Microsoft Windows documentation for more information about the CHKDSK command and the Disk Management tool.

**Unassigning a drive letter**

While installing an application on multiple nodes, you must first unassign drive letters and release the disks from one node, and then reserve the disks, mount the volumes using the same drive letters and then install the application on the failover node.

Complete these steps to unassign the drive letters from a node.

**To unassign drive letter**

1. Log in as Administrator.
2. Open Disk Management.
   
   ```bash
   C:\> diskmgmt.msc
   ```
3. Right-click the partition or logical drive and click *Change Drive Letter and Path*.
4. In the *Change Drive Letter and Paths* dialog box, click the drive letter and click *Remove*.

**Note:** You must run Disk Management on all systems each time you add a shared disk. This ensures each disk has a valid signature written to it, and that the device paths and symbolic links are updated.

**Releasing disks (if you use Windows LDM)**

To release a disk, type the following on the command line:

```bash
C:\> havol -scsitest /REL:<disk #>
```

For example, to release disk #4, type:

```
C:\> havol -scsitest /REL:4
```

Make a note of the disk number and the corresponding signature. You will require these details to identify and reserve the disks later.
Installing SQL Server 2000 on the first node

Before installing Microsoft SQL Server 2000 on the first cluster node, verify that the volumes or LUNs (virtual disks) on the filer are mounted or connected to the first cluster node.

Install Microsoft SQL Server 2000 on the first node using the SQL installation wizard.

Install the SQL program files to a local disk and the SQL data files to the shared storage managed by the cluster disk group. As you progress through the installation, use the following guidelines to create an installation that will function properly in your environment.

Note: Only the portions of the SQL Server installation procedure relevant to the SFW environment are documented. Refer to the Microsoft SQL Server 2000 documentation for detailed installation information. Also refer to the Microsoft SQL Server 2000 documentation on the use of /PAE and /AWE switches if you are installing multiple instances of SQL and anticipate intensive memory use.

To install Microsoft SQL Server 2000

1. From the browser menu, select **SQL Server 2000 Components > Install Database Server**. Proceed with the installation steps.

2. If you are running Windows Server 2003, click **Continue** at the message that says SQL Server 2000 SP2 and below is not supported by this version of Windows. You will install SQL Server 2000 SP4 after installing SQL Server.

3. On the Welcome screen, click **Next**.

4. In the Computer Name panel, select **Local Computer** and click **Next**.

5. Proceed through the installation to the Installation Definition panel.

6. In the Installation Definition panel, choose the **Server and Client Tools** option and click **Next**.

7. In the Instance Name panel, enter an instance name (for example INST1), and click **Next**.

   Use the same instance name when installing this instance of SQL Server 2000 on failover nodes. If you are installing multiple instances of SQL in the cluster, each must have its own unique instance name.
8 In the Setup Type panel, select the type of installation and click **Browse** to specify the destination folder for SQL Server program and data files.

![Setup Type Panel]

9 In the Choose Folder dialog box, make the following selections and click **Next**:

- For **Program Files**, select a volume on the local disk.
- For **Data Files**, select the volume created for the SQL Server system data files (INST1_DATA_FILES). You can allow the rest of the path (`\Program Files\Microsoft SQL Server`) to remain. You must set the same path on all nodes.
10 In the Service Accounts panel, make the following selections and click Next:

- Choose the Customize the settings for each service option.
- In the Services box, select the SQL Server option.
- In the Service Settings box, select Use a Domain User account and then specify the user name, password, and domain.
- Clear the Auto Start Service option.
- Repeat these steps for the SQL Server Agent option.

11 Follow the wizard instructions to complete the installation.

12 When you have completed the initial installation of SQL Server 2000, install SQL Server 2000 SP4.

Warning: Multiple instances of SQL Server 2000 must be installed in the same order on every node in the cluster.

Preparing to install SQL Server 2000 on the second node

Follow the procedures provided in this section before installing SQL Server on additional nodes. These procedures must be performed for every node that is intended to be a part of the cluster.
Stopping the SQL Server 2000 Service

Stop the SQL server service on the configured node so the databases on the shared disk can be manipulated by the installation on the second node.

To stop the SQL Server service

1. Click **Start > All Programs > Microsoft SQL Server > Service Manager** to open the SQL Server Service Manager.

   ![SQL Server Service Manager](image)

2. Select the server to stop from the **Server** list.

3. Click **Stop**.

4. Click **Yes** in the SQL Service Manager dialog box to confirm that you do want to stop the service.

Disconnecting virtual disks from the first node

See “Disconnecting virtual disks from the cluster nodes” on page 54.

Releasing disks from the first node (if you use Windows LDM)

See “Unassigning a drive letter” on page 57.
See “Releasing disks (if you use Windows LDM)” on page 57.

Connecting virtual disks to the second node

See “Connecting virtual disks to the cluster node” on page 53.

Mounting volumes on the second node (if you use Windows LDM)

See “Mounting volumes (if you use Windows LDM)” on page 56.
Renaming shared SQL Server 2000 files

Before installing SQL on the second node, open the SQL Server system data files volume (INST1DATA_FILES) and rename or remove the first node SQL Server system data files. The files will be replaced during the installation of SQL Server on the additional nodes.

If you rename the folder that contains the system data files, the files are available as backup files in case problems occur during the second node SQL Server installation. Once the installation completes successfully, you can then delete the renamed folder and its contents.

To rename shared SQL Server data files
1. On the computer on which the cluster disk group is imported, open the volume that holds the SQL Server data files.
2. Rename the folder that contains the SQL Server data files.

Installing SQL Server 2000 on the second node

Follow the procedures provided in this section to install and configure SQL Server on additional nodes.

Installing SQL Server

Before installing Microsoft SQL Server 2000 on the second node, verify that the volumes or LUNs (virtual disks) are mounted or connected to the second cluster node. Install Microsoft SQL Server 2000 on additional nodes using the SQL installation wizard.

See “Installing SQL Server 2000 on the first node” on page 58 for the installation steps.

Removing shared SQL Server 2000 files

If you renamed the shared SQL Server folder from the SQL Server system data files volume prior to installing SQL on the second node, you can delete the renamed folder and files now.

To delete the renamed SQL Server data files
1. On the computer on which the cluster disk group is imported, open the volume that holds the renamed SQL Server data files.
2. Select the renamed SQL Server data folder and files contained in the volume, and press Delete.
Setting the internal name of the clustered instance

Use the Query Analyzer to set the internal name of the clustered instance to be the virtual server name.

**Note:** Do this procedure after you install and configure SQL Server on the last node for this instance, so that you need to do the procedure only once. Do it from the last node, assuming that it is still connected to the shared volumes.

The virtual server name you assign must be unique within the cluster. The virtual server name is used by the SQL Server clients to access the database. You specify the virtual server name again when configuring the VCS SQL service group for this instance.

**Warning:** For a disaster recovery configuration, the virtual server name on the secondary site cluster must match the one on the primary site cluster.

To set the internal name of the clustered instance

1. Click **Start > All Programs > Microsoft SQL Server > Query Analyzer** to start the SQL Query Analyzer.
2. In the **Connect to SQL Server** window, provide connection information:

   - In **SQL Server**, enter the SQL Server machine name in the format `System_Name\Instance_Name`. For example `SYSTEM2\INST1`.
   - Select the **Start SQL server if it is stopped** checkbox.
   - Enter valid user credentials and click **OK**.
Installing and configuring SQL Server

Installing SQL Server 2000 on the second node

3  Find the SQL Server name:

   ■ In the upper pane of the query analyzer, enter the text "sp_helpserver"
   ■ Press F5.
   ■ Make note of the name listed in the lower pane, for example SYSTEM2\INST1. For a named instance, the name will be System_Name\Instance_Name. For a default instance, the name will be System_Name.

4  Delete the contents in the upper pane.

5  Disconnect the database:

   ■ In the upper pane, enter the following:
     "sp_dropserver 'System_Name\Instance_Name.'"
     where System_Name\Instance_Name is the name noted in step 3. For example, for named instance:
     "sp_dropserver 'SYSTEM2\INST1.'"
     For example, for a default instance:
     "sp_dropserver 'SYSTEM1.'"
   ■ Press F5.

6  Delete the contents in the upper pane.

7  Reconnect the database using the name of the virtual server:

   ■ In the top pane, enter
     "sp_addserver 'Virtual_Server_Name\Instance_Name',
     local"
     For example 'INST1-VS\INST1', local for a named instance, or 'INST1-VS', local for a default instance.
Press F5.

Proceed to configuring the SQL service group.

See “Configuring the SQL service group” on page 75.
Installing SQL Server 2005 on the first node

Verify that the volumes or LUNs (virtual disks) on the filer are mounted or connected to the first cluster node. Install Microsoft SQL Server 2005 on the first node using the SQL installation wizard.

Before you begin installing SQL Server 2005, verify that Microsoft Internet Information Services (IIS) is installed and enabled on the system. Otherwise, you will be prompted to install or enable IIS and then restart the installation.

Install the SQL program files to a local disk and the SQL data files to the shared storage managed by the cluster disk group. As you progress through the installation, use the following guidelines to create an installation that will function properly in your environment.

**Note:** Only the portions of the SQL Server installation procedure relevant to the SFW environment are documented. Refer to the Microsoft SQL Server 2005 documentation for detailed installation information.

To install Microsoft SQL Server 2005

1. Navigate to the installation directory and launch `splash.hta`.
2. Under the Install section, click **Server components, tools, Books Online, and samples**.
3. Continue with the installation, following the instructions in the Microsoft SQL Server 2005 Setup Wizard.
   Complete the SQL Server Component Update, System Configuration Check, and Registration Information panels.
4. XIn the Components to Install panel, select SQL Server Database Services and Workstation Components and optionally select any of the other components to install.
   If you install optional components on one node, install the same components in the same order on other nodes.
5. XClick **Advanced** and in the Feature Selection panel, specify the path for SQL Server data files and other selected services. Set the data files to the shared storage managed by the cluster disk group, as follows:
Expanding Database Services, click Data Files, and click Browse.

In the Change Folder panel, set the installation path to the drive letter and location of the volume that was created for the SQL Server system data files (INST1_DATA_FILES). You can allow the rest of the path (Program Files\Microsoft SQL Server) to remain and click OK. You must set the same path on all nodes.

If you selected the Analysis Services option in step 4 on page 66, expand Analysis Services, click Data Files, and click Browse to specify the same location as for the SQL Server data files. Click OK when done.

6 In the Feature Selection panel, expand Client Components and ensure that Connectivity Components and Management tools are selected. Click Next.

7 In the Instance Name panel, enter an instance name (for example, INST1) and click Next.
Use the same instance name when you install this instance of SQL Server 2005 on failover nodes. If you are installing multiple instances of SQL in the cluster, each instance must have a unique instance name.

8 In the Service Accounts panel, make the following selections and click Next:
  ■ Select **Use a domain user account**.
  
  ![Service Account Panel](image)

  ■ Specify the user name, password, and domain.

  **Note:** If SQL Server services are not installed with a domain user account, the SQL service group may fail to come online on the cluster nodes. It may come online only on the node on which SQL Server was installed last. In such a case, you must perform additional steps after configuring the SQL service group.
  

  ■ Clear all the check boxes that start services except for the SQL Browser, so that the SQL Server is not brought online.

9 Follow the wizard instructions to complete the installation. Reboot if prompted.

10 Install any SQL service packs or hotfixes if required.

11 Set all SQL services to manual start except for the SQL Browser service. Set the SQL Browser service to automatic.
Preparing to install SQL Server 2005 on the second node

Follow the procedures provided in this section before installing SQL Server 2005 on additional nodes. These procedures must be performed for every node that is intended to be a part of the cluster.

Stopping the SQL Server 2005 service

Stop a running SQL Server service on the configured node so the databases on the shared disk can be manipulated by the installation on the second node.

To stop the SQL Server service
1. Start the SQL Server Configuration Manager (Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Configuration Manager).
2. In the left pane, click SQL Server 2005 Services.
3. In the right pane, right-click the SQL Server instance and select Stop.
4. Repeat for all other SQL Server services that are running on the server.
5. Exit the SQL Server Configuration Manager.

Disconnecting virtual disks from the first node

See “Disconnecting virtual disks from the cluster nodes” on page 54.

Releasing disks from the first node (if you use Windows LDM)

See “Unassigning a drive letter” on page 57.
See "Releasing disks (if you use Windows LDM)" on page 57.

Connecting virtual disks to the second node

See "Connecting virtual disks to the cluster node" on page 53.

Mounting volumes on the second node (if you use Windows LDM)

See "Mounting volumes (if you use Windows LDM)" on page 56.
Installing and configuring SQL Server

Installing SQL Server 2005 on the second node

Renaming shared SQL Server 2005 files

Before installing SQL on the second node, open the SQL Server system data files volume (INST1_DATA_FILES) and rename or remove the first node SQL Server system data files. The files will be replaced during the installation of SQL Server on the additional nodes.

If you rename the folder that contains the system data files, the files are available as backup files in case problems occur during the second node SQL Server installation. Once the installation completes successfully, you can then delete the renamed folder and its contents.

To rename shared SQL Server data files

1. On the computer on which the cluster disk group is imported, open the volume that holds the SQL Server data files.
2. Rename the folder that contains the SQL Server data files.

Installing SQL Server 2005 on the second node

Verify that the volumes or LUNs (virtual disks) on the filer are mounted or connected to the first cluster node. Install Microsoft SQL Server 2005 on the first node using the SQL installation wizard.

See “Installing SQL Server 2005 on the first node” on page 66.

Removing shared SQL Server 2005 files

If you renamed the shared SQL Server folder from the SQL Server system data files volume prior to installing SQL on the second node, you can delete the renamed folder and files now.

To delete the renamed SQL Server data files

1. On the computer on which the cluster disk group is imported, open the volume that holds the renamed SQL Server data files.
2. Select the renamed SQL Server data folder and files contained in the volume, and press Delete.
Installing and configuring SQL Server

Installing SQL Server 2005 on the second node

Setting the internal name of the clustered instance

Use the SQL Server Management Studio to set the internal name of the clustered instance to be the virtual server name\instance name (for example, INST1-VS\INST1).

**Note:** Do this procedure after you install and configure SQL Server on the last node for this instance, so that you need to do the procedure only once. Do the procedure from the last node, assuming that the node is still connected to the shared volumes.

The virtual server name you assign must be unique within the cluster. The virtual server name\instance name is used by the SQL Server clients to access the database. You specify the virtual server name again when configuring the VCS SQL service group for this instance.

**Warning:** For a disaster recovery configuration, the virtual server name on the secondary site cluster must match the one on the primary site cluster.

Before you set the internal name of the instance, start the SQL Server services on the node that is currently connected to the shared volumes.

**To start a SQL Server service**

1. Start the SQL Server Configuration Manager (Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager).
2. In the left pane, click **SQL Server 2005 Services**.
3. In the right pane, right-click the SQL Server instance and select **Start**.
4. Repeat for all other SQL Server services that are not running on the server.
5. Exit the SQL Server Configuration Manager.

**To set the internal name of the clustered instance**

1. Start the SQL Server Management Studio (Start > All Programs > Microsoft SQL Server 2005> SQL Server Management Studio).
2. In the **Connect to Server** window, provide connection information:

- Select the Database Engine from the server type drop down list.
- Enter the name in the format `System_Name\Instance_Name`.
- Select the appropriate authentication method.
- Enter valid user credentials if using Domain authentication and click **Connect**.

3. Find the SQL Server name as follows:

   - Right-click the instance in the Object Explorer and click **New Query**.
   - In the right pane of the SQL Server Management Studio, enter the query text:
     ```sql
     sp_helpserver
     ```
   - Press **F5**. The right pane divides into an upper and lower pane.
     - Make note of the name listed in the lower pane, which is in the format `System_Name\Instance_Name`, for example, `SYSTEM1\INST1`. (For a default instance, you see only `System_Name`.)

4. Delete the contents in the upper pane.
5 Disconnect the database as follows:
   - In the upper pane, enter the following:
     \sp\dropserver "System_Name\Instance_Name"
     where System_Name\Instance_Name is the name noted in step 3.
     For example, for a named instance:
     \sp\dropserver "SYSTEM1\INST1"
     For example, for a default instance:
     \sp\dropserver "SYSTEM1"
   - Press F5.

6 Delete the contents in the upper pane.

7 Reconnect the database using the name of the virtual server:
   - In the top pane, enter the following:
     \sp\addserver "Virtual_Server_Name\Instance_Name",
     local
     For example, for a named instance:
     \sp\addserver "INST1-VS\INST1",
     local
     For example, for a default instance:
     \sp\addserver "INST1-VS",
     local
   - Press F5.

8 Exit the SQL Server Management Studio.
Assigning ports for multiple SQL Server instances

If you are running multiple SQL Server instances, you must assign a different port to each named instance. You can assign static or dynamic ports. Refer to the Microsoft Knowledge Base for the instructions on assigning ports.

At the time of this release, this information is in the following article:

Microsoft Knowledge Base Article - 823938: How to configure an instance of SQL Server to listen on a specific TCP port or a dynamic port

Refer to:

http://support.microsoft.com/kb/823938/en-us

If you wish to change the port after configuring the SQL service group, you must perform the steps in the following order:

- Bring the SQL service group online or partially online (upto the registry replication resource) on a cluster node.
- On the node on which the SQL service group is online or partially online, change the port assigned to the SQL instance. Refer to the instructions mentioned in the Microsoft Knowledge Base article specified earlier.
- Take the SQL service group offline on the node, and then bring it online again. The configuration changes will be replicated to the remaining cluster nodes.

Proceed to configuring the SQL service group.

See “Configuring the SQL service group” on page 75 for configuration steps.
Chapter 4

Configuring the SQL service group

This chapter contains the following topics:

- “About configuring the SQL service group” on page 76
- “Before configuring the SQL service group” on page 76
- “Configuring a SQL Server service group” on page 77
- “Running SnapManager for SQL” on page 82
- “Creating a SQL Server user-defined database” on page 82
- “Verifying the service group configuration” on page 86
- “Administering a SQL Server service group” on page 88
About configuring the SQL service group

Configuring the SQL Server service group involves creating resources for the NetApp and SQL agents. VCS provides several ways of configuring a service group, which include the service group configuration wizard, Cluster Manager (Java Console), and the command line. This chapter provides instructions on configuring a SQL service group using the SQL Server Configuration Wizard.

The SQL Server Configuration Wizard enables you to create a SQL Server service group and define the attributes for its resources on all the nodes within the cluster simultaneously.

Before configuring the SQL service group

- Verify that VCS, along with the VCS database agent for SQL Server, is installed on all the cluster nodes.
- Verify that you have configured a VCS cluster using VCS Cluster Configuration Wizard (VCW).
- Verify that SQL Server is installed and configured identically on all the cluster nodes.
- Verify that you have VCS Administrator privileges. This user classification is required to create and configure a service group.
- You must be a Local Administrator on the node where you run the wizard. If you wish to configure detail monitoring, you must be logged on as a Domain Administrator.
- You must be an Administrator for the NetApp filer containing the LUNs created to store SQL Server components.
- Verify that the Veritas High Availability Daemon (HAD) is running on the system from where you run the wizard.
- Verify the volumes or LUNs (virtual disks) created to store the following data components are mounted or connected to the node where you run the wizard and dismounted or disconnected from other nodes in the cluster:
  - SQL Server system data files
  - Registry replication information.
  - User database files
  - User database log files
- Verify the SQL Server 2000 or SQL Server 2005 instance is installed identically on all nodes that will participate in the service group.
If you have configured Windows Firewall, add the following to the Firewall Exceptions list:

- Port 14150 or the VCS Command Server service,
  \%vcs_home\%\bin\CmdServer.exe.
  Here, \%vcs_home\% is the installation directory for VCS, typically
  C:\Program Files\Veritas\Cluster Server.
- Port 14141
  For a detailed list of services and ports used by VCS, refer to the Veritas

Configuring a SQL Server service group

This section describes how to create a new SQL service group. To modify an existing service group, see “Modifying a SQL service group configuration” on page 88.

Symantec recommends reviewing the resource types and the attribute definitions of the agents before configuring the agents. You can find this information in the appendix.

See “Resource type definitions” on page 167.

For sample configuration files and resource dependency graphs of the SQL service groups, see “Sample configurations” on page 189.

If you wish to configure detail monitoring for Microsoft SQL, you must have the SQL Server agent running at the basic level of monitoring, that is, the DetailMonitor attribute must be set to 0. The SQL Server agent uses a script to monitor the status of the database. A sample SQL script, located at
\%VCS_HOME\%\bin\SQLServer<2000/2005>\sample_script.sql, is
provided with the agent for the purpose. If the script is successfully executed during monitoring, the agent considers the database instance available. If the execution fails, the database instance is considered not available and the service group faults and fails over to the failover nodes. You can customize the script to meet your configuration requirements.

Note: You should use a separate script for each SQL Server service group that exists in the cluster. The script should exist on all the nodes in the service group.

To create a SQL Server service group on the cluster

1. Ensure that you have stopped the SQL Server service for the instance.
2. Start the SQL Configuration Wizard from the Solutions Configuration Center or click `Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard`.

3. In the Select Configuration Option panel, choose `MS SQL Server Service Group Configuration` and `Create`, and click `Next`.

4. Verify that you have met the prerequisites listed and click `Next`.

5. Specify the service group name and system list:

- In the Service Group Name field, specify a name for the SQL Server service group, for example, `INST1_SG`. If there are multiple instances, ensure that the name is unique within the cluster.
- In the Available Cluster Systems box, select the systems on which to configure the service group and click the right-arrow to move the systems to the Systems in Priority Order list.
- To change the priority of a system in the Systems in Priority Order list, select the system and click the up and down arrow icons. Arrange the systems in priority order as failover targets for the group. The server that needs to come online first must be at the top of the list. For an active/active configuration, ensure that the active and failover systems are set differently for each instance. For example, if the system priority for the first instance is `SYSTEM1`, then `SYSTEM2`, the system priority for the second instance should be `SYSTEM2`, then `SYSTEM1`.
- Click `Next`.
6 In the SQL Server Instance Selection panel, select the SQL Server instance and any other services that were installed and that need to be configured for high availability in your environment.

Clear the **Configure NetApp SnapMirror Resource(s)** check box. This option is applicable only in case of a disaster recovery configuration. The SnapMirror resource is used to monitor replication between filers at the primary and the secondary site, in a disaster recovery configuration. If you are setting up a disaster recovery environment, check this check box to configure the SnapMirror resource at the primary site. Note that you must configure the SnapMirror resource only after you have configured the cluster at the secondary site.

Click **Next**.

7 The User Databases List panel summarizes the databases on this instance of SQL. Click **Next**.

8 In the Detail Monitoring Configuration panel, optionally enable a monitoring script as follows:

- Select the check box for the SQL Server instance for which detail monitoring will be configured. Only the instances selected in step 6 on page 79 are available for selection.
- Specify the fully qualified user name and password for connecting to SQL Server database. Make sure the specified user has SQL Server log on permissions.
- If the path of the script is same on all nodes, choose the **Global** option, click the **SQL Monitor Script** text box, and specify the path to the script.
Configuring the SQL service group

Configuring a SQL Server service group

on the first system displayed in the System Name list. If the path of the script is different on all nodes, choose the Per System option, and specify the path for the script on each node. Make sure the specified path exists on all the systems in the cluster.

- Select the Fail over service group if detail monitoring script execution fails checkbox, if not already selected. This will enable the SQL agent to fail over the service group if the detail monitoring script execution fails.
- Click Apply.

9 If you want to configure detail monitoring for additional instances, repeat step 8 on page 79 for all the instances for which detail monitoring will be configured.

10 Click Next.

11 In the Registry Replication Path panel, specify the mount path to the registry replication volume (INST1_REGREP_VOL) and click Next. Symantec recommends that RegRep resources and SQL data be in separate volumes.

12 Configure the virtual server as follows:

■ Enter the virtual name for the server, for example INST1-VS. Ensure that the virtual server name you enter is unique in the cluster. It is the same as the virtual server name specified when setting the internal name of the clustered instance.
Enter a unique virtual IP address that is currently not being used on your network, but is in the same subnet as the current computer.

Enter the subnet mask to which the virtual IP address belongs.

For each system in the cluster, select the public network adapter name. Select the **Adapter Display Name** field to view the adapters associated with a system.

The wizard displays all TCP/IP enabled adapters on a system, including the private network adapters, if they are TCP/IP enabled. Make sure that you select the adapters to be assigned to the public network, and not those assigned to the private network.

If you require a computer object to be created in the Active Directory (AD), click **Advanced Settings**, check the **Active Directory Update Required** checkbox, and select the Organizational Unit from the drop-down list.

Click **Next**.

13. On the Initiator Selection panel, select the initiator for the virtual disk from the list of available initiators displayed for each cluster node, and then click **Next**.

If you are configuring MPIO over FC, you must select at least 2 FC initiators for each cluster node. Note that the node from which you run this wizard already has an initiator selected by default. This is the initiator that was specified when you connected the LUNs to this cluster node.

14. In the Service Group Summary, review the service group configuration. The **Resources** box lists the configured resources. Click a resource to view its attributes and their configured values in the **Attributes** box.

The wizard assigns unique names to resources based on their respective name rules. Optionally, change the names of the resources, if desired.

- To edit a resource name, click the resource name or press the F2 key. Press Enter after editing each resource name.
- To cancel editing a resource name, press Esc.

15. Click **Next** and when prompted to confirm creating the service group, click **Yes**. Messages indicate the status of the commands.

16. Complete the SQL Server service group configuration:

- In the **Bring the service group online** check box, if you want to bring the service group online later, clear the check box.
  
  You may want to review the service group configuration in the Cluster Manager (Java Console) before bringing the service group online. You can use the Cluster Manager to bring the service group online later.
Configuring the SQL service group

Running SnapManager for SQL

- Click Finish to exit the wizard or click Next to configure another SQL service group or an MSDTC service group.
  The wizard marks all the resources in the service group as CRITICAL. If desired, use Cluster Manager (Java Console) or the command line to change the state.

To configure an MSDTC service group, see “Configuring an MSDTC service group for high availability” on page 91.

Running SnapManager for SQL

After configuring the service group, you may want to run the SnapManager Configuration Wizard on the node on which the service group is online, to schedule backups of SQL Server database. You must adhere to the following requirements while running SnapManager for SQL:

- Make sure the SQL service group is online.
- Do not move the SQL Server database components.

If you are scheduling backups in a VCS cluster, schedule them on the node on which the service group is online. If the SQL service group fails over to another node, you must set up the backup schedule again on the new node.

See the Network Appliance documentation for more information about running SnapManager for SQL.

Creating a SQL Server user-defined database

The following tasks enable you to use VCS to create and manage a SQL Server user-defined database.

- Create volumes for a user-defined SQL Server database and its transaction log.
- Create a new SQL Server user-defined database and point the database files and transaction log to the paths of the new volumes.
- Use the SQL Server Configuration Wizard to add the NetAppFiler and NetAppSnapDrive resources for the user databases.
Creating new volumes or LUNs

If you have not already created volumes or LUNs for a user-defined SQL Server database and its transaction log, create them now. In the sample deployment these volumes are named:

- INST1_DB1_VOL: contains a user-defined database file
- INST1_DB1_LOG: contains a user-defined database log file

Creating a new SQL Server database

Create a new SQL Server database and point the database files and transaction log to the new volumes or LUNs created for them.

To create a new SQL Server 2000 database

1. Open SQL Server Database Manager (Start > All Programs > Microsoft SQL Server > Enterprise Manager).
2. Right-click on Databases and then click New Database.
3. In the New Database page, enter a name for the new database.
4. Click the browse button (...) in the Location column, browse to the location of the volume where you want to create your user database, and click OK.
5. Choose other file properties as desired.
6. Click the Transaction Log tab.
7. Click ... (ellipsis button) in the Location column and browse to the location of the volume you created for the transaction log, and click OK.

To create a new SQL Server 2005 database

1. Open SQL Server Database Manager (Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio).
2. Expand the icon associated with your server.
3. Right-click on Databases and then click New Database.
4. In the New Database page, type a name for the new database.
5. Click ... (ellipsis button) in the Path column, browse to the location of the volume where you want to create your user database, and click OK.
6. Select and edit other file properties as desired.
7. Click ... (ellipsis button) in the Path column for the Transaction Log row and browse to the location of the volume you want to create for the transaction log, and click OK.
8 To add more data files if required:
   ■ Select Add.
   ■ Edit the properties in the new data file rows as required.
9 Click OK.

Adding storage agent resources to the SQL service group

Before running the SQL Server Agent wizard to add the storage agent resources:
   ■ Make sure the SQL service group is online.
   ■ Make sure the volumes for the user database and transaction logs are mounted.

Note: Mount or NetAppSnapDrive resources are required only if the database is created on a new volume.

To add storage agent resources to the SQL service group

1 Start the SQL Server Configuration Wizard from the Solutions Configuration Center or click Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard.
2 Select the MS-SQL Server Service Group Configuration, select the Edit option, and click Next.
3 Review the Prerequisites page and click Next.
4 In the Service Group Selection page, select the service group and click Next.
5 Click Yes on the VCS Notice informing you that the service is not completely offline. No adverse consequences are implied.
6 In the Service Group Configuration page, click Next.
7 In the SQL Server Instance Selection page, make sure the correct instance of SQL Server is selected and click Next.
8 In the User Databases List page, make sure the databases are shown with correct paths and click Next.
9 If a database is not configured correctly, a VCS warning appears indicating potential problems. Click OK to continue.
10 In the Detail Monitoring and succeeding pages, review the information and click Next to continue.
11 Click Yes to continue when a VCS Notice indicates the configuration will be modified.
To complete the user database configuration:

- Click **Finish** to exit the wizard.
  The wizard marks all the resources in the service group as **CRITICAL**. If desired, use Cluster Manager (Java Console) or the command line to change the state.
- Click **Next** to configure another SQL service group or an MSDTC service group.

To configure an MSDTC service group, see “Configuring an MSDTC service group for high availability” on page 91.
Verifying the service group configuration

Failover simulation is an important part of configuration testing. This section provides steps to verify the SQL Server service group configuration by bringing the service group online, taking the service group offline, and switching the service group to another cluster node.

Bringing the service group online

Perform the following steps to bring the service group online from the VCS Java or Web Console.

To bring a service group online from the Java Console

1. In the Cluster Explorer configuration tree, select the SQL service group to be taken online.
2. Right-click the service group name, and select Enable Resources. This enables all resources in the service group.
3. Right-click the service group name, and select the system on which to enable the service group. (Right-click > Enable > system_name or Right-click > Enable > All)
4. Save your configuration (File > Close Configuration).
5. Right-click the service group and select to online the service group on the system. (Right-click > Online > system_name)

Taking the service group offline

Perform the following steps to take the service group offline from the VCS Java or Web Console.

To take a service group offline from the Java Console

1. On the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group.
   or
   Select the cluster in the Cluster Explorer configuration tree, select the Service Groups tab, and right-click the service group icon in the view panel.
2. Choose Offline, and choose the appropriate system from the pop-up menu. (Right-click > Offline > system_name)
Switching the service group

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

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

To switch service groups

1. In the Veritas Cluster Manager (Java Console), click the cluster in the configuration tree, click the Service Groups tab, and right-click the service group icon in the view panel.
   - Click Switch To, and click the appropriate node from the menu.
   - In the dialog box, click Yes. The service group you selected is taken offline on the original node and brought online on the node you selected.
     If there is more than one service group, you must repeat this step until all the service groups are switched.

2. Verify that the service group is online on the node you selected to switch to in the earlier step.

3. To move all the resources back to the original node, repeat step 1 for each of the service groups.

To shut down an active cluster node

1. Gracefully shut down or restart the cluster node where the service group is online.

2. In the Veritas Cluster Manager (Java Console) on another node, connect to the cluster.

3. Verify that the service group has failed over successfully, and is online on the next node in the system list.

4. If you need to move all the service groups back to the original node:
   - Restart the node you shut down in step 1 on page 87.
   - Click Switch To, and click the appropriate node from the menu.
   - In the dialog box, click Yes. The service group you selected is taken offline and brought online on the node that you selected.
Administering a SQL Server service group

You can dynamically modify the SQL service group configuration in several ways, including the SQL Server Configuration Wizard, Cluster Manager (Java Console), Cluster Manager (Web Console), and the command line. The following steps describe how to modify the service group using the SQL Server Configuration Wizard.

Modifying a SQL service group configuration

Prerequisites

- If the SQL Server service group is online, you must run the wizard from a node on which the service group is online. You can then use the wizard to add resources to and remove them from the configuration. You cannot change resource attributes.

- To change the resource attributes, you must take the service group offline. However, the NetAppFiler and NetAppSnapDrive resources for the service group should be online on the node where you run the wizard and offline on all other nodes.

- If you are running the wizard to remove a node from the service group’s system list, do not run the wizard on the node being removed.

- If you are running the wizard to add or remove NetAppSnapDrive resources for user defined databases, make sure the service group is online.

To modify a SQL Server service group

1. Start the SQL Server Configuration Wizard. Click Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard.

2. In the Select Configuration Option panel, click MS SQL Server - Service Group Configuration, click Edit, and then click Next.

3. Review the prerequisites and click Next.

4. In the Service Group Selection panel, select the service group to modify and click Next.

5. In the Service Group Configuration panel, add or remove systems from the service group’s SystemList and click Next.

6. In the SQL Server Instance Selection panel, select the SQL Server instance to be made highly available and click Next.
Configuring the SQL service group

Administering a SQL Server service group

7 In the User Databases List panel, verify the master and user defined databases configured for the SQL instance. The wizard will create NetAppSnapDrive resource for each database. Click Next.

8 Follow the wizard instructions and make desired modifications to the service group configuration.

Deleting a SQL service group

The following steps describe how to delete a SQL Server service group using the configuration wizard.

To delete a SQL Server service group

1 Start the SQL Server Configuration Wizard. Click Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard.

2 In the Select Configuration Option dialog box, choose the MS-SQL Server - Service Group Configuration option, choose the Delete option, and click Next.

3 Review the prerequisites and click Next.

4 In the Service Group Selection dialog box, select the service group to delete and click Next.

5 In the Service Group Summary dialog box, click Next.

6 A message appears informing you that the wizard will run commands to delete the service group. Click Yes to delete the service group.

7 Click Finish.
Configuring the SQL service group

Administering a SQL Server service group
Configuring an MSDTC service group for high availability

This chapter contains the following topics:

■ “About configuring the MSDTC service group” on page 92
■ “Before configuring the MSDTC service group” on page 92
■ “Reviewing the configuration” on page 93
■ “Creating an MSDTC service group” on page 95
■ “Creating an MSDTC client” on page 97
■ “Verifying the installation” on page 98
About configuring the MSDTC service group

This chapter describes the steps required to create a new MSDTC service group, configure the MSDTC Server, and configure the MSDTC client using the configuration wizard. The MSDTC agent comprises two parts; MSDTC client and MSDTC server. The MSDTC client and the MSDTC server must not run on the same cluster node.

Before configuring the MSDTC service group

- You must be a cluster administrator. This user classification is required to create and configure a service group.
- You must be a local administrator on the node where you run the wizard.
- Verify that the SQL Server agent is installed on all cluster nodes.
- Verify that the VCS cluster is configured using the VCS Cluster Configuration Wizard.
- Verify that the MSDTC service is installed on all nodes that will participate in the MSDTC service group.
- Assign a unique virtual server name and virtual IP address to the MSDTC server.
- Verify that the Distributed Transaction Coordinator service is stopped.
- Verify that you have created the volumes or LUNs (virtual disks) for MSDTC log, and MSDTC registry replication, on the shared disk.
  See “Managing storage using Network Appliance filer” on page 52.
  See “Managing storage using Windows Logical Disk Manager” on page 55.
- Verify that the volumes or LUNs containing the MSDTC logs and registry replication directory are mounted or connected to one node (the node on which you are configuring the service group) and dismounted and disconnected from all other nodes.
- If you have configured Windows Firewall, add the following to the Firewall Exceptions list:
  - Port 14150 or the VCS Command Server service,
    %vcs_home%\bin\CmdServer.exe.
    Here, %vcs_home% is the installation directory for VCS, typically
    C:\Program Files\Veritas\Cluster Server.
  - Port 14141
  For a detailed list of services and ports used by VCS, refer to the Veritas Cluster Server Installation and Upgrade Guide.
Reviewing the configuration

MSDTC servers can coexist with SQL servers on the same cluster nodes. If the MSDTC server and the SQL server are running on the same node, the MSDTC client is left in the default configuration. If the MSDTC server is not configured on the same node as the SQL server, then the MSDTC client must be configured on that node using the SQL Server Configuration Wizard.

For instance, a SQL Server configuration in a VCS cluster might span four nodes and two sets of shared storage. Two configurations are possible:
- SQL server is configured on different nodes than the MSDTC server
- SQL server is configured on the same node as the MSDTC server

Figure 5-1 MSDTC Server configured on different nodes than SQL Server
Figure 5-2 MSDTC Server configured on the same node as SQL Server
Creating an MSDTC service group

MSDTC is a global resource and is accessed by more than one SQL Server service group. Symantec recommends you to configure one MSDTC service group in a VCS cluster. VCS provides an SQL Server Configuration Wizard that guides you through the process of configuring an MSDTC service group. You can also use this wizard to modify an MSDTC service group configuration. This section describes the steps required to create a new MSDTC service group using the wizard.

To configure an MSDTC service group

1. Start the SQL Server Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard**.
   If you have just configured a SQL service group and you are in the Configuration Wizard, this step is not necessary.

2. In the Select Configuration Option panel, click **MSDTC Server - Service Group Configuration**, click **Create**, and then click **Next**.

3. Verify that you have met the prerequisites and click **Next**.

4. Specify the service group name and system list.
   - Enter a name for MSDTC service group.
   - In the Available Cluster Systems box, select the systems on which to configure the service group and click the right-arrow to move the systems to the service group’s system list. Make sure to select the systems that are not in the SystemList attribute for an Exchange service group configured in the cluster.
     To remove a system from the service group’s system list, select the Systems in Priority Order list and click the left arrow.
     To change a system’s priority in the service group’s system list, select the system from the Systems in Priority Order and click the up and down arrows. The system at the top of the list has the highest priority while the system at the bottom of the list has the lowest priority.
   - Click **Next**. The wizard starts validating your configuration. Various messages indicate the validation status.

5. Specify the information related to the virtual server.
   - Enter the virtual name for the node. This is the server name on which DTC service is running. Ensure that the virtual server name you enter is unique in the cluster.
   - Enter a unique virtual IP address for the MSDTC server.
■ Enter the subnet mask to which the virtual IP address belongs.
■ Click **Advanced**... to specify additional details for the Lanman resource.
  ■ Select the **AD Update required** check box to enable the Lanman resource to update the Active Directory with the virtual name.
  ■ Select the distinguished name of the Organizational Unit for the virtual server. By default, the Lanman resource adds the virtual server to the default container Computers.
  The user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts.
  ■ Click **OK**.
  ■ For each system in the cluster, select the public network adapter name. Select the **Adapter Name** field to view the adapters associated with a system.
    The wizard displays all TCP/IP enabled adapters on a system, including the private network adapters, if they are TCP/IP enabled. Make sure that you select the adapters to be assigned to the public network, and not those assigned to the private network.
  ■ If you require a computer object to be created in the Active Directory (AD), click **Advanced**, check **AD Update**, and select the Organizational Unit from the drop down list.
  ■ Click **Next**.

6 Specify the drive letter for the MSDTC log and replication directory and click **Next**. Symantec recommends using different paths for these directories.
Clear the **Configure NetApp SnapMirror Resource(s)** check box. This option is applicable only in case of a disaster recovery configuration. The SnapMirror resource is used to monitor replication between filers at the primary and the secondary site, in a disaster recovery configuration. If you are setting up a disaster recovery environment, check this check box to configure the SnapMirror resource at the primary site. The SnapMirror resource must be configured only after you have configured the cluster at the secondary site.

7 On the Initiator Selection panel, select the initiator for the virtual disk from the list of available initiators displayed for each cluster node, and then click **Next**.
If you are configuring MPIO over FC, you must select at least two FC initiators for each cluster node. Note that the node from which you run this wizard already has an initiator selected by default. This is the initiator that was specified when you connected the LUNs to this cluster node.

8 Review the service group configuration and change the resource name if desired.
The Resources box lists the configured resources. Click on a resource to view its attributes and their configured values in the Attributes box.

- The wizard assigns unique names to resources. Change names of the resources, if desired.
  To edit a resource name, select the resource name and either click it or press the F2 key. Press enter after editing each resource name. To cancel editing a resource name, press Esc.
- Click Next to create the service group.
- A message appears informing you that the wizard will run commands to create the service group. Click Yes to create the service group.
  Various messages indicate the status of these commands. After the commands are executed, the completion dialog box appears.

9 In the Completing the MSDTC Configuration Wizard panel, check Bring the service group online to bring the configured service group online. To bring the service group online later, leave this option unchecked.

10 Click Finish.

11 Click Next to create an MSDTC client.

Creating an MSDTC client

Set the MSDTC client to run on nodes where:

- A SQL instance is configured to run
- The MSDTC server is not configured to run.

Before configuring the MSDTC configuration wizard to configure an MSDTC client:

- Verify the MSDTC service group is online in the cluster.
- Verify the node on which you run the wizard is not a part of an MSDTC service group system list.

To configure an MSDTC client

1 Start the SQL Server Configuration Wizard. Click Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard.

2 Click MSDTC Client Configuration and click Next.

3 Verify that you have met the prerequisites and click Next.

4 Specify the nodes on which the MSDTC client will be configured.
  - Select the nodes in the Available Cluster Systems list.
Make sure you select the systems that are not in the SystemList attribute for an Exchange service group configured in the cluster.

- Click the right arrow to add them to the Selected systems list.
- The Unavailable Cluster Systems lists the nodes that have an MSDTC service group configured and are not available for setting up an MSDTC client.
  MSDTC client must not be configured on a node that has MSDTC server configured.
- Click **Next**.

5. If the MSDTC service group is not online in the cluster, an informational message appears informing you that the wizard will bring the MSDTC service group online. Click **Yes**.

6. Specify the virtual DTC name and click **Next**.

7. Click Next to return to the **Select Configuration Option** choices.
   See “Configuring a SQL Server service group” on page 77 if you have not already configured the SQL Server service group.

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

### Verifying the installation

Verify your installation by switching online nodes or by shutting down the computer that is currently online. Either process will test that the service group can be smoothly transferred between nodes.

Shutting down a node creates an actual failure, stressing your system, but more truly testing its high availability than by switching nodes. If you do shut down the online computer in your cluster, remember to bring it back up after you have confirmed that the service group successfully failed over to another node.

Complete the procedure “Verifying the service group configuration” on page 86 to verify the service group configuration.
Making a standalone SQL Server highly available

This chapter contains the following topics:

- “About making a standalone SQL server highly available” on page 100
- “Reviewing the configuration” on page 101
- “Configuring the storage hardware and network” on page 103
- “Preparing the standalone SQL Server” on page 104
- “Installing and configuring VCS on the standalone SQL server” on page 106
- “Installing and configuring SQL Server on additional nodes” on page 106
- “Moving the existing SQL Server data files and user databases” on page 107
- “Configuring the VCS SQL Server service group” on page 107
- “Creating a SQL Server user-defined database” on page 108
- “Verifying the installation” on page 108
About making a standalone SQL server highly available

This chapter describes the procedure to convert a standalone SQL Server into a clustered SQL Server in a new Veritas Cluster Server environment. This environment involves an active-passive configuration with one to one failover capabilities.

If you are planning a new SQL Server deployment, refer to “Installing and configuring SQL Server” on page 49. If you are planning to deploy an active-active configuration with multiple SQL instances, refer to “Active-Active configuration” on page 109.

Note: In addition to the information contained in this chapter, the procedures described in Microsoft Knowledge Base Article - 224071: INF: Moving SQL Server databases to a New Location with Detach/Attach are required. Refer to: http://support.microsoft.com/default.aspx?scid=kb;en-us;224071
Reviewing the configuration

This chapter describes the tasks needed to incorporate an existing standalone SQL Server into a high available environment in order to ensure that the mission critical SQL resource is always available.

This chapter describes the tasks necessary to create a virtual server in an active-passive SQL configuration. The active node of the cluster hosts the virtual server. The second node is a dedicated redundant server able to take over and host the virtual server in the event of a failure on the active node. At the end of this process, their environment will look like this:

Figure 6-1  Active-Passive configuration

The virtual SQL Server is online on SYSTEM1, serving client requests. The shared LUNs (virtual disks) provide storage for the SQL Server databases. SYSTEM2 waits in a warm standby state as a backup node, prepared to begin handling client requests if SYSTEM1 becomes unavailable. From the user’s perspective there will be a small delay as the backup node comes online, but the interruption in effective service is minimized.
Sample configuration

A sample setup is used through this guide to illustrate the installation and configuration tasks.

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

- SQL virtual server: the IP address should be the same on all nodes
- Cluster IP address: used by Veritas Cluster Manager (Web Console)

You should have these IP addresses available before you start deploying your environment. The following names describe the objects created and used during the installation and configuration:

<table>
<thead>
<tr>
<th>Name</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM1  &amp; SYSTEM2</td>
<td>server names; SYSTEM1 is the existing standalone SQL server</td>
</tr>
<tr>
<td>INST1_SG</td>
<td>Microsoft SQL Server service group</td>
</tr>
<tr>
<td>SQL_CLUS1</td>
<td>virtual SQL server cluster</td>
</tr>
<tr>
<td>INST1_DATA_FILES</td>
<td>volume for Microsoft SQL Server system data files</td>
</tr>
<tr>
<td>INST1_DB1_VOL</td>
<td>volume for storing a Microsoft SQL Server user-defined database</td>
</tr>
<tr>
<td>INST1_DB1_LOG</td>
<td>volume for storing a Microsoft SQL Server user-defined database log file</td>
</tr>
<tr>
<td>INST1_REGREP_VOL</td>
<td>volume that contains the list of registry keys that must be replicated among cluster systems for the SQL server</td>
</tr>
<tr>
<td>INST1</td>
<td>SQL Instance Name</td>
</tr>
<tr>
<td>INST1-VS</td>
<td>name of the SQL Virtual Server</td>
</tr>
</tbody>
</table>
Configuring the storage hardware and network

Use the following procedures to configure the hardware and verify DNS settings.

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

To verify the DNS settings for all systems on which SQL will be installed
1. Open the Control Panel (Start > Control Panel).
2. Open Network and Dial-up Connections.
3. Ensure the public network adapter is the first bound adapter:
   - From the Advanced menu, click Advanced Settings.
   - On the Adapters and Bindings tab, verify the public adapter is the first adapter in the Connections list. If necessary, use the arrow button to move the adapter to the top of the list.
   - Click OK.
4. In the Network and Dial-up Connections window, double-click the adapter for the public network.
   When enabling DNS name resolution, make sure that you use the public network adapters, and not those configured for the VCS private network.
5. From the status window, click Properties.
Preparing the standalone SQL Server

Complete the following tasks before you begin the process of installing VCS and creating a clustered environment:

- Backing up existing SQL data
- Setting SQL Server services to manual start

Backing up existing SQL data

Create a backup of the data on the existing standalone SQL server.
Setting SQL Server services to manual start

Set all SQL Server services to manual start.

To set SQL Server services to manual start

1. Open the SQL Server Service Manager (Start > All Programs > Microsoft SQL Server > Service Manager).

   - Select the standalone server that you plan to incorporate into the cluster from the Server list.
   - Select a service from the Services list.
   - Clear the Auto-start service when OS starts check box.

2. Repeat these steps for all other SQL Server services that are running on the server.
Installing and configuring VCS on the standalone SQL server

Before converting the existing standalone SQL into a clustered server, complete the following procedures:

- Install VCS on the standalone SQL server. Refer to the Veritas Cluster Server Installation and Upgrade Guide for more information.
- Configure the cluster using the VCS Cluster Configuration Wizard (VCW). See “Configuring the cluster” on page 31.
- Create volumes or LUNs (virtual disks) necessary to manage the SQL Server storage. See “Managing storage using Network Appliance filer” on page 52. See “Managing storage using Windows Logical Disk Manager” on page 55.

Installing and configuring SQL Server on additional nodes

Before installing Microsoft SQL Server on additional nodes, ensure the shared volumes or LUNs are imported on the node. SQL Server must have the same configuration on all nodes in the cluster. You will need the following information:

- Instance name (if applicable)
- Destination folder for Program Files and Data Files
- Authentication Mode

Complete the procedures specified in the following topics:
For SQL Server 2000, see “Preparing to install SQL Server 2000 on the second node” on page 60.
For SQL Server 2005, see “Preparing to install SQL Server 2005 on the second node” on page 69.
Moving the existing SQL Server data files and user databases

After completing the SQL installation and configuration on the additional nodes, move the existing standalone SQL Server data files and user databases from the local drive to the shared drives to ensure proper failover operations in the cluster. Complete the following tasks to move the databases:

1. Stop the SQL Server service.
   For SQL Server 2000, see “Stopping the SQL Server 2000 Service” on page 61.
   For SQL Server 2005, see “Stopping the SQL Server 2005 service” on page 69.

2. Verify that you have backed up your existing data.

3. Import the volumes or LUNs to the node where the original files are located on the local drives and mount the volumes (add drive letters).
   See “Connecting virtual disks to the cluster node” on page 53.

4. Move the SQL Server data files and user databases to the shared volumes or LUNs. Follow the procedures described in Microsoft Knowledge Base Article - 224071: INF: Moving SQL Server databases to a New Location with Detach/Attach.
   http://support.microsoft.com/default.aspx?scid=kb;en-us;224071

5. Restart SQL Server.

To start the SQL service

1. Open the SQL Server Service Manager (Start > All Programs > Microsoft SQL Server > Service Manager).

2. Click Start.

Configuring the VCS SQL Server service group

The SQL Server Configuration Wizard enables you to create a SQL Server service group and define the attributes for its resources on all the nodes within the cluster simultaneously.

Complete the procedure “Configuring a SQL Server service group” on page 77 to configure the SQL Server service group.
Creating a SQL Server user-defined database

Complete the procedure “Creating a SQL Server user-defined database” on page 82 to create and manage a SQL Server user-defined database. The procedure includes the following tasks:

- Create volumes for a user-defined SQL Server database and its transaction log.
- Create a new SQL Server user-defined database and point the database files and transaction log to the paths of the new volumes.
- Use the SQL Server Configuration Wizard to add the DiskRes and Mount or NetAppFiler and NetAppSnapDrive resources for the user databases.

Verifying the installation

Verify your installation by switching online nodes or by shutting down the computer that is currently online. Either process will test that the service group can be smoothly transferred between nodes.

Shutting down a node creates an actual failure, stressing your system, but more truly testing its high availability than by switching nodes. If you do shut down the online computer in your cluster, remember to bring it back up after you have confirmed that the service group successfully failed over to another node.

Complete the procedure “Verifying the service group configuration” on page 86 to verify the service group configuration.
Chapter 7

Active-Active configuration

This chapter contains the following topics:

- “About active-active configuration” on page 110
- “Reviewing the configuration” on page 110
- “Installing VCS and configuring the cluster” on page 114
- “Configuring volumes or virtual disks for SQL Server” on page 114
- “Installing and configuring the first instance of SQL Server” on page 115
- “Configuring the VCS service group for the first SQL Server instance” on page 116
- “Creating a SQL Server user-defined database” on page 116
- “Repeating SQL Server installation for additional instances” on page 116
- “Verifying the configuration” on page 117
About active-active configuration

This chapter describes how to install and configure VCS for SQL Server that includes active-active clustering.

Reviewing the configuration

A SQL Server instance is a completely independent SQL Server installation, with its own services, master database, storage, and memory resources. Each instance is defined uniquely by a separate SQL Server virtual server and service group.

SQL Server supports up to 16 independent instances of SQL Server to run on a single machine. A SQL Server instance can fail over to any of the other nodes configured nodes on its system list.

The following figure illustrates a two node active-active configuration. The SQL Server databases are configured on the shared storage on volumes or LUNs. Each SQL Server virtual server is configured in a separate SQL Server service group. Each service group can fail over to the other node in the cluster.

**Figure 7-1**  Active-active configuration

![Active-active configuration diagram](image)

For example, consider a two-node cluster hosting two SQL Server Virtual Servers, BILLING_VS and PAYROLL_VS. The table below and the sample configuration illustrate that the virtual servers are configured in two separate service groups with BILLING_VS online on SYSTEM1 but able to fail over to
SYSTEM2, and PAYROLL_VS online on SYSTEM2 but able to fail over to SYSTEM1.

**Table 7-1** Active-active configuration

<table>
<thead>
<tr>
<th>SQL Virtual Server</th>
<th>Service Group</th>
<th>System List</th>
</tr>
</thead>
<tbody>
<tr>
<td>BILLING_VS</td>
<td>BILLING_SG</td>
<td>SYSTEM1, SYSTEM2</td>
</tr>
<tr>
<td>PAYROLL_VS</td>
<td>PAYROLL_SG</td>
<td>SYSTEM2, SYSTEM1</td>
</tr>
</tbody>
</table>

**Sample configuration**

A sample setup is used to illustrate the installation and configuration tasks for two instances of SQL server, Billing and Payroll. During normal operation, one instance will be online on each of the two servers. If a failure occurs, the instance on the failing node will be brought online on the other server, resulting in two instances running on one server.

During the configuration process, create virtual IP addresses for the following:

- Billing virtual server: virtual IP address is the same on all nodes
- Payroll virtual server: virtual IP address is the same on all nodes
- Cluster IP address: used by Web Console

You should have these IP addresses available before you begin to deploy your environment.
The following names describe the objects created and used during the installation and configuration:

**Table 7-2**  
Active-active configuration objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM1 &amp; SYSTEM2</td>
<td>server names</td>
</tr>
<tr>
<td>SQL_CLUS1</td>
<td>virtual SQL server cluster</td>
</tr>
<tr>
<td>BILLING_VS_SYS_FILES</td>
<td>volume for the SQL Server system data files for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_VS_SYS_FILES</td>
<td>volume for the SQL Server system data files for the payroll instance</td>
</tr>
<tr>
<td>BILLING_DATA</td>
<td>volume for a SQL Server user-defined database for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_DATA</td>
<td>volume for a SQL Server user-defined database for the payroll instance</td>
</tr>
<tr>
<td>BILLING_LOG</td>
<td>volume for a SQL Server user-defined database log file for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_LOG</td>
<td>volume for a SQL Server user-defined database log file for the payroll instance</td>
</tr>
<tr>
<td>BILLING_REGREP</td>
<td>volume for the list of registry keys replicated among the nodes for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_REGREP</td>
<td>volume for the list of registry keys replicated among the nodes for the payroll instance</td>
</tr>
<tr>
<td>BILLING_INST</td>
<td>instance name for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_INST</td>
<td>instance name for the payroll instance</td>
</tr>
<tr>
<td>BILLING_VS</td>
<td>virtual SQL server name for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_VS</td>
<td>virtual SQL server name for the payroll instance</td>
</tr>
<tr>
<td>BILLING_SG</td>
<td>SQL Server service group for the billing instance</td>
</tr>
<tr>
<td>PAYROLL_SG</td>
<td>SQL Server service group for the payroll instance</td>
</tr>
</tbody>
</table>
Configuring the storage hardware and network

Use the following procedures to configure the hardware and verify DNS settings.

To configure the hardware

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

To verify the DNS settings for all systems on which SQL will be installed

1. Open the Control Panel (Start > Control Panel).
2. Open Network and Dial-up Connections.
3. Ensure the public network adapter is the first bound adapter:
   - From the Advanced menu, click Advanced Settings.
   - On the Adapters and Bindings tab, verify the public adapter is the first adapter in the Connections list. If necessary, use the arrow button to move the adapter to the top of the list.
   - Click OK.
4. In the Network and Dial-up Connections window, double-click the adapter for the public network.
   When enabling DNS name resolution, make sure that you use the public network adapters, and not those configured for the VCS private network.
5. From the status window, click Properties.
6 On the General tab:
   ■ Select the Internet Protocol (TCP/IP) check box.
   ■ Click Properties.

7 Select the Use the following DNS server addresses option.

8 Verify that the correct value for the IP address of the DNS server.

9 Click Advanced.

10 On the DNS tab, make sure the Register this connection's address in DNS check box is selected.

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

12 Click OK.

Installing VCS and configuring the cluster

Complete the following procedures to install VCS and then establish the cluster:

■ Install VCS. Refer to the Veritas Cluster Server Installation and Upgrade Guide for more information.

■ Configure the VCS cluster using the VCS Cluster Configuration Wizard (VCW).
   See “Configuring the cluster” on page 31.

Configuring volumes or virtual disks for SQL Server

For each instance of SQL Server, create volumes or LUNs (virtual disks) on the shared storage, as follows:

For the Billing instance, create the following:

■ BILLING_VS_SYS_FILES: volume for the SQL Server system data files
■ BILLING-REGREP: volume for the list of registry keys replicated among cluster nodes for the Billing instance

For the Payroll instance, create the following:

■ PAYROLL_VS_SYS_FILES: volume for the SQL Server system data files
■ PAYROLL_REGREP: volume for the list of registry keys replicated among cluster nodes for the Payroll instance

See “Managing storage using Network Appliance filer” on page 52.
See “Managing storage using Windows Logical Disk Manager” on page 55.
Installing and configuring the first instance of SQL Server

As you follow the procedures to install and configure SQL Server on the cluster, make the following changes to the process:

- Do not accept the default instance name. Specify an instance name for each SQL Server installation.
- Each SQL Server instance must be assigned a different port. The default port is 1433; ports for subsequent instances are generally assigned in descending order (1432, 1431, 1430, etc.).
- Set a unique internal name for each instance, for example BILLING_VS.

Complete the following tasks to install and configure the first SQL Server instance on all nodes of the cluster:

For SQL Server 2000

- “Installing SQL Server 2000 on the first node” on page 58
- “Preparing to install SQL Server 2000 on the second node” on page 60
- “Installing SQL Server 2000 on the second node” on page 62
- “Setting the internal name of the clustered instance” on page 63

For SQL Server 2005

- “Installing SQL Server 2005 on the first node” on page 66
- “Preparing to install SQL Server 2005 on the second node” on page 69
- “Installing SQL Server 2005 on the second node” on page 70
- “Setting the internal name of the clustered instance” on page 71
Configuring the VCS service group for the first SQL Server instance

Consider the following points as you configure the SQL Server service group for the first instance:

- Assign a unique name to the SQL Server service group, for example BILLING_SG.
- Pay close attention to the priority order of the systems. For example, if the system priority for the first instance is SYSTEM1 then SYSTEM2; reverse the priority order for the second instance, so that SYSTEM2 has a higher priority.

See “Configuring a SQL Server service group” on page 77 for instructions.

Creating a SQL Server user-defined database

Create a user-defined database and then configure it with VCS. The procedure includes the following tasks:

- Create volumes or LUNs for a user-defined SQL Server database and its transaction log.
- Create a new SQL Server user-defined database and point the database files and transaction log to the paths of the new volumes.
- Add new VCS storage agent resources (Mount or NetAppSnapDrive) and link them to the existing DiskRes or NetAppFiler resource in the SQL Service Group.

See “Creating a SQL Server user-defined database” on page 82.

Repeating SQL Server installation for additional instances

Repeat the previous steps to install and configure one or more additional SQL Server instances, making the same changes to the process:

- Do not accept the default instance name. Specify a unique instance name for each SQL Server installation.
- Each SQL Server instance must be assigned a different port. The default port is 1433; ports for subsequent instances are generally assigned in descending order (1432, 1431, 1430, etc.).
- Set a unique internal name for each instance, for example PAYROLL_VS.
Complete the following tasks to install and configure additional SQL Server instances on all nodes of the cluster:

**For SQL Server 2000**
- “Installing SQL Server 2000 on the first node” on page 58
- “Preparing to install SQL Server 2000 on the second node” on page 60
- “Installing SQL Server 2000 on the second node” on page 62
- “Setting the internal name of the clustered instance” on page 63

**For SQL Server 2005**
- “Installing SQL Server 2005 on the first node” on page 66
- “Preparing to install SQL Server 2005 on the second node” on page 69
- “Installing SQL Server 2005 on the second node” on page 70
- “Setting the internal name of the clustered instance” on page 71

Consider the following points as you configure the SQL Server service groups for the additional instances:
- Assign a unique name to the SQL Server service group, for example PAYROLL_SG.
- Pay close attention to the priority order of the systems. For example, if the system priority for the first instance is SYSTEM1 then SYSTEM2; reverse the priority order for the second instance, so that SYSTEM2 has a higher priority.

See “Configuring the SQL service group” on page 75 for instructions.

Create any SQL Server user-defined databases required for your environment. See “Creating a SQL Server user-defined database” on page 82 for instructions.

**Verifying the configuration**

See “Verifying the service group configuration” on page 86 for instructions.
Active-Active configuration

Verifying the configuration
Disaster recovery configuration

This chapter contains the following topics:

- “About disaster recovery configuration” on page 120
- “What is a disaster recovery solution?” on page 120
- “What needs to be protected in a SQL Server environment?” on page 121
- “Typical disaster recovery configuration” on page 122
- “Disaster recovery: New SQL Server 2000 installation” on page 123
- “Creating a parallel environment on the secondary site” on page 126
- “Configuring DR components on the primary and secondary sites” on page 127
- “Disaster recovery: New SQL Server 2005 installation” on page 128
- “Creating a parallel environment on the secondary site” on page 132
- “Installing DR components on the primary and secondary sites” on page 132
- “Configuring DR components” on page 133
- “Configuring replication using Network Appliance SnapMirror” on page 133
- “Configuring SnapMirror resources at the primary site” on page 134
- “Configuring the Global Cluster Option for wide-area failover” on page 135
About disaster recovery configuration

This chapter describes how to set up a disaster recovery solution for SQL Server using the VCS agents for Network Appliance SnapMirror and Microsoft SQL Server.

What is a disaster recovery solution?

A disaster recovery (DR) solution is a series of procedures you can use to safely and efficiently restore application data and services in the event of a catastrophic failure. A typical DR solution requires clusters on primary and secondary sites with replication between those sites. The cluster on the primary site provides data and services during normal operation; the cluster on the secondary site provides data and services if the cluster on the primary site fails. Symantec recommends that you configure the secondary site only after you have established a local cluster with the GCO Option at the primary site.

Why implement a disaster recovery solution?

A DR solution is vital for businesses that rely on the availability of data. A well-designed DR solution prepares a business for unexpected disasters and provides the following benefits in a DR situation:

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

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

Note: A DR solution requires a well-defined backup strategy. Refer to your backup product documentation for information on configuring backup.
Understanding replication

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

In the event that the primary site data center is destroyed, the application data is readily available at the remote site, and the application can be restarted at the remote site. Refer to the NetApp documentation for more information on replication in a NetApp storage environment.

What needs to be protected in a SQL Server environment?

The following components of a SQL server environment must be protected in the event of a disaster:

- **User Databases**: The most critical component in any SQL Server implementation is the user data that is stored in user-defined databases.

- **Logins**: Logins allow clients to connect to SQL Server and execute queries on user data. Logins are stored in the master database and each of the user-defined databases.

- **Jobs**: Jobs are a set of scheduled tasks that maintain SQL Server databases. The job configuration is stored in the msdb system database.

- **Alerts**: Alerts are actions that are taken when a specific event occurs. They are used to respond to and correct errors that occur in SQL Server. The alert configuration is stored in the msdb system database.

- **Operators**: Operators are contacts that address problems occurring in SQL Server. They are notified in the event of errors. The operator configuration is stored in the msdb system database.

- **Extended Stored Procedures**: Extended stored procedures are external routines that are called from within SQL Server. They are typically stored in DLL files on the file system.

- **Other Server Extensions**: SQL Server is a very flexible database engine and it is possible to extend its functionality in several ways. These extensions are also important to the operation of the SQL Server.
Typical disaster recovery configuration

A Disaster Recovery (DR) configuration enables you to restore application data and services in the event of a catastrophic failure. A typical DR solution requires primary and secondary sites, and clusters within those sites. The clusters at the primary and secondary sites are a part of the global cluster. The cluster at the primary site provides data and services during normal operation, and the cluster at the secondary site provides data and services if the primary site fails. VCS continuously monitors and communicates events between clusters. Inter-cluster communication ensures that the global cluster is aware of the state of the global service group at all times.

**Figure 8-1** Typical Disaster Recovery configuration

The illustration displays an environment with a DR solution that is prepared for a disaster. The primary site consists of two nodes, System1 and System2. The secondary site consists of two nodes, System3 and System4. Each site has a clustered setup with the nodes set up appropriately for failover within the site. Filer1 in the cluster on the primary site replicates to Filer2 in the cluster on the secondary site. Replication between the filers is set up using NetApp SnapMirror for SQL. If the Microsoft SQL Server server on System1 fails, SQL Server comes online on node System2 and begins servicing requests. From the user’s perspective there might be a small delay as the backup node comes online, but the interruption in effective service is minimal.

When a failure occurs, such as an earthquake that destroys the data center in which the primary site resides, the DR solution is activated. VCS fails over the entire service group to the cluster at the secondary site. System3 at the secondary site takes over, and the data that was replicated to the secondary site is used to restore the application services to clients.
Disaster recovery: New SQL Server 2000 installation

This section provides information on how to install and configure the high availability and SQL 2000 components on the primary and secondary sites, with the intent of creating a parallel setup for the SQL service group on both sites. The configuration process is the same for both sites.

Reviewing the configuration

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

- SQL virtual server: the IP address should be the same on all nodes
- Cluster IP address for the primary site--used for VCS Cluster Management Console (Single Cluster Mode), also known as Web Console.
- Cluster IP address for the secondary site--used for VCS Cluster Management Console (Single Cluster Mode), also known as Web Console.

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

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 VCS from mistakenly declaring a system down, Symantec recommends disabling the Ethernet autonegotiation options on the private network adapters. Contact the NIC manufacturer for details on this process.
   - Symantec recommends removing TCP/IP from private NICs to lower system overhead.
3. Use independent hubs or switches for each VCS communication network (GAB and LLT). You can use cross-over Ethernet cables for two-node clusters. LLT supports hub-based or switch network paths, or two-system clusters with direct network links.
4. Verify that each system can access the storage devices. Verify that each system recognizes the attached shared disk and that the attached shared disks are visible.
To verify the DNS settings and binding order for Windows Server 2003 systems

1. Open the Control Panel (Start>Control Panel).
2. Double-click Network Connections, or right-click Network Connections and click Open.
3. Ensure the public network adapter is the first bound adapter:
   - 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.
   - Click OK.
4. In the Network and Dial-up Connections window, double-click the adapter for the public network.
   When enabling DNS name resolution, make sure that you use the public network adapters, and not those configured for the VCS private network.
5. In the Public Status dialog box, in the General tab, click Properties.
6. In the Public Properties dialog box, in the General tab:
   - Select the Internet Protocol (TCP/IP) check box.
   - Click Properties.
7. Select the Use the following DNS server addresses option.
8. Verify the correct value for the IP address of the DNS server.
9. Click Advanced.
10. In the DNS tab, make sure the Register this connection’s address in DNS check box is selected.
11. Make sure the correct domain suffix is entered in the DNS suffix for this connection field.
12. Click OK.
Installing VCS and configure the cluster

- Install VCS for Windows
- Select the Global Cluster Option for VCS to enable wide-area failover. Select the option to install Veritas Cluster Server Agent for Microsoft SQL Server. Refer to the Veritas Cluster Server Installation and Upgrade Guide for more information.
- Configure cluster components including the Wide-Area Connector (WAC) resource for global clusters, using the VCS Cluster Configuration Wizard (VCW).
  See “Configuring the cluster” on page 31 for instructions.

Configuring volumes or LUNs on the shared storage

- Create volumes or LUNs required for SQL Server.
- Ensure that the volumes or LUNs (virtual disks) are mounted or connected to the first cluster node.
  See “Managing storage using Network Appliance filer” on page 52.
  See “Managing storage using Windows Logical Disk Manager” on page 55.

Installing and configuring SQL Server 2000 at the primary site

- Install and configure SQL Server 2000
- Configure SQL services
- Stop the SQL services
- Rename shared SQL 2000 files from the virtual disks.
- Install SQL Server 2000 on the additional node.
- Set the internal name of the clustered instance.
  See Chapter 3, “Installing and configuring SQL Server” on page 49.

Configuring the VCS SQL service group

- Create a SQL Server service group using the VCS SQL Server Configuration Wizard.
Creating a parallel environment on the secondary site

After setting up a high availability environment on the primary site, use the following guidelines to complete the same tasks on the secondary site:

Before you begin to configure the secondary site, offline the SQL Server resource, the SQL virtual server name resource, the MSSearch resource (if present), and the SQL virtual IP resource on the primary site.

Caution: Before you begin creating the SQL Server service group for the cluster at the secondary site, make sure that the SQL Server service group at the primary site is offline.

- “Reviewing the configuration” on page 123
- “Configuring the cluster” on page 31
- “Managing storage using Network Appliance filer” on page 52
- “Managing storage using Windows Logical Disk Manager” on page 55

During the creation of virtual disks and volumes for the secondary site, make sure the following is exactly the same as the cluster on the primary site:

- NetApp filer LUNs
- Volume sizes
- Volume names
- Drive letters

- “Installing SQL Server 2000 on the first node” on page 58
  Select the same options at the secondary site as you did at the primary site.

- “Preparing to install SQL Server 2000 on the second node” on page 60
  The instance name must be the same on the primary site and secondary site.
Configuring DR components on the primary and secondary sites

To complete the process of creating a DR solution, proceed to “Configuring DR components” on page 133 after performing the tasks outlined in this chapter.
Disaster recovery: New SQL Server 2005 installation

This section provides information on how to install and configure the high availability and SQL 2005 components on the primary and secondary sites, with the intent of creating a parallel setup for the SQL service group on both sites. The configuration process is the same for both sites.

Perform the following tasks to set up a disaster recovery environment for SQL Server 2005.

Reviewing the configuration

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

- SQL virtual server: the IP address should be the same on all nodes at the primary and secondary sites
- Cluster IP address for the primary site—used for VCS Cluster Management Console (Single Cluster Mode), also known as Web Console.
- Cluster IP address for the secondary site—used for VCS Cluster Management Console (Single Cluster Mode), also known as Web Console.

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

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

To verify the DNS settings and binding order for Windows Server 2003 systems
1 Open the Control Panel (Start>Control Panel).
2 Double-click Network Connections, or right-click Network Connections and click Open.
3 Ensure the public network adapter is the first bound adapter:
   ■ 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.
   ■ Click OK.
4 In the Network and Dial-up Connections window, double-click the adapter for the public network.
When enabling DNS name resolution, make sure that you use the public network adapters, and not those configured for the VCS private network.
5 In the Public Status dialog box, in the General tab, click Properties.
6 In the Public Properties dialog box, in the General tab:
   ■ Select the Internet Protocol (TCP/IP) check box.
   ■ Click Properties.
7 Select the Use the following DNS server addresses option.
8 Verify the correct value for the IP address of the DNS server.
9 Click Advanced.
10 In the DNS tab, make sure the Register this connection’s address in DNS check box is selected.
11 Make sure the correct domain suffix is entered in the DNS suffix for this connection field.
12 Click OK.

Installing VCS and configuring the cluster
Perform the following tasks:
Install VCS. Select the Global Cluster Option for VCS to enable wide-area failover.

Select the option to install Veritas Cluster Server Agent for Microsoft SQL Server
Refer to the Veritas Cluster Server Installation and Upgrade Guide for more information.

Configure cluster components including the Wide-Area Connector (WAC) resource for global clusters, using the VCS Cluster Configuration Wizard (VCW).

See “Configuring the cluster” on page 31 for instructions.

**Configuring volumes or LUNs on the shared storage**

Perform the following tasks:

- Create volumes or LUNs required for SQL Server.
- Ensure that the volumes or LUNs (virtual disks) are connected to the first cluster node.

See “Managing storage using Network Appliance filer” on page 52.
See “Managing storage using Windows Logical Disk Manager” on page 55.

**Installing and configuring SQL Server 2005 at the primary site**

Perform the following tasks:

- Create volumes or virtual disks and ensure that they are mounted or connected to the first cluster node
- Install and configure SQL Server 2005
- Configure SQL services
- Stop the SQL services
- Rename shared SQL 2005 files from the virtual disks
- Install SQL Server 2005 on the additional node
- Set the internal name of the clustered instance

See Chapter 3, “Installing and configuring SQL Server” on page 49.
Configuring the VCS SQL service group

Perform the following tasks:

- Create a SQL Server service group using the VCS SQL Server Configuration Wizard
- If required, create volumes for a user-defined database and transaction log
- If required, create a new user-defined database in SQL Server
- If required, add VCS storage agent resources for a user-defined database in VCS
- Verify the configuration

See "Configuring the SQL service group" on page 75 for instructions.
Creating a parallel environment on the secondary site

After setting up a high availability environment on the primary site, use the following guidelines to complete the same tasks on the secondary site:

**Caution:** Before you begin to configure the secondary site, offline the SQL Server resource, the SQL virtual server name resource, the MSSearch resource (if present), and the SQL virtual IP resource on the primary site. Before you begin creating the SQL Server service group for the cluster at the secondary site, make sure that the SQL Server service group at the primary site is offline.

- “Reviewing the configuration” on page 128
- “Configuring the cluster” on page 31
- “Managing storage using Network Appliance filer” on page 52
  “Managing storage using Windows Logical Disk Manager” on page 55
During the creation of volumes or LUNs (virtual disks) for the secondary site, make sure the following is exactly the same as the cluster on the primary site:
- Volume sizes
- Volume names
- Drive letters

- “Installing SQL Server 2005 on the first node” on page 66
  Select the same options at the secondary site as you did at the primary site.

- “Preparing to install SQL Server 2005 on the second node” on page 69
  The instance name must be the same on the primary site and secondary site.

- “Installing SQL Server 2005 on the second node” on page 70
- “Configuring the SQL service group” on page 75
  The service group name and virtual computer name must be the same on both the primary site and secondary site.

Installing DR components on the primary and secondary sites

To complete the process of creating a DR solution, proceed to “Configuring DR components” on page 133 after performing the tasks outlined in this chapter.
Disaster recovery configuration

Configuring DR components

After configuring the high availability and SQL components on the primary and secondary sites, complete the disaster recovery solution by configuring the disaster recovery components for both sites.

Perform the following tasks:

- Set up volume replication using Network Appliance SnapMirror.
  See “Configuring replication using Network Appliance SnapMirror” on page 133.

- Configuring SnapMirror resources in the SQL service group at the primary site.
  See “Configuring SnapMirror resources at the primary site” on page 134.

- Configure GCO option for wide-area failover.
  See “Configuring the Global Cluster Option for wide-area failover” on page 135.

Configuring replication using Network Appliance SnapMirror

You can replicate SQL Server data by establishing a SnapMirror relationship between the filers at the primary and secondary sites. Before configuring replication, make sure the service group is offline at the secondary site.

SnapMirror replicates snapshots taken on a filer and applies them to a remote filer over a wide area network; these snapshots can be used by the target host to provide rapid failover in case of a disaster.

If required, you can transfer the initial base snapshot image from the primary to secondary via tape, and then set up incremental SnapMirror updates to the destination filer. After you set up a SnapMirror relationship, ensure that the state of the volumes (that are to be replicated) at the primary site shows as SnapMirrored.

Refer to Network Appliance documentation for more information.
Configuring SnapMirror resources at the primary site

Configure NetAppSnapMirror resources at the primary site to monitor data replication from the primary to the secondary site. Creating a resource at the primary site will enable the filer to replicate from the primary to the secondary site.

You may want to repeat this procedure and create a NetAppSnapMirror resource at the secondary site. This is required in cases where:

- the service group is online at the secondary site (either it is failed over or switched to the secondary site) and the filer should replicate from secondary to primary site
- if you want to fail over or switch the service group from the secondary to the primary site

The following steps describe how to add the resources using the SQL Server Configuration Wizard.

Verify that the LUNs created to store the registry replication information and the SQL Server database are connected to the node on which you run the wizard, and disconnected from other nodes in the cluster.

To configure SnapMirror resource using the SQL Server Configuration Wizard

1. Start the SQL Server Configuration Wizard. Click Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > SQL Server Configuration Wizard.
   If you are running this procedure on the secondary site, ensure that the service group is online up to the snapdrive resources.

2. In the Select Configuration Option panel, click MS SQL Server Service Group Configuration, click Edit, and then click Next.

3. Review the prerequisites and then click Next.

4. In the Service Group Selection panel, select the service group to modify and click Next.

5. In the Service Group Configuration panel, verify the list of systems in the service group and click Next.

6. On the SQL Server Instance Selection panel, check Configure the NetApp SnapMirror resource(s) and click Next.
   An informational message appears if you chose to configure a SnapMirror resource without configuring replication between Network Appliance filers
Disaster recovery configuration

Configuring the Global Cluster Option for wide-area failover

at primary and secondary sites. Review the message and click Yes to continue.

7 Accept default values in the subsequent wizard panels and click Next till you
reach the wizard completion panel.

8 On the Configuration Status panel, do not check the Bring the service group
online check box. Click Finish.

Configuring the Global Cluster Option for wide-area failover

The Global Cluster option is required to manage global clustering for wide-area disaster recovery. Creating a global cluster environment involves:

- Connecting standalone clusters by adding a remote cluster to a local cluster.
- Converting the local service group that is common to all the clusters to a
  global service group.

You need to create a wide-area connector resource for global clusters. You can use the VCS Java Console or Web Console to perform global cluster operations; this guide only provides procedures for the Java Console. Refer to the Veritas Cluster Server Administrator’s Guide for more information on GCO operations available from the Java and Web consoles.

Prerequisites

Creating a global cluster environment requires:

- Wide-area Connector process is configured and the ClusterService group is
  online at both sites. See “Configuring Wide-Area Connector process for global clusters” on page 47 for instructions.
- All service groups properly configured and able to come online.
- The service group serving as the global group has the same unique name
  across all applicable clusters.
- The clusters use the same version of VCS.
- The clusters use the same operating system.
- The clusters are standalone and do not already belong to a global cluster environment.
The names of the clusters at the primary and secondary sites and the virtual IP addresses associated with them are registered in the DNS with reverse lookup.

Linking clusters: Adding a remote cluster to a local cluster

The VCS Java Console provides a wizard to create global clusters by linking standalone clusters or bringing a standalone cluster into an existing global environment.

- If you are creating a global cluster environment for the first time with two standalone clusters, run the wizard from either the cluster on the primary site or the cluster on the secondary site.
- If you are adding a standalone cluster to an existing global cluster environment, run the wizard from a cluster already in the global cluster environment.

The following information is required for the Remote Cluster Configuration Wizard in Cluster Explorer:

- The active host name or IP address of each cluster in the global configuration and of the cluster being added to the configuration.
- The user name and password of the administrator for each cluster in the configuration.
- The user name and password of the administrator for the cluster being added to the configuration.

Note: Symantec does not support adding a cluster that is already part of a global cluster environment. To merge the clusters of one global cluster environment (for example, cluster A and cluster B) with the clusters of another global environment (for example, cluster C and cluster D), separate cluster C and cluster D into standalone clusters and add them one by one to the environment containing cluster A and cluster B.

To add a remote cluster in Cluster Explorer

1. From Cluster Explorer, click Add/Delete Remote Cluster on the Edit menu.  
   or
   From the Cluster Explorer configuration tree, right-click the cluster name, and click Add/Delete Remote Cluster.

2. Review the required information for the Remote Cluster Configuration Wizard and click Next.

3. In the Wizard Options panel, click Add Cluster, then click Next.
4 In the New Cluster Details panel, enter the details of the new cluster as follows:
  If the cluster is not running in secure mode:
  ■ Enter the host name of a cluster system, an IP address of a cluster system, or the IP address of the cluster that will join the global environment.
  ■ If necessary, change the default port number.
  ■ Enter the user name.
  ■ Enter the password.
  ■ Click Next.
  If the cluster is running in secure mode:
  ■ Enter the host name of a cluster system, an IP address of a cluster system, or the IP address of the cluster that will join the global environment.
  ■ Verify the port number.
  ■ Choose to connect to the remote cluster with the credentials used for the current cluster connection, or enter new credentials, including the user name, password, and the domain.
  ■ If you connected to the remote cluster earlier through the wizard, you can use the credentials from the previous connection.
  ■ Click Next.
5 Click Finish. After running the wizard, the configurations on all the relevant clusters are in read-write mode; the wizard does not close the configurations.
6 Verify that the heartbeat connection between clusters is alive. From the command window enter hahb -display. The state attribute in the output should show alive. If the state is unknown, then offline and online the ClusterService group.

Converting a local service group to a global service group

After linking the clusters, use the Global Group Configuration wizard to convert a local service group that is common to the global clusters to a global group. This wizard also enables you to convert global groups into local groups.

To convert a local service group to a global group

1 From Cluster Explorer, click Configure Global Groups on the Edit menu. or
From the Cluster Explorer configuration tree, right-click the cluster, and click **Configure Global Groups**.

or

From the Cluster Explorer configuration tree, right-click the service group, click **Configure As Global**, and proceed to step 3b.

2 Review the information required for the Global Group Configuration wizard and click **Next**.

3 Enter the details of the service group to modify:
   - Click the name of the service group that will be converted from a local group to a global group, or vice versa.
   - From the **Available Clusters** box, click the clusters on which the group can come online. Click the right arrow to move the cluster name to the **Clusters for Service Group** box; for global to local cluster conversion, click the left arrow to move the cluster name back to the **Available Clusters** box. A priority number (starting with 0) indicates the cluster on which the group will attempt to come online. If necessary, double-click the entry in the **Priority** column and enter the new value.
   - Select the policy for cluster failover as follows:
     - **Manual** Prevents a group from automatically failing over to another cluster.
     - **Auto** Enables a group to automatically fail over to another cluster if it is unable to fail over within the cluster, or if the entire cluster fails.
     - **Connected** Enables a group to automatically fail over to another cluster if it is unable to fail over within the cluster.
   - Click **Next**.

4 Enter or review the connection details for each cluster. Click the **Configure** icon to review the remote cluster information for each cluster:

- **Cluster not in secure mode**
  - Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
  - Verify the port number.
  - Enter the user name.
  - Enter the password.
  - Click **OK**.
  - Repeat these steps for each cluster in the global environment.
Disaster recovery configuration
Configuring the Global Cluster Option for wide-area failover

Cluster in secure mode
- Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
- Verify the port number.
- Choose to connect to the remote cluster with the credentials used for the current cluster connection, or enter new credentials, including the user name, password, and domain.
- If you connected to the remote cluster earlier through the wizard, you can use the credentials from the previous connection.
- Click OK.
- Repeat these steps for each cluster in the global environment.

5 Click Next, then click Finish.
At this point, you must bring the global service group online from Cluster Explorer.

Bringing a global service group online
After converting the local service group that is common to the global clusters to a global group, use the Cluster Explorer to bring the global service group online.

To bring a remote global service group online from Cluster Explorer
1 In the Service Groups tab of the configuration tree, right-click the service group.
   or
   Click a cluster in the configuration tree, click the Service Groups tab, and right-click the service group icon in the view panel.
2 Click Online, and click Remote online.
3 In the Online global group dialog box:
   - Click the remote cluster to bring the group online.
   - Click the specific system, or click Any System, to bring the group online.
   - Click OK.
Administering global service groups

Administering global groups requires the following conditions:

■ A group that will serve as the global group must have the same name across all applicable clusters.

■ You must know the user name and password for the administrator to each cluster in the configuration.

Use the VCS Java Console or Web Console to bring a global group online, take a global group offline, or switch a global group on a remote cluster. The section below provides additional procedures for administering global groups from the Java Console. Refer to the Veritas Cluster Server Administrator’s Guide for more information on global cluster operations from the Java Console and Web Console.

Note: For remote cluster operations, the user must have the same name and privilege as the user logged on to the local cluster.

Taking a remote global service group offline

Use Cluster Explorer to take a remote global service group offline.

To take a remote global service group offline from Cluster Explorer

1 In the Service Groups tab of the configuration tree, right-click the service group.

   or

   Click a cluster in the configuration tree, click the Service Groups tab, and right-click the service group icon in the view panel.

2 Click Offline, and click Remote offline.

3 In the Offline global group dialog box:

   ■ Click the remote cluster to take the group offline.

   ■ Click the specific system, or click All Systems, to take the group offline.

   ■ Click OK.

Switching a remote service group

Use Cluster Explorer to switch a remote service group.

To switch a remote service group from Cluster Explorer

1 In the Service Groups tab of the configuration tree, right-click the service group.
Disaster recovery configuration
Configuring the Global Cluster Option for wide-area failover

or
Click a cluster in the configuration tree, click the Service Groups tab, and right-click the service group icon in the view panel.

2 Click Switch To, and click Remote switch.

3 In the Switch global group dialog box:
   ■ Click the cluster to switch the group.
   ■ Click the specific system, or click Any System, to take the group offline.
   ■ Click OK.

Deleting a remote cluster
If necessary, use the Remote Cluster Configuration wizard to delete a remote cluster. This operation involves the following tasks:

■ Taking the wide area cluster (wac) resource in the ClusterService group offline on the cluster that will be removed from the global environment. For example, to delete cluster C2 from a global environment containing C1 and C2, log on to C2 and take the wac resource offline.

■ Removing the name of the specified cluster (C2) from the cluster lists of the other global groups using the Global Group Configuration wizard. Note that the Remote Cluster Configuration wizard in Cluster Explorer automatically updates the cluster lists for heartbeats. Log on to the local cluster (C1) to complete this task before using the Global Group Configuration wizard.

■ Deleting the cluster (C2) from the local cluster (C1) through the Remote Cluster Configuration wizard.

Note: You cannot delete a remote cluster if the cluster is part of a cluster list for global service groups or global heartbeats, or if the cluster is in the RUNNING, BUILD, INQUIRY, EXITING, or TRANSITIONING states.

Use Cluster Explorer to take the wide area cluster resource offline, remove a cluster from the cluster list for a global group, and delete a remote cluster from the local cluster.

To take the wide area cluster (wac) resource offline
1 From Cluster Monitor, log on to the cluster that will be deleted from the global cluster environment.

2 In the Service Groups tab of the Cluster Explorer configuration tree, right-click the wac resource under the Application type in the ClusterService group.
or

Click a service group in the configuration tree, click the **Resources** tab, and right-click the **wac** resource in the view panel.

3. Click **Offline**, and click the appropriate system from the menu.

### To remove a cluster from a cluster list for a global group

1. From Cluster Explorer, click **Configure Global Groups** on the **Edit** menu.

2. Click **Next**.

3. Enter the details of the service group to modify:
   - Click the name of the service group.
   - For global to local cluster conversion, click the left arrow to move the cluster name from the cluster list back to the **Available Clusters** box.
   - Click **Next**.

4. Enter or review the connection details for each cluster. Click the **Configure** icon to review the remote cluster information for each cluster:
   - If the cluster is not running in secure mode:
     - Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
     - Verify the port number.
     - Enter the user name.
     - Enter the password.
     - Click **OK**.
   - If the cluster is running in secure mode:
     - Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
     - Verify the port number.
     - Choose to connect to the remote cluster using the connected cluster’s credentials, or enter new credentials, including the user name, password, and domain.
     - Click **OK**.

5. Click **Next**.

6. Click **Finish**.

### To delete a remote cluster from the local cluster

1. From Cluster Explorer, click **Add/Delete Remote Cluster** on the **Edit** menu.

   or
From the Cluster Explorer configuration tree, right-click the cluster name, and click **Add/Delete Remote Clusters**.

2. Review the required information for the **Remote Cluster Configuration** wizard and click **Next**.

3. On the **Wizard Options** panel, click **Delete Cluster**, then click **Next**.

4. In the **Delete Cluster panel**, click the name of the remote cluster to delete, then click **Next**.
5 Review the connection details for each cluster. Click the **Configure** icon to review the remote cluster information for each cluster:

![Global Cluster Configuration Wizard](image)

If the cluster is not running in secure mode:

- Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
- Verify the port number.
- Enter the user name.
- Enter the password.
- Click **OK**.

If the cluster is running in secure mode:

- Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
- Verify the port number.
- Choose to connect to the remote cluster with the credentials used for the current cluster connection, or enter new credentials, including the user name, password, and the domain.
  
  If you connected to the remote cluster earlier through the wizard, you can use the credentials from the previous connection.
- Click **OK**.

6 Click **Finish**.
Removing VCS

This chapter contains the following topics:

■ “About removing VCS” on page 146
■ “Prerequisites” on page 146
■ “Removing the VCS configuration” on page 146
■ “Uninstalling the agents” on page 146
■ “License management” on page 147
About removing VCS

This chapter describes steps to remove VCS.

Prerequisites

- You must have administrative access to all systems selected for cluster operations. For this, add the domain user to the local Administrators group of each system.
- You must be a domain user.
- You must be a member of the Local Administrators group for all nodes where you are installing.

Removing the VCS configuration

Before you remove the VCS, use the VCS Cluster Configuration Wizard (VCW) to delete the VCS configuration from all nodes.
For instructions, see the chapter on Modifying the Cluster Configuration in the Veritas Cluster Server Administrator’s Guide.

Uninstalling the agents

This section describes steps for uninstalling VCS.

Prerequisites

- Verify that you have local administrative privileges on the node where you are uninstalling the agent.
- Verify that all SQL service groups are offline on all nodes in the cluster.

Instructions

Follow these steps to remove VCS from the cluster nodes.

To remove VCS

1  In the Add/Remove Programs applet, click VCS 5.1 for Windows (Server Components) and click Remove.
2  Review the Welcome page and click Next.
3  Select the check box if you want to remove the client components and click Next.

4  Specify the nodes from which you want to remove the agents.
   ■ Select the node. This may take some time depending on the size of the domain and network conditions.
   ■ Click Add. To remove a node, highlight the node in the computer list and click Remove.
   ■ Click Next.

5  The installer validates the system for uninstallation. After the node is accepted, click Next.
   If a node is rejected, the Comments column displays the cause for rejecting the node. Highlight the node to view a detailed information about the failure in the Details box. Resolve the error, highlight the node in the selected systems list, and click Validate Again. Once all the nodes are accepted, click Next.

6  Review the summary of your selections and click Uninstall.

7  The installer displays the status of uninstallation.

8  After the uninstallation is complete, review the report and click Next.

9  Click Finish.
   After uninstallation you may be required to reboot the system. After rebooting the system, the SnapDrive service may fail to start with a logon failure. In such cases, reset the password for the SnapDrive service account and then start the service.

License management

The product installer also allows you to add or remove license keys for options in your installation of VCS components.

To add or remove license keys

1  Open the Windows Control Panel and click Add or Remove Programs.

2  Select Veritas Cluster Server 5.1 for Windows (Server Components) and click Change.

3  The Symantec Product Installer screen appears. Select License Management. Click Next.

4  The license key screen appears. Enter the license key you want to add and click Update. If you want to remove a license key, select the license key in the Licenses field and click Remove.
Troubleshooting the agents

This chapter contains the following topics:

- “About troubleshooting VCS agents” on page 150
- “VCS logging” on page 150
- “Network Appliance agents error messages” on page 153
- “Error messages and descriptions” on page 155
About troubleshooting VCS agents

This chapter describes how to troubleshoot common problems in the VCS agents for Network Appliance and Microsoft SQL Server. The chapter lists the error messages, and describes the problem associated with the agent. Recommended solution is included, where applicable.

VCS logging

VCS generates two error message logs: the engine logs and the agent logs. Log file names are appended by letters. Letter A indicates the first log file, B the second, C the third, and so on.

The agent log is located at %VCS_HOME%\log\agent_A.txt. The format of agent log messages is:

Timestamp (Year/MM/DD) | Mnemonic | Severity | UMI | Agent Type | Resource Name | Entry Point | Message Text

The agent log message components are defined as follows:

- Timestamp denotes the date and time when the message was logged.
- Mnemonic denotes which Veritas product logs the message. For VCS enterprise agent for Microsoft SQL, mnemonic is ‘VCS’.
- Severity denotes the seriousness of the message. Severity of the VCS error messages is classified into the following types:
  - CRITICAL indicates a critical error within a VCS process. Contact Technical Support immediately.
  - ERROR indicates failure of a cluster component, unanticipated state change, or termination or unsuccessful completion of a VCS action.
  - WARNING indicates a warning or error, but not an actual fault.
  - NOTE informs that VCS has initiated an action.
  - INFO informs about various state messages or comments. Of these, CRITICAL, ERROR, and WARNING indicate actual errors. NOTE and INFO provide additional information.
- UMI or Unique Message ID is a combination of Originator ID, Category ID, and Message ID. For example, the UMI for a message generated by the SQLServer agent would resemble: V-16-20020-13
  - Originator ID for all VCS products is ‘V-16.’ Category ID for SQLServer agent is 20020, for MSDTC is 20021, and that for MSSearch agent is 20022.
  - Message ID is a unique number assigned to the message text.
- Message text denotes the actual message string.
You can view these message logs using Notepad or any text editor. All messages are logged to the engine and the agent logs. Messages of type CRITICAL and ERROR are also written to the Windows event log.

A typical agent log resembles:

```
2004/01/12 11:22:47 VCS NOTICE V-16-20020-10
Instance name is not specified. Agent will operate on default instance.
```

**VCS Cluster Configuration Wizard logs**

The VCS Cluster Configuration Wizard (VCW) log is located at %allusersprofile%\Application Data\Veritas\Cluster Server\vcw.log.

Here, %allusersprofile% is the file system directory containing application data for all users. A typical path is C:\Documents and Settings\All Users\.

The format of the wizard log is

```
ThreadId | Message Text
```

- **ThreadId**: the ID of the thread initiated by the wizard.
- **Message Text**: the actual message generated by the wizard.

A typical wizard log resembles:

```
00000576-00000264: ExecMethod return 00000000.
00000576-00000110: CRegistry::Query for VCS License failed. Error=0x00000000
00000576-00000264: ExecMethod return 00000000.
00000576-00000264: ExecMethod return 00000001.
00000576-00000127: QueryDWORDValue returned 0x00000001
00000576-00000132: CRegistry::Query for VxSS Root information failed. Error=0x00000001
```

**VCWsilent logs**

The VCWsilent log is located at <currentdirectory>\vcwsilent.log.

Here, <currentdirectory> is the directory from where the VCWsilent.exe is run.

A typical VCWsilent log resembles:

```
000005540-00000064: 5540: STARTING - Discovering NICs on the selected machines...
000009956-00000064: 9956: STARTING - Generating private network related files...
000009956-00000048: 9956: COMPLETED - Generating LLT host files...
```
00009956-00000048: 9956: COMPLETED - Generating GAB tab files...
00009956-00000048: 9956: COMPLETED - Generating main.cf file...
00009956-00000064: 9956: STARTING - Configuring LLT on all the nodes.
00009956-00000048: 9956: COMPLETED - Configuring LLT on all the nodes.
## Network Appliance agents error messages

This section describes the error messages for the NetApp agents.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to open connection to filer %s.</td>
<td>Make sure that the VCS Helper service account is part of the administrator's group on the local host and the filer. Make sure the private network is functioning properly. Verify you can ping the IP used for the private storage network. This is the IP defined the StorageIP attribute of the NetAppFiler resource.</td>
</tr>
<tr>
<td>Failed to initialize ONTAPI on system</td>
<td>The agent could not find the file NTAPADMIN.DLL on the system. Verify the file exists in the %VCS_HOME%\bin directory.</td>
</tr>
<tr>
<td>Invalid attributes exist in the configuration</td>
<td>Some agent attributes have not been defined or have been defined incorrectly. Verify the configuration definition for the agent.</td>
</tr>
<tr>
<td>ONTAP API called failed for object_name on filer_name.</td>
<td>The specified API failed on the specified object. See the NetApp ONTAP API documentation for information about the associated error message.</td>
</tr>
<tr>
<td>Volume %s on filer %s is not a SnapMirror replicated volume</td>
<td>Verify replication is set up on the specified volume.</td>
</tr>
<tr>
<td>Multiple snapmirror destinations for a volume is not supported by this agent. 'snapmirror status' for volume %s on filer %s returned multiple status entries. Administrative intervention required</td>
<td>There should be only one destination per source volume.</td>
</tr>
<tr>
<td>Initialize VLibNetAppHost::Initialize() failed. (error_type: %s, error_code: 0x%s)</td>
<td>The agent could not detect the iSCSI or FC Initiator on the host. Make sure that you have installed and configured Microsoft iSCSI Initiator or an FC Initiator on each node.</td>
</tr>
</tbody>
</table>
Failed to connect/disconnect virtual disk. (error_type: %s, error_code: 0x%s, error_message: %s)

This could occur because one or more of the following parameters are defined incorrectly in the VCS configuration:
- Filer name
- Volume name/LUN name
- Share name
- Storage IP

Verify the configuration definition of the resource. Make sure each attribute is defined correctly.

Unable to create/delete online lock file %s. Error code %s.

Make sure you have write permissions on the specified directory.
# Error messages and descriptions

The following table lists the messages of type ERROR and WARNING. Each message includes a description and a recommended solution, if applicable.

## Agent for SQL Server 2000

This section describes the error messages for the SQL Server 2000 agent.

### Table 10-2  SQL Server 2000 agents error messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid value specified for attribute <code>attribute name</code>.</td>
<td>No value provided for the specified attribute. Solution: Provide a value for the attribute.</td>
</tr>
<tr>
<td>Failed to lookup the account name 'account name'. <code>Error = Error code.</code></td>
<td>Invalid user information specified for detail monitoring. Solution: Provide the correct user information</td>
</tr>
<tr>
<td>Failed to open the SCM handle. <code>Error = Error code.</code></td>
<td>The agent fails to get a handle to the Service Control Manager (SCM). This could occur if the specified SCM database does not exist or the requested access is denied. Solution: Verify that SCM can be run on the host. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service 'service name' is not in stopped state.</td>
<td>The service is in an invalid state. Solution: Check the state of the service.</td>
</tr>
<tr>
<td>Failed to start the service 'service name'. <code>Error = Error code.</code></td>
<td>The agent failed to start the service. Solution: See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>SQL Server Instance name is not specified. Agent will operate on the default instance.</td>
<td>No value spaced-out for SQL Server instance name. Agent would operate on the default SQL Server instance.</td>
</tr>
<tr>
<td>The service 'service name' did not start within the specified time limit.</td>
<td>The agent failed to start the service within the time limit as specified in the SQLOnlineTimeout attribute.</td>
</tr>
<tr>
<td>The 'service name' service is not in stopped or running state. <code>State=state name</code>.</td>
<td>The service is in an invalid state.</td>
</tr>
</tbody>
</table>
### Table 10-2  SQL Server 2000 agents error messages (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The 'service name' service is in state name state, while the 'service name' service is in state name state.</td>
<td>The SQL Server and the SQL agent service are not in the same state. Both the services must be in ONLINE state to bring the service group online.</td>
</tr>
<tr>
<td>Failed to get the password attribute.  Error = Error code.</td>
<td>Incorrect encrypted password specified for detail monitoring.</td>
</tr>
<tr>
<td></td>
<td>Solution: Provide a password that is encrypted using the ‘VCSencrypt’ utility.</td>
</tr>
<tr>
<td>Failed to open the service ‘service name’.  Error = Error code.</td>
<td>The agent failed to open the service from the Service Control Manager.</td>
</tr>
<tr>
<td></td>
<td>Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
<tr>
<td>The service ‘service name’ is not in running state. Attempt to stop it might be unsuccessful.</td>
<td>The SQL Server service could be in PAUSE, PAUSE PENDING, or START PENDING state.</td>
</tr>
<tr>
<td></td>
<td>Solution: Resume the service and then attempt to stop it.</td>
</tr>
<tr>
<td>The service ‘service name’ did not stop.  Error = Error code.</td>
<td>The agent failed to stop the service. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service ‘service name’ did not stop within the specified timeout.  Error = Error code.</td>
<td>The agent failed to stop the service within the time limit as specified in the SQLOfflineTimeout attribute.</td>
</tr>
<tr>
<td>Sql script has failed with error error code.</td>
<td>The SQL script for detail monitoring failed. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>Could not find the database path for instance instance name. Please correct the instance name specified.</td>
<td>The instance name specified for the SQL Server instance is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Solution: Specify the correct SQL Server instance name.</td>
</tr>
<tr>
<td>Mount specified does not contain the database for instance instance name. Please correct the mount path.</td>
<td>The specified mount does not contain the data pertaining to a given instance name.</td>
</tr>
<tr>
<td></td>
<td>Solution: Specify the correct mount path.</td>
</tr>
<tr>
<td>The password attribute has not been configured.</td>
<td>The password attribute used for detail monitoring is not configured.</td>
</tr>
</tbody>
</table>
Troubleshooting the agents

Error messages and descriptions

Agent for MSSearch

This section describes the error messages for the MSSearch agent.

### Table 10-3  MSSearch agent error messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The AppName attribute has not been configured.</td>
<td>No value specified for the AppName attribute.</td>
</tr>
<tr>
<td></td>
<td>Solution: Specify a valid value for the AppName attribute.</td>
</tr>
<tr>
<td>Failed to instantiate the Microsoft Search COM object. Error = Error code.</td>
<td>MSSearch is not installed. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>Failed to open the Microsoft Search service. Error = Error code.</td>
<td>The agent failed to open the MSSearch service from the Service Control Manager (SCM).</td>
</tr>
<tr>
<td></td>
<td>Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
</tbody>
</table>
This section describes the error messages for the MSDTC agent.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lanman attribute has not been configured.</td>
<td>No value specified for the LanmanResName attribute. Solution: Specify a valid value for the LanmanResName attribute.</td>
</tr>
<tr>
<td>MountResName attribute has not been configured.</td>
<td>No value specified for MountResName attribute. Solution: Specify a valid value for the MountResName attribute.</td>
</tr>
<tr>
<td>LogPath attribute has not been configured.</td>
<td>No value specified for LogPath attribute. Solution: Specify a valid value for the MountResName attribute.</td>
</tr>
<tr>
<td>Failed to open the SCM handle. Error = Error code.</td>
<td>The agent fails to get a handle to the Service Control Manager (SCM). This could occur if the specified SCM database does not exist or the requested access is denied. Solution: Verify that SCM can be run on the host. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>Failed to open the MSDTC service. Error = Error code.</td>
<td>The agent failed to open the MSDTC service from the Service Control Manager (SCM). Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
<tr>
<td>Failed to start the MSDTC service. Error = Error code.</td>
<td>The agent failed to start the MSDTC service. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The MSDTC log path is 'path name'. Configured one is 'path name'.</td>
<td>The specified path for the MSDTC logs is different from the actual path. Solution: Specify the correct MSDTC log path.</td>
</tr>
<tr>
<td>The MSDTC service is not in running state. Offline might be unsuccessful.</td>
<td>The MSDTC service could be in PAUSE, PAUSE PENDING, or START PENDING state. Solution: Resume the service and then attempt to stop it.</td>
</tr>
</tbody>
</table>
Troubleshooting the agents
Error messages and descriptions

Table 10-4 MSDTC agent error messages (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to stop the MSDTC service. Error = Error code.</td>
<td>The MSDTC service could not be stopped. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>Failed to wait for the MSDTC service to stop. Error = Error code.</td>
<td>The agent could not stop the service within the specified time limit of 20 seconds. See the associated Windows error code for more information.</td>
</tr>
</tbody>
</table>

Agent for SQL Server 2005
This section describes the error messages for the SQL Server 2005 agent.

Table 10-5 SQL Server 2005 agents error messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to convert the argument list. Error = Error code.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Invalid value specified for attribute attribute name.</td>
<td>No value provided for the specified attribute. Solution: Provide a value for the attribute.</td>
</tr>
<tr>
<td>Failed to open the SCM handle. Error = Error code.</td>
<td>The agent fails to get a handle to the Service Control Manager (SCM). This could occur if the specified SCM database does not exist or the requested access is denied. Solution: Verify that SCM can be run on the host. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service service name is not in stopped state.</td>
<td>The service is in an invalid state. Solution: Check the state of the service.</td>
</tr>
<tr>
<td>Failed to start the service service name. Error = Error code.</td>
<td>The agent failed to start the service. Solution: See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>SQL Server Instance name is not specified. Agent will operate on the default instance.</td>
<td>No value spaced-out for SQL Server instance name. Agent would operate on the default SQL Server instance.</td>
</tr>
</tbody>
</table>
Table 10-5  SQL Server 2005 agents error messages (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to set the virtual computer name in the environment of the service name. Error = Error code.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>The service service name did not start within the specified time limit.</td>
<td>The agent failed to start the service within the time limit as specified in the SQLOnlineTimeout attribute.</td>
</tr>
<tr>
<td>Failed to wait for the service service name to start. Error = Error code.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>The service name service is not in stopped or running state. State=state name.</td>
<td>The service is in an invalid state.</td>
</tr>
<tr>
<td>Failed to get the password attribute. Error = Error code.</td>
<td>Incorrect encrypted password specified for detail monitoring. Solution: Provide a password that is encrypted using the ‘VCSencrypt’ utility.</td>
</tr>
<tr>
<td>Failed to convert the password attribute. Error = Error code.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Failed to open the service service name. Error = Error code.</td>
<td>The agent failed to open the service from the Service Control Manager. Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
<tr>
<td>Failed to query the status of the service service name. Error = Error code.</td>
<td>The agent failed to query the state of the service. Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
<tr>
<td>The service service name is not in running state. Attempt to stop it might be unsuccessful.</td>
<td>The SQL Server service could be in PAUSE, PAUSE PENDING, or START PENDING state. Solution: Resume the service and then attempt to stop it.</td>
</tr>
<tr>
<td>The service service name did not stop. Error = Error code.</td>
<td>The agent failed to stop the service. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service service name did not stop within the specified timeout. Error = Error code.</td>
<td>The agent failed to stop the service within the time limit as specified in the SQLOfflineTimeout attribute.</td>
</tr>
</tbody>
</table>

Table 10-5  SQL Server 2005 agents error messages (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sql script has failed with error <em>error code</em>.</td>
<td>The SQL script for detail monitoring failed. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>Error occurred while getting the process exit code. <em>Error = Error code.</em></td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>WaitForSingleObject failed with error <em>error code</em>.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>The password attribute has not been configured.</td>
<td>The password attribute used for detail monitoring is not configured.</td>
</tr>
<tr>
<td>Failed to start the Sql script. <em>User = user name, Domain = domain name, Error = Error code.</em></td>
<td>The agent failed to execute the script for detail monitoring. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>Unable to convert the buffer to UNICODE. <em>Error = Error code</em></td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Sql script failed. Script output: <em>output</em></td>
<td>The SQL script failed to monitor the SQL Server instance. See the script output for more information.</td>
</tr>
<tr>
<td>Failed to get the temporary file path. <em>Error : Error code</em></td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Failed to create the temporary file. <em>Error = Error code.</em></td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Failed read the temporary file. <em>Error = Error code.</em></td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Failed to remove the virtual name environment for the service <em>service name.</em></td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
</tbody>
</table>
Agent for SQL Server 2005 Agent service

This section describes the error messages for the SQL Server 2005 Agent service agent.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to convert the argument list. Error = Error code.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Invalid value specified for attribute attribute name.</td>
<td>No value provided for the specified attribute. Solution: Provide a value for the attribute.</td>
</tr>
<tr>
<td>Failed to initialize the SQLAgService2005 agent.</td>
<td>The agent failed to initialize the SQLAgService2005 agent for the SQL Server 2005 Agent Service. Solution: Verify whether the SQLAgService2005 agent exists.</td>
</tr>
<tr>
<td>Failed to open the SCM handle. Error = Error code.</td>
<td>The agent fails to get a handle to the Service Control Manager (SCM). This could occur if the specified SCM database does not exist or the requested access is denied. Solution: Verify that SCM can be run on the host. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service service name is not in stopped state.</td>
<td>The service is in an invalid state. Solution: Check the state of the service.</td>
</tr>
<tr>
<td>Failed to start the service service name. Error = Error code.</td>
<td>The agent failed to start the service. Solution: See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>SQL Server Instance name is not specified. Agent will operate on the default instance.</td>
<td>No value spaced-out for SQL Server instance name. Agent would operate on the default SQL Server instance.</td>
</tr>
<tr>
<td>Failed to set the virtual computer name in the environment of the service service name. Error = Error code.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>The service service name did not start within the specified time limit.</td>
<td>The agent failed to start the service within the time limit as specified in the SQLOnlineTimeout attribute.</td>
</tr>
</tbody>
</table>
Failed to wait for the service `service name` to start. Error = `Error code`. This is a VCS internal error. Solution: Contact Symantec Technical Support.

The `service name` service is not in stopped or running state. State = `state name`. The service is in an invalid state.

Failed to open the service `service name`. Error = `Error code`. The agent failed to open the service from the Service Control Manager. Solution: Check whether the service is present in the Service Control Manager.

Failed to query the status of the service `service name`. Error = `Error code`. The agent failed to query the state of the service. Solution: Check whether the service is present in the Service Control Manager.

The service `service name` is not in running state. Attempt to stop it might be unsuccessful. The SQL Server service could be in `PAUSE`, `PAUSE PENDING`, or `START PENDING` state. Solution: Resume the service and then attempt to stop it.

The service `service name` did not stop. Error = `Error code`. The agent failed to stop the service. See the associated Windows error code for more information.

The service `service name` did not stop within the specified timeout. Error = `Error code`. The agent failed to stop the service within the time limit as specified in the SQLOfflineTimeout attribute.

Failed to remove the virtual name environment for the service `service name`. This is a VCS internal error. Solution: Contact Symantec Technical Support.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to wait for the service <code>service name</code> to start. Error = <code>Error code</code>.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>The <code>service name</code> service is not in stopped or running state. State = <code>state name</code>.</td>
<td>The service is in an invalid state.</td>
</tr>
<tr>
<td>Failed to open the service <code>service name</code>. Error = <code>Error code</code>.</td>
<td>The agent failed to open the service from the Service Control Manager. Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
<tr>
<td>Failed to query the status of the service <code>service name</code>. Error = <code>Error code</code>.</td>
<td>The agent failed to query the state of the service. Solution: Check whether the service is present in the Service Control Manager.</td>
</tr>
<tr>
<td>The service <code>service name</code> is not in running state. Attempt to stop it might be unsuccessful.</td>
<td>The SQL Server service could be in <code>PAUSE</code>, <code>PAUSE PENDING</code>, or <code>START PENDING</code> state. Solution: Resume the service and then attempt to stop it.</td>
</tr>
<tr>
<td>The service <code>service name</code> did not stop. Error = <code>Error code</code>.</td>
<td>The agent failed to stop the service. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service <code>service name</code> did not stop within the specified timeout. Error = <code>Error code</code>.</td>
<td>The agent failed to stop the service within the time limit as specified in the SQLOfflineTimeout attribute.</td>
</tr>
<tr>
<td>Failed to remove the virtual name environment for the service <code>service name</code>.</td>
<td>This is a VCS internal error. Solution: Contact Symantec Technical Support.</td>
</tr>
</tbody>
</table>
Agent for SQL Server 2005 Analysis service

This section describes the error messages for the SQL Server 2005 Analysis service agent.

Table 10-7 SQL Server 2005 Analysis service agent error messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to convert the argument list. Error = Error code.</td>
<td>This is a VCS internal error.</td>
</tr>
<tr>
<td></td>
<td>Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>Invalid value specified for attribute attribute name.</td>
<td>No value provided for the specified attribute.</td>
</tr>
<tr>
<td></td>
<td>Solution: Provide a value for the attribute.</td>
</tr>
<tr>
<td>Failed to initialize the SQLOlapService2005 agent.</td>
<td>The agent failed to initialize the SQLOlapService2005 agent for the SQL Server 2005 Analysis Service.</td>
</tr>
<tr>
<td></td>
<td>Solution: Verify whether the SQLOlapService2005 agent exists.</td>
</tr>
<tr>
<td>Failed to open the SCM handle. Error = Error code.</td>
<td>The agent fails to get a handle to the Service Control Manager (SCM). This could occur if the specified SCM database does not exist or the requested access is denied.</td>
</tr>
<tr>
<td></td>
<td>Solution: Verify that SCM can be run on the host. See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>The service service name is not in stopped state.</td>
<td>The service is in an invalid state.</td>
</tr>
<tr>
<td></td>
<td>Solution: Check the state of the service.</td>
</tr>
<tr>
<td>Failed to start the service service name. Error = Error code.</td>
<td>The agent failed to start the service.</td>
</tr>
<tr>
<td></td>
<td>Solution: See the associated Windows error code for more information.</td>
</tr>
<tr>
<td>SQL Server Instance name is not specified. Agent will operate on the default instance.</td>
<td>No value spaced-out for SQL Server instance name. Agent would operate on the default SQL Server instance.</td>
</tr>
<tr>
<td>Failed to set the virtual computer name in the environment of the service service name. Error = Error code.</td>
<td>This is a VCS internal error.</td>
</tr>
<tr>
<td></td>
<td>Solution: Contact Symantec Technical Support.</td>
</tr>
<tr>
<td>The service service name did not start within the specified time limit.</td>
<td>The agent failed to start the service within the time limit as specified in the SQLOnlineTimeout attribute.</td>
</tr>
</tbody>
</table>
Troubleshooting the agents
Error messages and descriptions

Failed to wait for the service *service name* to start. Error = *Error code*.
This is a VCS internal error.
Solution: Contact Symantec Technical Support.

The service *service name* service is not in stopped or running state. State = *state name*.
The service is in an invalid state.

Failed to open the service *service name*. Error = *Error code*.
The agent failed to open the service from the Service Control Manager.
Solution: Check whether the service is present in the Service Control Manager.

Failed to query the status of the service *service name*. Error = *Error code*.
The agent failed to query the state of the service.
Solution: Check whether the service is present in the Service Control Manager.

The service *service name* is not in running state. Attempt to stop it might be unsuccessful.
The SQL Server service could be in PAUSE, PAUSE PENDING, or START PENDING state.
Solution: Resume the service and then attempt to stop it.

The service *service name* did not stop. Error = *Error code*.
The agent failed to stop the service. See the associated Windows error code for more information.

The service *service name* did not stop within the specified timeout. Error = *Error code*.
The agent failed to stop the service within the time limit as specified in the SQLOfflineTimeout attribute.

Failed to remove the virtual name environment for the service *service name*.
This is a VCS internal error.
Solution: Contact Symantec Technical Support.

Table 10-7 SQL Server 2005 Analysis service agent error messages (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
</table>
| Failed to wait for the service *service name* to start. Error = *Error code*. | This is a VCS internal error.
Solution: Contact Symantec Technical Support. |
| The service *service name* service is not in stopped or running state. State = *state name*. | The service is in an invalid state. |
| Failed to open the service *service name*. Error = *Error code*. | The agent failed to open the service from the Service Control Manager.
Solution: Check whether the service is present in the Service Control Manager. |
| Failed to query the status of the service *service name*. Error = *Error code*. | The agent failed to query the state of the service.
Solution: Check whether the service is present in the Service Control Manager. |
| The service *service name* is not in running state. Attempt to stop it might be unsuccessful. | The SQL Server service could be in PAUSE, PAUSE PENDING, or START PENDING state.
Solution: Resume the service and then attempt to stop it. |
| The service *service name* did not stop. Error = *Error code*. | The agent failed to stop the service. See the associated Windows error code for more information. |
| The service *service name* did not stop within the specified timeout. Error = *Error code*. | The agent failed to stop the service within the time limit as specified in the SQLOfflineTimeout attribute. |
| Failed to remove the virtual name environment for the service *service name*. | This is a VCS internal error.
Solution: Contact Symantec Technical Support. |
Troubleshooting the agents

Error messages and descriptions
Resource type definitions

This chapter contains the following topics:

- “About resource type definitions” on page 168
- “NetApp Filer agent” on page 168
- “NetApp SnapDrive agent” on page 169
- “NetApp SnapMirror agent” on page 170
- “Agent for SQL Server 2000” on page 172
- “Agent for MSSearch service” on page 176
- “Agent for SQL Server 2005” on page 178
- “Agent for SQL Server 2005 agent service” on page 182
- “Agent for SQL Server 2005 analysis service” on page 184
- “MSDTC agent” on page 186
About resource type definitions

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

The sample dependency graph depicts the resource types, resources, and resource dependencies required to create the service groups.

NetApp Filer agent

The NetApp Filer agent is configured as a resource of type NetAppFiler.

Resource type definition

```c
type NetAppFiler {
    static int MonitorInterval = 30
    static i18nstr ArgList[] = { FilerName, StorageIP } 
    static str Operations = None
    str FilerName
    str StorageIP
}
```

Attribute definitions

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type - Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilerName</td>
<td>string-scalar</td>
<td>DNS-resolvable name or IP address of the locally</td>
</tr>
<tr>
<td></td>
<td></td>
<td>attached filer.</td>
</tr>
<tr>
<td>StorageIP</td>
<td>string -scalar</td>
<td>The private storage IP address of the filer.</td>
</tr>
</tbody>
</table>
NetApp SnapDrive agent

The NetApp SnapDrive agent is configured as a resource of type NetAppSnapDrive.

Resource type definition

type NetAppSnapDrive
{
    static int MonitorInterval = 30
    static int NumThreads = 1
    static i18nstr ArgList[] = { FilerResName, "FilerResName:FilerName", "FilerResName:StorageIP", VolumeName, ShareName, LUN, MountPath, Initiator, InitiatorMonitorInterval }
    str FilerResName
    str VolumeName
    str ShareName
    str LUN
    str MountPath
    str Initiator[]
    int InitiatorMonitorInterval = 30
}

Attribute definitions

Table A-2  NetApp SnapDrive agent attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type - Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilerResName</td>
<td>string-scalar</td>
<td>Name of the VCS NetAppFiler-type resource in the service group.</td>
</tr>
<tr>
<td>VolumeName</td>
<td>string-scalar</td>
<td>Name of the volume containing the virtual disk. Define the volume name in the same case as on the filer.</td>
</tr>
<tr>
<td>ShareName</td>
<td>string-scalar</td>
<td>Name of the CIFS share containing the virtual disk.</td>
</tr>
<tr>
<td>LUN</td>
<td>string-scalar</td>
<td>Name of the LUN (virtual disk) on the filer that is presented to the host for mounting. Define the LUN name in the same case as on the filer.</td>
</tr>
<tr>
<td>MountPath</td>
<td>string-scalar</td>
<td>Drive letter to be assigned to the virtual disk.</td>
</tr>
<tr>
<td>Initiator</td>
<td>string-vector</td>
<td>Name of iSCSI or FC initiator the host uses to connect virtual disks. You can retrieve this value from the Disk Management console.</td>
</tr>
</tbody>
</table>
NetApp SnapMirror agent

The NetApp SnapMirror agent is configured as a resource of type NetAppSnapMirror.

Resource type definition

```c
type NetAppSnapMirror {
    static keylist SupportedActions = { fbsync }
    static int MonitorInterval = 300
    static int NumThreads = 1
    static i18nstr ArgList[] = { FilerResName,
                               "FilerResName:FilerName",
                               "FilerResName:StorageIP", VolumeName,
                               SnapMirrorArguments,
                               SnapMirrorSchedule,  AppResName }
    str FilerResName
    str VolumeName
    str SnapMirrorArguments
    str SnapMirrorSchedule
    str AppResName
}
```

Attribute definitions

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type - Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilerResName</td>
<td>string-scalar</td>
<td>Name of the VCS NetAppFiler-type resource in the group.</td>
</tr>
<tr>
<td>VolumeName</td>
<td>string-scalar</td>
<td>Name of the volume containing the virtual disk. Define the volume name in the same case as on the filer.</td>
</tr>
<tr>
<td>SnapMirrorArguments</td>
<td>string-scalar</td>
<td>Specifies the SnapMirror arguments such as maximum transfer speed and restart mode.</td>
</tr>
<tr>
<td>SnapMirrorSchedule</td>
<td>string-scalar</td>
<td>Specifies the schedule the destination uses for updating data. Do not assign a value for this attribute if you use SnapManager. By default, this attribute is not assigned any value.</td>
</tr>
</tbody>
</table>
### Table A-3  NetApp SnapMirror agent attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type - Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppResName</td>
<td>string-scalar</td>
<td>Name of the resource configured to monitor the application being made highly available.</td>
</tr>
</tbody>
</table>
Agent for SQL Server 2000

The agent for SQL Server 2000 is configured as a resource of type SQLServer2000.

Resource type definition

type SQLServer2000 {
    static i18nstr ArgList[] = {Instance,
        "LanmanResName:VirtualName", "MountResName:MountPath",
        SQLOnlineTimeout, SQLOfflineTimeout, DetailMonitor,
        SQLDetailMonitorTimeout, Username, Domain, Password, SQLFile
    }
    str Instance
    str LanmanResName
    int SQLOnlineTimeout = 90
    int SQLOfflineTimeout = 90
    boolean DetailMonitor = 0
    boolean FaultOnDMScriptFailure = 1
    int SQLDetailMonitorTimeout = 30
    i18nstr Username
    i18nstr Domain
    str Password
    i18nstr SQLFile
    str MountResName
}

Attribute definitions

Review the following information to familiarize yourself with the required agent attributes for a SQLServer2000 resource type. This information will assist you during the agent configuration.

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>string-scalar</td>
<td>Name of instance to monitor. If the attribute is blank, the agent monitors the default instance.</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>string-scalar</td>
<td>The Lanman resource name on which the SQL Server 2000 resource depends.</td>
</tr>
<tr>
<td>MountResName</td>
<td>string-scalar</td>
<td>The mount resource name on which the SQL Server 2000 resource depends.</td>
</tr>
<tr>
<td>SQLOnlineTimeout</td>
<td>integer-scalar</td>
<td>Number of seconds that can elapse before online entry point aborts. Default is 90.</td>
</tr>
</tbody>
</table>
### Table A-4  SQL Server 2000 agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLOfflineTimeout</td>
<td>integer-scalar</td>
<td>Number of seconds that can elapse before offline entry point aborts. Default is 90.</td>
</tr>
</tbody>
</table>

### Table A-5  SQL Server 2000 agent optional attributes

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DetailMonitor</td>
<td>boolean</td>
<td>Defines whether the agent performs detail monitoring of SQL Server 2000 database. The value 0 indicates the agent will not monitor the database in detail. The value 1 indicates the agent will. Default = 0. <strong>Note:</strong> If the attribute is set to 1, the attributes Username, Password, Domain, SQLDetailMonitorTimeOut, and SQLFile must be assigned appropriate values.</td>
</tr>
<tr>
<td>FaultOnDMScriptFailure</td>
<td>boolean</td>
<td>Defines whether the agent fails over the service group if the detail monitoring script execution fails. Default = 1. The value 1 indicates that the agent fails over the service group if detail monitoring script fails to execute. The value 0 indicates that it does not.</td>
</tr>
<tr>
<td>SQLDetailMonitor Timeout</td>
<td>integer-scalar</td>
<td>Number of seconds that can elapse before the detail monitor routine aborts. Default is 30.</td>
</tr>
<tr>
<td>Username</td>
<td>string-scalar</td>
<td>The Microsoft Windows authentication name when logging in to a database for detail monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1. <strong>Note:</strong> This attribute can take localized values.</td>
</tr>
</tbody>
</table>
The following example describes typical service groups configured to monitor the state of SQL Server 2000 in a VCS cluster. A sample configuration graphically depicts the resources and their dependencies within the service group. For more information about these resources and resource types, see the chapter VCS Resource Types and Agents in the *Veritas Cluster Server Administrator’s Guide*.

In the sample dependency graph below, the shared virtual disk is configured using the NetApp Filer (NetAppFiler) resource. The virtual name for the SQL Server is created using the Lanman resource. The service group IP address for the SQL Server is configured using the IP and NIC resources. The Netapp SnapDrive mount point is created using the NetappSnapDrive resource. SQL Server 2000 registry is replicated using the RegRep and RegRepNetAppSnapDrive resources. The SQL Server 2000 resource comes online after each of these resources are brought online.

**Table A-5 SQL Server 2000 agent optional attributes (continued)**

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Domain              | string-scalar      | Domain for the user account. This attribute is used to create a trusted connection to the SQL Server 2000 instance if “DetailMonitor” attribute is set to 1.  
*Note:* This attribute can take localized values. |
| Password            | string-scalar      | Password for logging in to a database for detail monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1. |
| SQLFile             | string-scalar      | The location of the SQLFile executed during a monitor cycle. This attribute must not be null if the “DetailMonitor” attribute is set to 1.  
*Note:* This attribute can take localized values. |
Figure A-1  SQL Server 2000 service group dependency graph
Agent for MSSESearch service

The agent for MSSESearch service is configured as a resource of type MSSESearch.

Resource type definition

```plaintext
type MSSESearch {
    static i18nstr ArgList[] = { AppName }
    str AppName
}
```

Attribute definitions

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

<table>
<thead>
<tr>
<th>Required Attribute</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppName</td>
<td>string-scalar</td>
<td>The name of MSSESearch instance to be monitored. See &quot;MSSESearch service&quot; on page 20 for more information.</td>
</tr>
</tbody>
</table>
Sample dependency graph

The following examples describe typical service groups configured to monitor the state of MSSearch service in a VCS cluster. A sample configuration graphically depicts the resources and their dependencies within the service group. For more information about these resources and resource types, see the chapter VCS Resource Types and Agents in the *Veritas Cluster Server Administrator’s Guide*.

In the sample configuration shown in the dependency graph below, the shared virtual disk is configured using the NetApp Filer (NetAppFiler) resource. The MSSearch service depends upon the SQL Server 2000 service. The virtual name for the SQL Server is created using the Lanman resource. The service group IP address for the SQL Server is configured using the IP and NIC resources. The Netapp SnapDrive mount point is created using the NetappSnapDrive resource. SQL Server 2000 and MSSearch registry is replicated using the RegRep and RegRepNetAppSnapDrive resources. Different mounts are used for SQL Server 2000 and MSSearch registry replication. The MSSearch resource comes online after each of these resources are brought online.

**Figure A-2** Typical MSSearch service service group dependency graph
Agent for SQL Server 2005

The agent for SQL Server 2005 is configured as a resource of type SQLServer2005.

Resource type definition

type SQLServer2005 {
    static i18nstr ArgList[] =
        {Instance,"LanmanResName:VirtualName",SQLOnlineTimeout,
        SQLOfflineTimeout,DetailMonitor, SQLDetailMonitorTimeout,
        Username, Domain, Password, SQLFile }
    str Instance
    str LanmanResName
    int SQLOnlineTimeout = 90
    int SQLOfflineTimeout = 90
    boolean DetailMonitor = 0
    boolean FaultOnDMScriptFailure = 1
    int SQLDetailMonitorTimeout = 30
    i18nstr Username
    i18nstr Domain
    str Password
    i18nstr SQLFile
}

Attribute definitions

Review the following information to familiarize yourself with the required agent attributes for a SQLServer2005 resource type. This information will assist you during the agent configuration.

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>string-scalar</td>
<td>Name of instance to monitor. If the attribute is blank, the agent monitors the default instance.</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>string-scalar</td>
<td>The Lanman resource name on which the SQL Server 2005 resource depends.</td>
</tr>
<tr>
<td>SQLOnlineTimeout</td>
<td>integer-scalar</td>
<td>Number of seconds that can elapse before online entry point aborts. Default is 90.</td>
</tr>
<tr>
<td>SQLOfflineTimeout</td>
<td>integer-scalar</td>
<td>Number of seconds that can elapse before offline entry point aborts. Default is 90.</td>
</tr>
<tr>
<td>Optional Attributes</td>
<td>Type and Dimension</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DetailMonitor</td>
<td>boolean</td>
<td>Defines whether the agent performs detail monitoring of SQL Server 2005 database. The value 0 indicates the agent will not monitor the database in detail. The value 1 indicates the agent will. Default = 0. <strong>Note:</strong> If the attribute is set to 1, the attributes Username, Password, Domain, SQLDetailMonitorTimeOut, and SQLFile must be assigned appropriate values.</td>
</tr>
<tr>
<td>FaultOnDMScriptFailure</td>
<td>boolean</td>
<td>Defines whether the agent fails over the service group if the detail monitoring script execution fails. Default = 1. The value 1 indicates that the agent fails over the service group if detail monitoring script fails to execute. The value 0 indicates that it does not.</td>
</tr>
<tr>
<td>SQLDetailMonitor Timeout</td>
<td>integer-scalar</td>
<td>Number of seconds that can elapse before the detail monitor routine aborts. Default is 30.</td>
</tr>
<tr>
<td>Username</td>
<td>string-scalar</td>
<td>The Microsoft Windows authentication name when logging in to a database for detail monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1. <strong>Note:</strong> This attribute can take localized values.</td>
</tr>
<tr>
<td>Domain</td>
<td>string-scalar</td>
<td>Domain for the user account. This attribute is used to create a trusted connection to the SQL Server 2005 instance if “DetailMonitor” attribute is set to 1. <strong>Note:</strong> This attribute can take localized values.</td>
</tr>
</tbody>
</table>
### Table A-8  SQL Server 2005 agent optional attributes (continued)

<table>
<thead>
<tr>
<th>Optional Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>string-scalar</td>
<td>Password for logging in to a database for in-depth monitoring. This attribute must not be null if “DetailMonitor” attribute is set to 1.</td>
</tr>
</tbody>
</table>
| SQLFile             | string-scalar      | The location of the SQLFile executed during a monitor cycle. This attribute must not be null if the “DetailMonitor” attribute is set to 1.  
**Note:** This attribute can take localized values. |
Sample dependency graph

The following example describes typical service groups configured to monitor the state of SQL Server 2005 in a VCS cluster. A sample configuration graphically depicts the resources and their dependencies within the service group. For more information about these resources and resource types, see the chapter VCS Resource Types and Agents in the *Veritas Cluster Server Administrator’s Guide*.

In the sample dependency graph below, the shared virtual disk is configured using the NetApp Filer (NetAppFiler) resource. The virtual name for the SQL Server is created using the Lanman resource. The service group IP address for the SQL Server is configured using the IP and NIC resources. The Netapp SnapDrive mount point is created using the NetappSnapDrive resource. SQL Server 2005 registry is replicated using the RegRep and RegRepNetAppSnapDrive resources. The SQL Server 2005 resource comes online after each of these resources are brought online.

*Figure A-3*  SQL Server 2005 service group dependency graph
Agent for SQL Server 2005 agent service

The agent for SQL Server 2005 Agent service is configured as a resource of type SQLAgService2005.

Resource type definition

```csharp
type SQLAgService2005 {
    static i18nstr ArgList[] = {"SQLServer2005ResName:Instance", "LanmanResName:VirtualName"}
    string SQLServer2005ResName
    string LanmanResName
}
```

Attribute definitions

Review the following information to familiarize yourself with the required agent attributes for a SQLAgService2005 resource type. This information will assist you during the agent configuration.

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLServer2005ResName</td>
<td>string-scalar</td>
<td>The name of the SQLServer2005 resource on which the SQL Server 2005 Agent service resource depends.</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>string-scalar</td>
<td>The Lanman resource name on which the SQL Server 2005 resource depends.</td>
</tr>
</tbody>
</table>
Sample dependency graph

The following example describes typical service groups configured to monitor the state of SQL Server 2005 Agent service in a VCS cluster. A sample configuration graphically depicts the resources and their dependencies within the service group. For more information about these resources and resource types, see the chapter VCS Resource Types and Agents in the *Veritas Cluster Server Administrator’s Guide*.

In the sample dependency graph below, the shared virtual disk is configured using the NetApp Filer (NetAppFiler) resource. The virtual name for the SQL Server is created using the Lanman resource. The service group IP address for the SQL Server is configured using the IP and NIC resources. The Netapp SnapDrive mount point is created using the NetappSnapDrive resource. SQL Server 2005 registry is replicated using the RegRep and RegRepNetAppSnapDrive resources. The SQL Server 2005 Agent service resource depends on the SQL Server 2005 resource. The SQL Server 2005 Agent service resource comes online after each of these resources are brought online.

Figure A-4  SQL Server 2005 Agent Service service group dependency graph
Agent for SQL Server 2005 analysis service

The agent for SQL Server 2005 Analysis service is configured as a resource of type SQLOlapService2005.

Resource type definition

```csharp
    type SQLOlapService2005 (
        static i18nstr ArgList[] = {"SQLServer2005ResName:Instance", "LanmanResName:VirtualName" }
        str SQLServer2005ResName
        str LanmanResName
    )
```

Attribute definitions

Review the following information to familiarize yourself with the required agent attributes for a SQLOlapService2005 resource type. This information will assist you during the agent configuration.

Table A-10  SQL Server 2005 Analysis service agent required attributes

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLServer2005ResName</td>
<td>string-scalar</td>
<td>The name of the SQLServer2005 resource on which the SQL Server 2005 Analysis service resource depends.</td>
</tr>
<tr>
<td>LanmanResName</td>
<td>string-scalar</td>
<td>The Lanman resource name on which the SQL Server 2005 resource depends.</td>
</tr>
</tbody>
</table>
Sample dependency graph

The following example describes typical service groups configured to monitor the state of SQL Server 2005 Analysis service in a VCS cluster. A sample configuration graphically depicts the resources and their dependencies within the service group. For more information about these resources and resource types, see the chapter VCS Resource Types and Agents in the *Veritas Cluster Server Administrator’s Guide*.

In the sample dependency graph below, the shared virtual disk is configured using the NetApp Filer (NetAppFiler) resource. The virtual name for the SQL Server is created using the Lanman resource. The service group IP address for the SQL Server is configured using the IP and NIC resources. The Netapp SnapDrive mount point is created using the NetappSnapDrive resource. SQL Server 2005 registry is replicated using the RegRep and RegRepNetAppSnapDrive resources. The SQL Server 2005 Analysis service resource depends on the SQL Server 2005 resource. The SQL Server 2005 Analysis service resource comes online after each of these resources are brought online.

**Figure A-5** SQL Server 2005 Analysis Service service group dependency graph
MSDTC agent

The MSDTC agent is configured as a resource of type MSDTC.

Resource type definition

type MSDTC {
    static i18nstr ArgList[] = {"LanmanResName:VirtualName", "MountResName:MountPath", LogPath }
    str LanmanResName
    str MountResName
    i18nstr LogPath
}

Attribute definitions

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

<table>
<thead>
<tr>
<th>Required Attributes</th>
<th>Type and Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>LanmanResName</td>
<td>string-scalar</td>
<td>Name of the Lanman resource on which the MSDTC resource depends.</td>
</tr>
<tr>
<td>MountResName</td>
<td>string-scalar</td>
<td>The mount resource name on which the MSDTC resource depends.</td>
</tr>
<tr>
<td>LogPath</td>
<td>string-scalar</td>
<td>The path for MSDTC logs. This attribute can take localized values.</td>
</tr>
</tbody>
</table>
Sample dependency graph

The following examples describe typical service groups configured to monitor the state of an MSDTC service group in a VCS cluster. A sample configuration graphically depicts the resources and their dependencies within the service group. For more information about these resources and resource types, see the chapter VCS Resource Types and Agents in the *Veritas Cluster Server Administrator’s Guide*.

In the sample configuration shown in the dependency graph below, the shared virtual disk is configured using the NetApp Filer (NetAppFiler) resource. The virtual name for the MSDTC Server is created using the Lanman resource. The service group IP address for the MSDTC Server is configured using the IP and NIC resources. The Netapp SnapDrive mount point is created using the NetappSnapDrive resource. MSDTC registry is replicated using the RegRep and RegRepNetAppSnapDrive resources. The MSDTC resource comes online after each of these resources are brought online.

*Figure A-6*  MSDTC service group dependency graph
Resource type definitions
MSDTC agent
Sample configurations

This chapter contains the following topics:

■ “About sample configurations” on page 190
■ “Sample configuration for a SQL Server 2000 cluster” on page 190
■ “Sample configuration for a SQL Server 2005 cluster” on page 194
About sample configurations

The sample configurations in this appendix describe typical service groups configured to monitor the state of SQL Server 2000 and SQL Server 2005 in a VCS cluster using Network Appliance Filers to manage shared storage.

Sample configuration for a SQL Server 2000 cluster

The following sample configuration depicts a two node cluster. A SQL Server service group with MSSEarch instance is configured in the cluster. The MSDTC service group is also configured on the same nodes.

```
include "types.cf"

cluster clsec (
    UserNames = { a = bIIc }
    ClusterAddress = "10.217.60.172"
    Administrators = { a }
)
remotecluster cl48_49 (
    ClusterAddress = "10.217.60.169"
)
heartbeat Icmp (
    ClusterList = { cl48_49 }
    AYATimeout = 30
    Arguments @cl48_49 = { "10.217.60.169" }
)
system VCSW2K244 (
)

group sq (
    SystemList = { VCSW2K244 = 0 }
    ClusterList = { cl48_49 = 1, clsec = 0 }
    Authority = 1
    ClusterFailOverPolicy = Auto
)
IP sq-IP (
    Address = "10.217.60.173"
    SubNetMask = "255.255.252.0"
    MACAddress @VCSW2K244 = "00-0B-DB-95-9C-A0"
)
Lanman sq-Lanman (
    VirtualName = VTEST1
    IPResName = sq-IP
)
MSSearch sq-MSSearch (
    AppName = "SQLServer$TEST1"
)
NIC sq-NIC (
    MACAddress @VCSW2K244 = "00-0B-DB-95-9C-A0"
)
Sample configuration for a SQL Server 2000 cluster

NetAppFile sq-NetAppFile

FilerName = netapp-vcs
StorageIP = "10.212.88.100"

NetAppSnapDrive sq-NetAppSnapDrive

FilerName = sq-NetAppFile
VolumeName = vol9
ShareName = data09
LUN = "d90.lun"
MountPath = I
Initiator @VCS2K244 = "iqn.1991-05.com.microsoft:vcsw2k244.vcs.dev"

NetAppSnapDrive sq-NetAppSnapDrive-1

FilerName = sq-NetAppFile
VolumeName = vol9
ShareName = data09
LUN = "d91.lun"
MountPath = J
Initiator @VCS2K244 = "iqn.1991-05.com.microsoft:vcsw2k244.vcs.dev"

NetAppSnapMirror sq-NetAppSnapMirror

FilerName = sq-NetAppFile
VolumeName = vol9

RegRep sq-RegRep-MSSQL

MountResName = sq-NetAppSnapDrive-1
ReplicationDirectory = "\RegRep\sq-RegRep-MSSQL"
Keys = {
"HKLM\SOFTWARE\Microsoft\MSSQLServer\Client" = "",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\TEST1" = "",
"HKLM\SOFTWARE\Network Appliance\SnapManager for SQL Server\Server" = ""
}
ExcludeKeys = {
"HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\TEST1\Setup",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\TEST1\SQLServerAgent\Subsystems",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\TEST1\Tracking"
}

RegRep sq-RegRep-MSSearch

MountResName = sq-NetAppSnapDrive-1
ReplicationDirectory = "\RegRep\sq-RegRep-MSSearch"
Keys ={
"HKLM\SOFTWARE\Microsoft\Search\1.0\Applications\SQLServer\TEST1\Setup" = "",
"HKLM\SOFTWARE\Microsoft\Search\1.0\CatalogNames\SQLServer\TEST1" = "",
"HKLM\SOFTWARE\Microsoft\Search\1.0\"}
Sample configuration for a SQL Server 2000 cluster

```powershell
# Sample configuration

Databases\SQLServer$TEST1" = ",
"HKLM\Software\Microsoft\Search\1.0\Gather\SQLServer$TEST1" = ",
"HKLM\Software\Microsoft\Search\1.0\Gathering Manager\Applications\SQLServer$TEST1" = ",
"HKLM\Software\Microsoft\Search\1.0\Indexer\SQLServer$TEST1" = ",

SQLServer2000 sq-SQLServer2000 (Critical = 0 Instance = TEST1 LanmanResName = sq-Lanman MountResName = sq-NetAppSnapDrive DetailMonitor = 1 Username = administrator Domain = "vcs.dev" Password = AKEmBMiMPmFEdGBgCGd SQLFile = "c:\\script.sql"

sq-SQLServer2000 requires sq-RegRep-MSSQL
sq-SQLServer2000 requires sq-Lanman
sq-SQLServer2000 requires sq-NetAppSnapDrive
sq-NetAppSnapDrive requires sq-NetAppSnapMirror
sq-RegRep-MSSQL requires sq-NetAppSnapDrive-1
sq-NetAppSnapDrive-1 requires sq-NetAppSnapMirror
sq-IP requires sq-NIC
sq-Lanman requires sq-IP
sq-NetAppSnapMirror requires sq-NetAppFiler
sq-MSSearch requires sq-SQLServer2000
sq-MSSearch requires sq-RegRep-MSSearch
sq-RegRep-MSSearch requires sq-NetAppSnapDrive-1

// resource dependency tree
//
// group sq
// { MSSearch sq-MSSearch
//   { SQLServer2000 sq-SQLServer2000
//     { RegRep sq-RegRep-MSSQL
//       { NetAppSnapDrive sq-NetAppSnapDrive-1
//         { NetAppSnapMirror sq-NetAppSnapMirror
//           { NetAppFiler sq-NetAppFiler
//             }
//           }
//         }
//       }
//     }
//   }
// }
// Lanman sq-Lanman
// }
```
Sample configurations

Sample configuration for a SQL Server 2000 cluster

// IP sq-IP
// {
//     NIC sq-NIC
// }
// NetAppSnapDrive sq-NetAppSnapDrive
// {
//     NetAppSnapMirror sq-NetAppSnapMirror
//     {
//         NetAppFiler sq-NetAppFiler
//     }
// }
// RegRep sq-RegRep-MSSearch
// {
//     NetAppSnapDrive sq-NetAppSnapDrive-1
//     {
//         NetAppSnapMirror sq-NetAppSnapMirror
//     }
//     {
//         NetAppFiler sq-NetAppFiler
//     }
// }
//
//}
Sample configuration for a SQL Server 2005 cluster

The following sample configuration depicts a two node SQL Server cluster with MSDTC server configured. A SQL Server service group with MSSearch service, SQL Server Agent service, and SQL Server Analysis service is configured in the cluster. The MSDTC service group is also configured on the same nodes.

```plaintext
include *types.cf*

cluster clnew4533 {
    UserNames = { a = eHHb }
    ClusterAddress = "10.217.60.166"
    Administrators = { a }
}

remotecluster clremote {
    ClusterAddress = "10.217.119.60"
}

heartbeat Icmp {
    ClusterList = { clremote }
    AYATimeout = 30
    Arguments @clremote = { "10.217.119.60" }
}

system VCSW2K246 {
    
}

system VCSW2K247 {
    
}

group sqlg {
    SystemList = { VCSW2K246 = 0, VCSW2K247 = 1 }
    ClusterList = { clnew4533 = 1, clremote = 0 }
    Authority = 1
    ClusterFailOverPolicy = Auto
}

IP sqlg-IP {
    Address = "10.217.60.167"
    SubNetMask = "255.255.252.0"
    MACAddress @VCSW2K246 = "00-0B-DB-95-9E-6C"
    MACAddress @VCSW2K247 = "00-0B-DB-95-9D-F4"
}

Lanman sqlg-Lanman {
    VirtualName = VHD
    IPResName = sqlg-IP
}
```
Sample configurations for a SQL Server 2005 cluster

**NIC sqlg-NIC**

```plaintext
MACAddress @VCSW2K246 = "00-0B-DB-95-9E-6C"
MACAddress @VCSW2K247 = "00-0B-DB-95-9D-F4"
```

**NetAppFiler sqlg-NetAppFiler**

```plaintext
FilerName = vcsfiler01
StorageIP = "10.217.60.153"
```

**NetAppSnapDrive sqlg-NetAppSnapDrive**

```plaintext
Critical = 0
FilerResName = sqlg-NetAppFiler
VolumeName = vol3
ShareName = data03
LUN = "d30.lun"
MountPath = I
Initiator @VCSW2K246 = "iqn.1991-05.com.microsoft:vcsw2k246.vcs.dev"
Initiator @VCSW2K247 = "iqn.1991-05.com.microsoft:vcsw2k247.vcs.dev"
```

```plaintext
Critical = 0
FilerResName = sqlg-NetAppFiler
VolumeName = vol3
ShareName = data03
LUN = "d31.lun"
MountPath = J
Initiator @VCSW2K246 = "iqn.1991-05.com.microsoft:vcsw2k246.vcs.dev"
Initiator @VCSW2K247 = "iqn.1991-05.com.microsoft:vcsw2k247.vcs.dev"
```

**NetAppSnapMirror sqlg-NetAppSnapMirror**

```plaintext
FilerResName = sqlg-NetAppFiler
VolumeName = vol3
```

**RegRep sqlg-RegRep-MSSQL**

```plaintext
MountResName = sqlg-NetAppSnapDrive-1
ReplicationDirectory = "\RegRep\sqlg-RegRep-MSSQL"
Keys @VCSW2K246 = {"HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.1\MSSQLServer" = "SaveRestoreFile:sqlg-RegRep-MSSQL\MSSQLServer.reg", "HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.1\\PROVIDERS" = "SaveRestoreFile:sqlg-RegRep-MSSQL_PROVIDERS.reg", "HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.1\\InstanceName" = "SaveRestoreFile:sqlg-RegRep-MSSQL_InstanceName.reg"}
```
Sample configuration for a SQL Server 2005 cluster

Sample configurations

SQLServer2005 sqlg-SQLServer2005

Critical = 0
Instance = HD
LanmanResName = sqlg-Lanman

sqlg-SQLServer2005 requires sqlg-RegRep-MSSQL
sqlg-SQLServer2005 requires sqlg-Lanman
sqlg-SQLServer2005 requires sqlg-NetAppSnapDrive
sqlg-NetAppSnapDrive requires sqlg-NetAppSnapMirror
sqlg-RegRep-MSSQL requires sqlg-NetAppSnapDrive-1
sqlg-NetAppSnapDrive-1 requires sqlg-NetAppSnapMirror
sqlg-IP requires sqlg-NIC
sqlg-Lanman requires sqlg-IP
sqlg-NetAppSnapMirror requires sqlg-NetAppFiler

// resource dependency tree
//
// group sqlg
// {
// SQLServer2005 sqlg-SQLServer2005
// { // RegRep sqlg-RegRep-MSSQL
// { 

Server\MSSQL.1\Replication" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_Replication.reg",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\SQLServerAgent" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_SQLServerAgent.reg",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\SQLServerSCP" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_SQLServerSCP.reg" } } Keys @VCSW2K247 = {

"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\MSSQLServer" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_MSSQLServer.reg",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\PROVIDERS" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_PROVIDERS.reg",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\Replication" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_Replication.reg",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\SQLServerAgent" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_SQLServerAgent.reg",
"HKLM\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.1\SQLServerSCP" =
"SaveRestoreFile:sqlg-RegRep-MSSQL_SQLServerSCP.reg" } ExcludeKeys = { "" }

SQLServer2005 sqlg-SQLServer2005 (Critical = 0
Instance = HD
LanmanResName = sqlg-Lanman

}
Sample configuration for a SQL Server 2005 cluster

//        NetAppSnapDrive sqlg-NetAppSnapDrive-1
//         {
//          NetAppSnapMirror sqlg-NetAppSnapMirror
//           {
//            NetAppFiler sqlg-NetAppFiler
//            }
//           }
//         }
//     }
//     Lanman sqlg-Lanman
//      {
//       IP sqlg-IP
//        {
//         NIC sqlg-NIC
//        }
//      }
//     }
//    NetAppSnapDrive sqlg-NetAppSnapDrive
//     {
//      NetAppSnapMirror sqlg-NetAppSnapMirror
//       {
//        NetAppFiler sqlg-NetAppFiler
//       }
//      }
//    }
//  }
// }

Sample configurations
Sample configuration for a SQL Server 2005 cluster
### Index

**A**
- Active/Active
  - configuration diagram 110
  - configuration overview 110
  - configuring network and storage 113
  - creating a user-defined database 116
- Active/Active environment
  - definition of 22
- Active-Active
  - configuring VCS SQL Server service group 116
- application failure, detecting 21
- attribute definitions
  - MSDTC agent 186
  - MSSearch agent 176
  - SQL Server 2000 agent 172
  - SQL Server 2005 agent 178
  - SQL Server Agent Service agent 182
  - SQL Server Analysis Service agent 184

**C**
- clusters
  - configuring (DR) 125, 129
  - configuring (HA) 31
  - setting the internal name of the clustered instance (2000) 63
  - setting the internal name of the clustered instance (2005) 71
- configurations
  - Disaster Recovery 27, 122
- configure
  - LLT over UDP using VCW 37
- configuring
  - cluster (DR) 125, 129
  - cluster (HA) 31
  - SQL Server 2000 DR overview 123
  - SQL Server 2005 DR overview 128
  - SQL Server service group 2000 125
  - SQL Server service group 2005 131
- converting
  - moving data files and databases (HA) 107
  - standalone SQL conversion to HA 101

**D**
- database
  - new database for SQL Server 2000 83
  - user-defined for SQL Server 2000 82
- database agent
  - installing 30
- dependency graph
  - MSDTC agent 187
  - MSSearch agent 177
  - SQL Server 2000 agent 174
  - SQL Server 2005 agent 181
  - SQL Server Agent Service agent 183
  - SQL Server Analysis Service agent 185
- disaster recovery (DR)
  - deploying for SQL Server 2000 123
  - deploying for SQL Server 2005 128
  - illustrated 27, 122
  - protection in a SQL Server environment 121
  - rationale 120
  - setting up a secondary SQL Server 2000 site 126
  - setting up a secondary SQL Server 2005 site 132
  - typical configuration 122
- Disaster Recovery configuration 27, 122

**G**
- Global Cluster Option (GCO)
  - prerequisites 135

**I**
- installation
  - repairing 147
- installing
  - before installing SQL Server 2000 on a second node 60
  - before installing SQL Server 2005 on a second node 69
  - SQL Server 2000 on a second node (VCS) 62
  - SQL Server 2000 on the first node 58
SQL Server 2000 tasks (DR) 123
SQL Server 2000, secondary site tasks 126
SQL Server 2005 on a second node (VCS) 70
SQL Server 2005 on the first node 66, 130
SQL Server 2005 tasks (DR) 128
SQL Server 2005, secondary site tasks 132
VCS for NetApp (DR) 125
VCS for Windows (DR) 125, 129
verifying the installation 98
internal name
setting for the clustered instance (SQL 2000) 63
setting for the clustered instance (SQL 2005) 71
L
LLT over UDP
configuring using VCW 37
logging
VCW logs 151
VCWSilent logs 151
Logs
VC 150
VCS Cluster Configuration Wizard 151
VCWSilent 151
M
MSDTC
configuring the client (VCS) 97
creating an MSDTC service group 95
HA configuration overview 93
service group configuration (VCS) 93
MSDTC agent
attributes 186
operations 19
MSDTC agent attributes
LanmanResName 186
LogPath 186
MountResName 186
MSDTC service 20
MSSearch agent
attributes 176
operations 17
MSSearch agent attribute, AppName 176
MSSearch service 20
multiple SQL Server instances
assigning the port 74
P
port assignment for multiple instances 74
Q
Query Analyzer 63
R
repairing the installation 147
replication
defined 121
resource type definition
MSDTC agent 186
MSSearch agent 176
SQL Server 2000 agent 172
SQL Server 2005 agent 178
SQL Server Agent service agent 182
SQL Server Analysis Service agent 184
S
sample configurations
SQL Server (HA) 111
standalone SQL Server conversion (HA) 102
Security Services
configuring 38
service groups
administering global groups 140
SQL agent
removing 146
uninstalling 146
SQL cluster
Disaster Recovery setup 27, 122
SQL cluster configuration
Disaster Recovery 27, 122
SQL Server 2000
before installing on a second node 60
configuring the SQL Server service group 125
creating a new database 83
DR configuration overview 123
installing on a second node (HA) 62
installing on the first node 58
new installation tasks (DR) 123
overview of user-defined database 82
removing shared files 62
removing shared files on the second node 70
stopping the SQL Server service 61
tasks for setting up a secondary site 126
SQL Server 2000 database agent
configuring the SQL Server service group (Active-Active) 116
VCS for Windows
uninstalling 145, 146

MSSearch agent 17
SQL Server agent 17
SQL Server 2005
before installing on a second node 69
configuring the SQL Server service group 131
DR configuration overview 128
HA sample configuration 111
installing on a second node 70
installing on the first node 66, 130
Management Studio 71
new installation tasks (DR) 128
removing shared files 70
start a SQL Server service 71
stopping the SQL Server service 69
tasks for setting up a secondary site 132
SQL Server 2005 agent
attributes 178
SQL Server agent
attributes 172
operations 17, 18
SQL Server Agent Service agent
attributes 182
SQL Server Analysis Service agent
attributes 184
SQL Server database agent
monitoring options 21
MSDTC agent 19
SQL Server services
MSDTC 20
MSSearch 20
standalone SQL Server
configuring storage hardware and network 103
installing and configuring SFW (HA) 106
overview of HA configuration 101
preparing for conversion (HA) 104
sample HA configuration 102

U
uninstalling
SQL agent 146

V
VCS
configuring the cluster for DR 125, 129
configuring the cluster for HA 31
configuring the SQL Server service group 125, 131