# Veritas™ Cluster Server Implementation Guide for Microsoft Exchange

Windows Server 2003

5.1

# Veritas Cluster Server Implementation Guide for Microsoft Exchange



Veritas Cluster Server



Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

## 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

Veritas Cluster Server is a licensed product. See the *Veritas Cluster Server Installation 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.

# Contents

Chapter 1

# Introducing the VCS agents for Exchange and NetApp

This chapter contains the following topics:

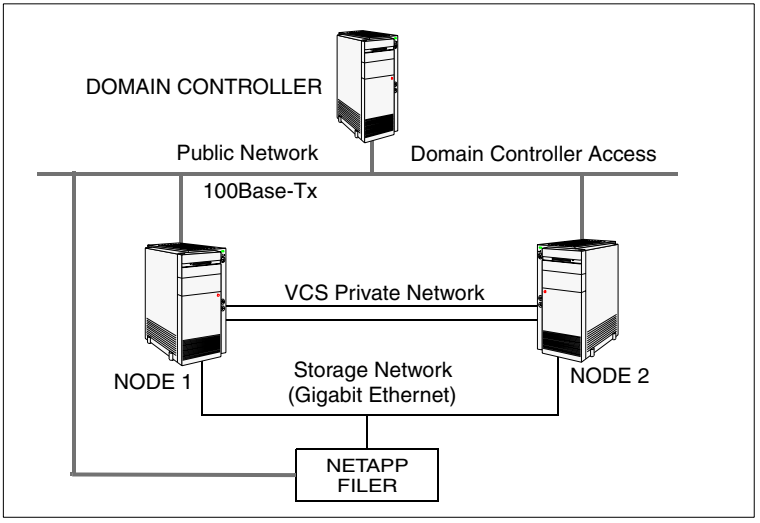
# About the VCS agents for Exchange and NetApp

The Veritas Cluster Server (VCS) application agent for Exchange provides high availability to Microsoft Exchange Server. The VCS application agent for Network Appliance (NetApp) SnapMirror enables configuring NetApp filers over an iSCSI or Fibre Channel (FC) connection in a VCS cluster environment. Both agents work together to provide high availability and disaster recovery to Exchange Server in environments using 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 on page 10 illustrates a typical VCS cluster configuration in a NetApp storage environment.

**Figure 1-1** Typical VCS configuration in a NetApp storage environment




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 127.

# VCS application agent for Microsoft Exchange

The VCS application agent for Microsoft Exchange monitors Exchange services and Exchange protocol servers in a VCS cluster, brings them online, and takes them offline.

The VCS application agent for Microsoft Exchange contains the following agents:

- Exchange Service agent—Monitors core Exchange services.
- Exchange Protocol agent—Monitors Exchange protocol servers configured under the Exchange protocol services.

Both agents work in conjunction to provide high availability for Microsoft Exchange.

## Exchange Service agent

The Exchange Service (ExchService) agent brings the following Exchange services online, monitors their status, and takes them offline:

- Microsoft Exchange System Attendant (MSExchangeSA):
  The Exchange component responsible for monitoring, maintenance and Active Directory lookup services, and ensuring that operations run smoothly.
- Microsoft Exchange Information Store (MSExchangeIS):
  The Exchange storage used to hold messages in users' mailboxes and in public folders.
- Microsoft Exchange Message Transfer Agent (MSExchangeMTA):
  The Exchange component responsible for routing messages.
- Microsoft Exchange Routing Engine (RESvc):
  The Exchange routing engine service.
- Microsoft Exchange Management Service (MSExchangeMGMT):
  Provides Exchange management information through WMI.

Each Exchange Server service is configured as a VCS resource of type ExchService.

---

**Note:** The agent does not support the Active Directory Connector and the Site Replication Service. Do not run these services on systems that are part of the VCS Exchange cluster.

---

### Agent functions

- Online—Starts the configured Exchange service.
- Offline—Stops the configured Exchange service.
- Monitor—Determines the state of the configured Exchange service by querying the Service Control Manager (SCM).
  The agent verifies the state of the enabled databases (databases that are automatically mounted when the service starts up). If an enabled database is dismounted, the agent returns UNKNOWN state.
- Action—Disables the automatic mounting of Exchange databases on the secondary site.

---

**Note:** The VCS application agent for Microsoft Exchange monitors only the enabled databases. To enable databases, run Microsoft Exchange System Manager and clear the **Do not mount this store at start-up** check box in database properties. If the agent detects that an enabled database is not mounted, it returns an UNKNOWN state for the MSExchangeIS resource. So, to dismount a database, check **Do not mount this store at start-up** and disable the database.

---

### State definition

- Online—Indicates that the configured Exchange service has started.
- Offline—Indicates that the configured Exchange service has stopped.
- Unknown—Indicates that the agent is unable to determine the state of the configured Exchange service.

## Exchange Protocol agent

The Exchange Protocol (ExchProtocol) agent starts, stops, and monitors Exchange protocol servers configured under the following Exchange protocols:

- Post Office Protocol (POP3SVC): Internet messaging protocol used to access email from a remote location.
- Simple Mail Transfer Protocol (SMTPSVC): TCP/IP protocol used to transfer email over the Internet, which is also the native mail transport protocol in Microsoft Exchange.
- Internet Message Access Protocol (IMAP4SVC): Internet messaging protocol used to access email messages stored on a remote server.
- World Wide Web (W3SVC): World Wide Web service.

The agent can monitor multiple virtual servers. Each virtual server to be monitored is configured as a VCS resource of type ExchProtocol.

### Agent functions

- Online—Starts the configured Exchange protocol servers.
- Offline—Stops the configured Exchange protocol servers.
- Monitor—Determines the state of the configured Exchange protocol servers.

### State definition

- Online—Indicates that the configured Exchange protocol server has started.
- Offline—Indicates that the configured Exchange protocol server has stopped.
- Unknown—Indicates that the agent is unable to determine the state of the configured Exchange protocol server.

## VCS hardware replication agent for Network Appliance

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 function

- 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 connectivitiy 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 functions

- 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 resynchronize the data manually.
- 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 offlining this resource is no indication of a pending role swap.

# How the agents make Microsoft Exchange highly available

The VCS application agent for Microsoft Exchange detects an application failure if a configured Exchange service is not running or if a configured virtual server is not available. The Network Appliance agents ensure consistent data access to the node on which Exchange Server is running.

This section describes how the agents migrate Exchange Server to another node in local clusters and in global disaster recovery environments.

## Local cluster configuration

When the Exchange agent detects an application or host failure, VCS attempts to fail over the Exchange service group to the next available system in the service group's SystemList.

The Network Appliance agents connects the virtual disks (LUNs) containing Exchange data to the new node. The configured Exchange services and virtual servers are started on the new node, thus ensuring continuous availability for Exchange data, including configured mailboxes.

## 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 Exchange services on the remote node (using the VCS agents for Exchange Server)

See "Managing failover in a disaster recovery environment" on page 104 for more information.

# Typical Exchange configurations in a VCS cluster

The VCS application agent for Microsoft Exchange supports the Active-Passive and the Any-to-Any configurations. It also supports the Disaster Recovery configuration.

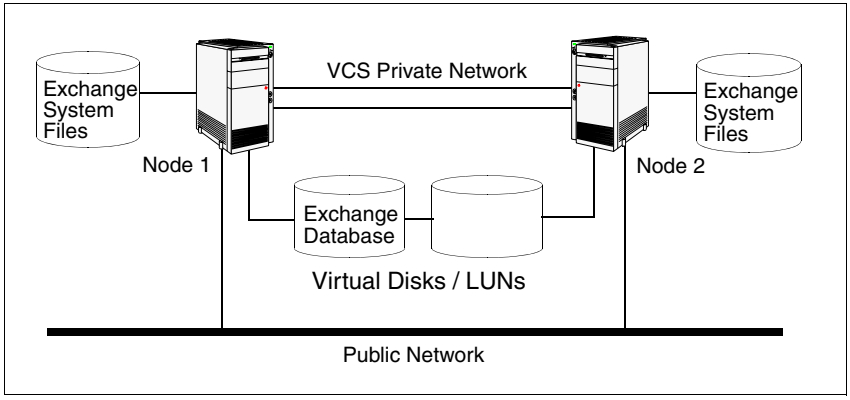
## Active-Passive failover configuration

An Active-Passive setup involves one to one failover capabilities. For example, if you have two nodes (SYSTEM1 and SYSTEM2), SYSTEM1 can fail over to SYSTEM2.

In an Active-Passive configuration, one or more Exchange virtual servers can exist in a cluster, but each server must be managed by a service group configured with a distinct set of nodes in the cluster.

In a typical two-node configuration, Microsoft Exchange and VCS application agent for Microsoft Exchange are installed on both nodes. The Exchange database is on shared storage. The shared storage can be managed using Windows Logical Disk Management or the Network Appliance suite of products.

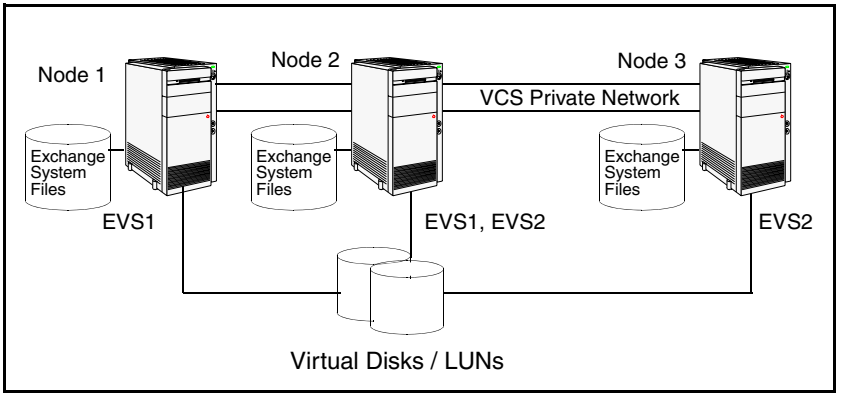
**Figure 1-2** Active-Passive fail over configuration



## Any-to-Any failover configuration

In an Any-to-Any configuration, each Exchange virtual server in the cluster can be configured in a separate service group. Each service group can fail over to any configured node in the cluster, provided that no other Exchange virtual server is online on that node. In other words, you must ensure that an Exchange service group does not fail over to a node on which another Exchange service group is online.

**Figure 1-3** Any-to-Any fail over configuration

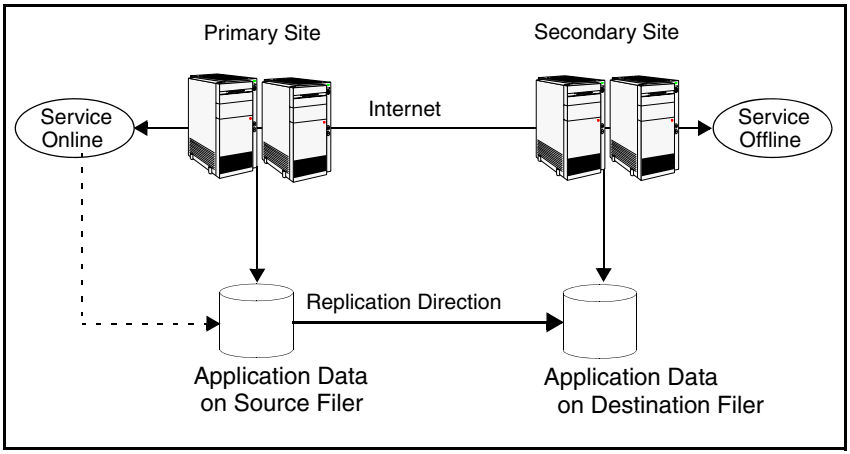



For example, consider a three-node cluster hosting two Exchange virtual servers, EVS1 and EVS2. The virtual servers are configured in VCS in two service groups such that nodes 1 and 2 host the EVS1 service group and nodes 2 and 3 host the EVS2 service group. If node 1 (or node 3) fails, the service group containing the EVS resources is failed over to node 2.

## 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** Disaster Recovery configuration




The illustration displays a disaster recovery configuration in a NetApp storage environment. In this case, the primary site is replicating its application data to the secondary site.

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

Chapter 2

# Installing the VCS agent for Exchange

This chapter contains the following topics:

# About installing the VCS application agent for Exchange

This chapter describes how to install the VCS application agent for Microsoft Exchange in a VCS cluster, provided it was not selected while installing VCS. The agent is installed using the installer for VCS. The installer installs the agent on selected systems in the cluster and adds the ExchService and the ExchProtocol resource types to the cluster configuration.

Complete these steps if you did not install the agent while installing VCS.

# Before installing the VCS agent for Exchange

This section lists the prerequisites for installing VCS application agent for Microsoft Exchange in a VCS cluster.

- Verify that you have VCS is 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

Repeat these steps on all systems where VCS application agent for Microsoft Exchange is to be installed.

### To install the agent

1. Start the installer for VCS. In the Add/Remove Programs applet, click **Veritas Cluster Server 5.1 for Windows - Server Components** and click **Change**.
2. In the Veritas Cluster Server for Windows dialog box, choose the **Add or Remove** option and click **Next**.
3. In the VCS options panel, click **Next**.
4. Check **Veritas Cluster Server Application Agent for Exchange** and click **Next**.
   The disk space required for the installation is displayed towards 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 An informational message appears if you selected the DMP option. Review the information and click **OK** to continue.

7 Review the summary of your selections and click **Update** to start the installation. The installer displays the status of installation.

8 After the installation is complete, review the installation report, click **Next** and then click **Finish**.

# Configuring the cluster

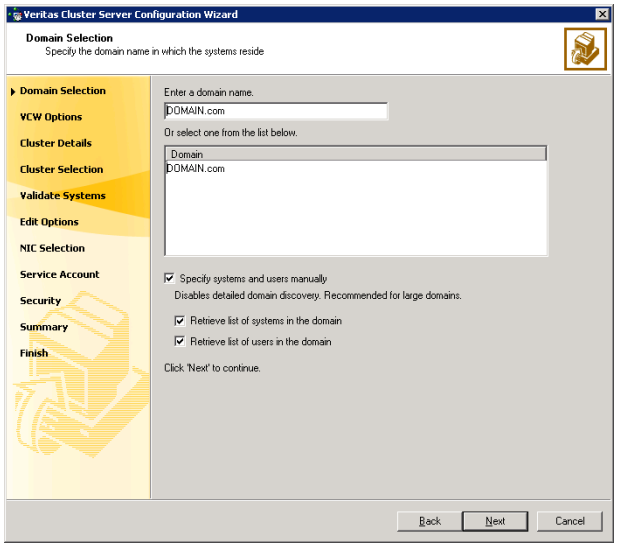
After installing the software, set up the components required to run Veritas Cluster Server. The VCS Cluster Configuration Wizard (VCW) sets up the cluster infrastructure, including LLT and GAB, and provides an option of configuring the Symantec Product Authentication Service in the cluster. The wizard also configures the ClusterService group, which contains resources for Cluster Management Console (Single Cluster Mode) also referred to as 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.



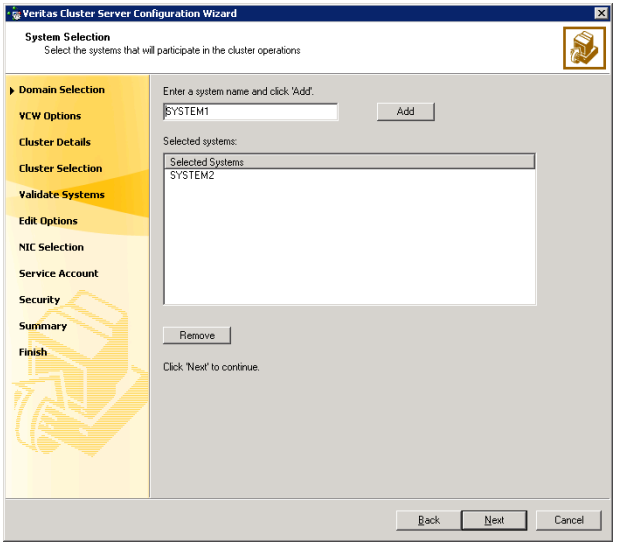

To discover information about all systems and users in the domain:

- Clear the **Specify systems and users manually** check box.
- Click **Next**.
  Proceed to step 8 on page 27.

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

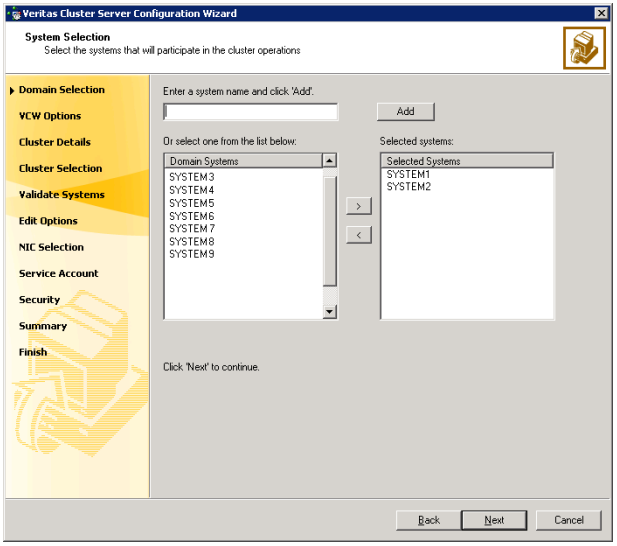
- Check the **Specify systems and users manually** check box.
  Additionally, you may instruct the wizard to retrieve a list of systems and users in the domain by selecting appropriate check boxes.
- Click **Next**.
  If you chose to retrieve the list of systems, proceed to step 6 on page 26. Otherwise, proceed to the next step.

5 On the System Selection panel, type the name of each system to be added, click **Add**, and then click **Next**. Do not specify systems that are part of another cluster.




Proceed to step 8 on page 27.

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.



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:

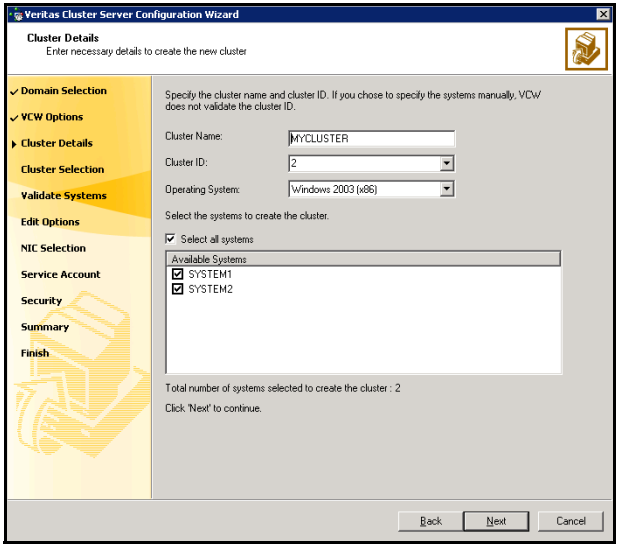
- System is not pingable.
- WMI access is disabled on the system.
- Wizard is unable to retrieve the system architecture or operating system.
- VCS is either not installed on the system or the version of VCS is different from what is installed on the system on which you are running the wizard.

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**.



| | |
|---|---|
| Cluster Name | Type a name for the new cluster. Symantec recommends a maximum length of 32 characters for the cluster name. |
| Cluster ID | Select a cluster ID from the suggested cluster IDs in the drop-down list, or type a unique ID for the cluster. The cluster ID can be any number from 0 to 255. |
| | **Caution:** If you chose to specify systems and users manually in step 4 on page 25 or if you share a private network between more than one domain, make sure that the cluster ID is unique. |
| Operating System | From the drop-down list, select the operating system that the systems are running. |
| Available Systems | Select the systems that will be part of the cluster.<br>The wizard discovers the NICs on the selected systems. For single-node clusters with the required number of NICs, the wizard prompts you to configure a private link heartbeat. In the dialog box, click **Yes** to configure a private link heartbeat.<br>Check the **Select all systems** check box to select all the systems simultaneously. |

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

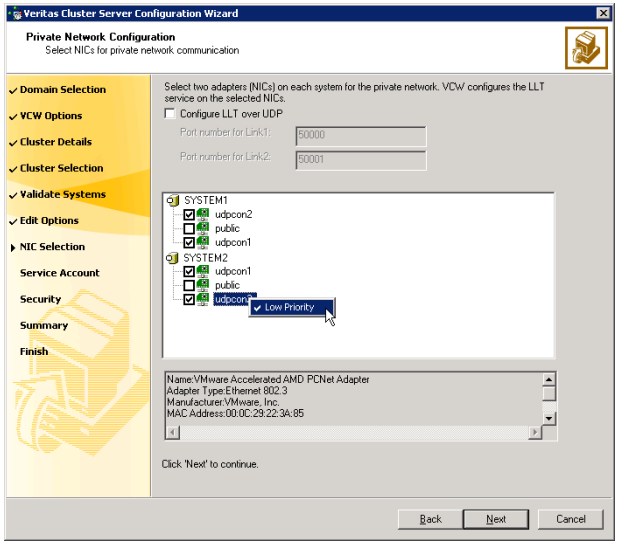
If a system is not validated, review the message associated with the failure and restart the wizard after rectifying the problem.

If you chose to configure a private link heartbeat in step 9 on page 27, proceed to the next step. Otherwise, proceed to step 12 on page 31.

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



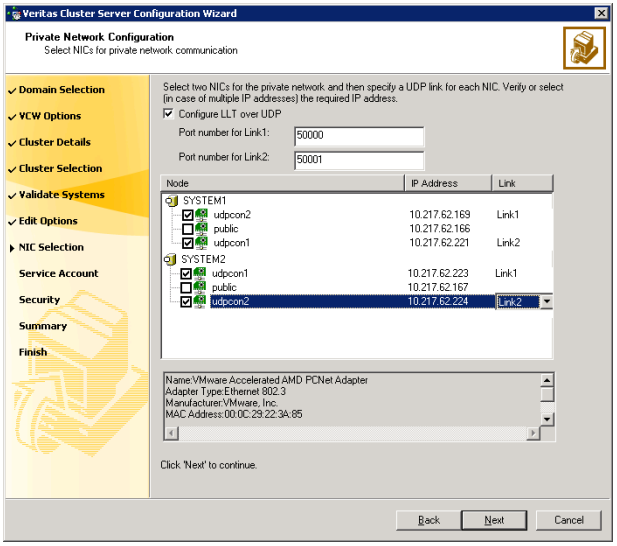

  - Select the check boxes next to the two NICs to be assigned to the private network.

    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

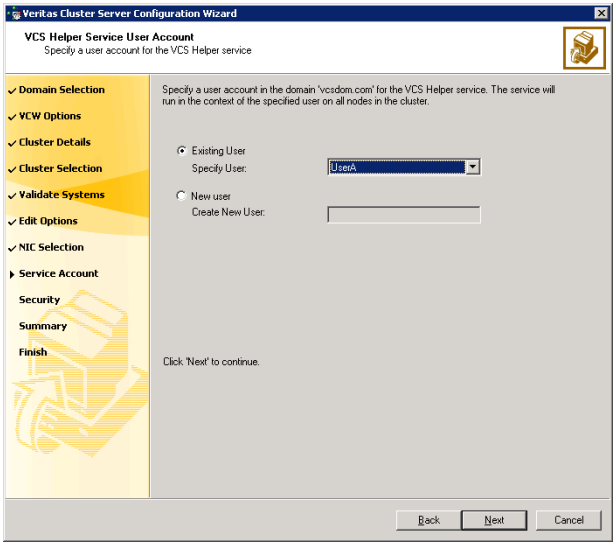



  - Check the **Configure LLT over UDP** check box.
  - Specify a unique UDP port in the **Port number for Link1** and **Port number for Link2** fields. You can use ports in the range 49152 to 65535. The default ports numbers are 50000 and 50001 respectively.
  - Select the check boxes next to the two 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.



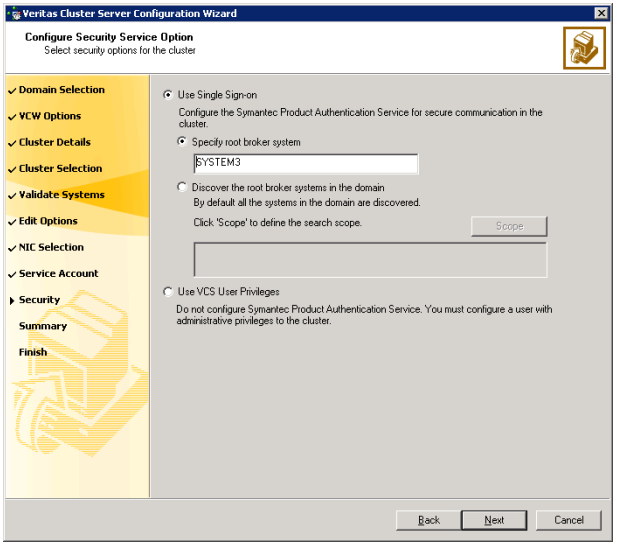

- To specify an existing user, do one of the following:
  - Click **Existing user** and select a user name from the drop-down list,
  - If you chose not to retrieve the list of users in step 4 on page 25, type the user name in the **Specify User** field, and then click **Next**.
- To specify a new user, 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.

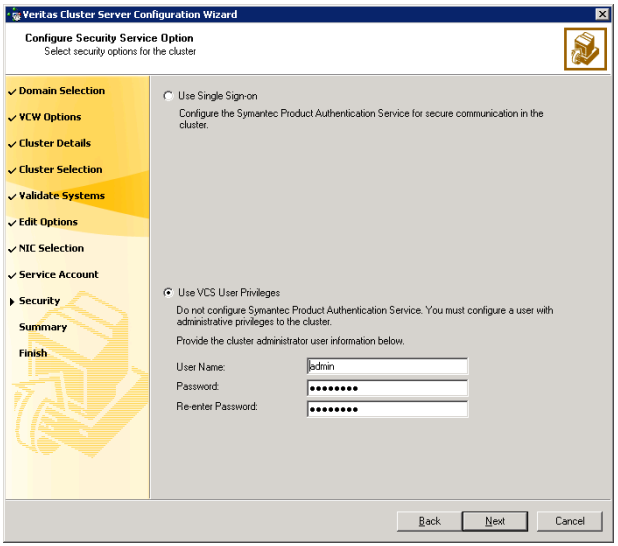
**Table 2-1** Search criteria examples

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

  You can add multiple search criterion; the wizard will search for systems that match *ALL* the conditions specified.
- Click **Next**. The wizard discovers and displays a list of all the root brokers. Click to select a system that will serve as the root broker and then click **Next**.

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

- To use 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.

---

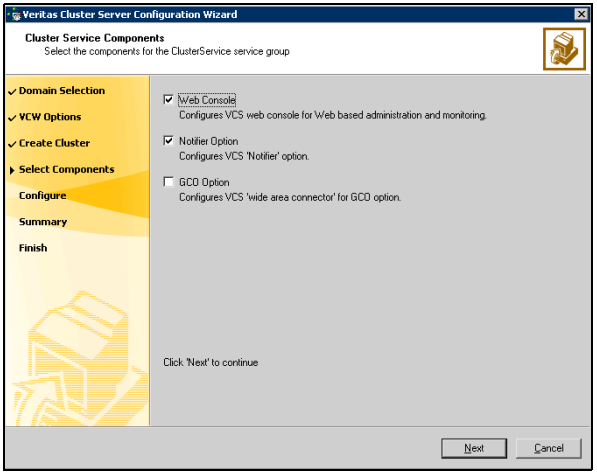
**Note:** After configuring the cluster you must not change the names of the nodes that are part of the cluster. If you wish to change a node name, run this wizard to remove the node from the cluster, rename the system, and then run this wizard again to add the system to the cluster.

---

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 36.

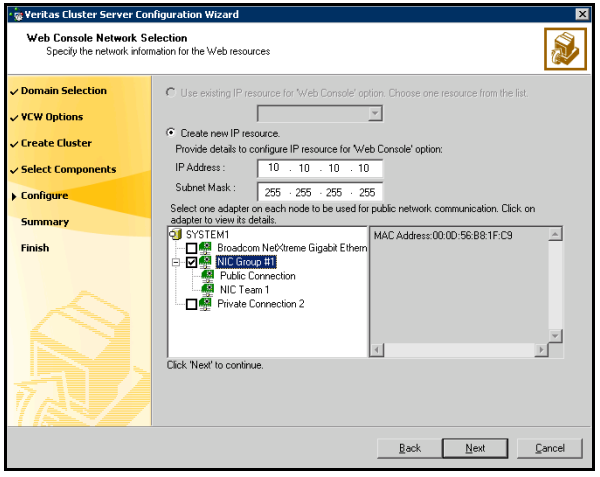
- Check the **Notifier Option** checkbox to configure notification of important events to designated recipients.
  See "Configuring notification" on page 37.

## 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**.




- 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 37.

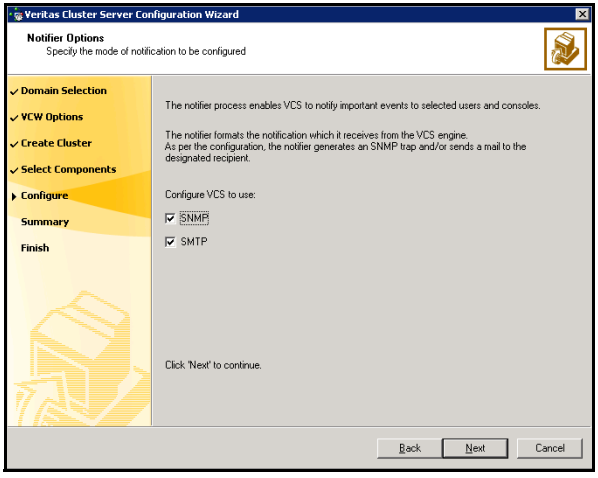
Otherwise, click **Finish** to exit the wizard.

## Configuring notification

This section describes steps to configure notification.

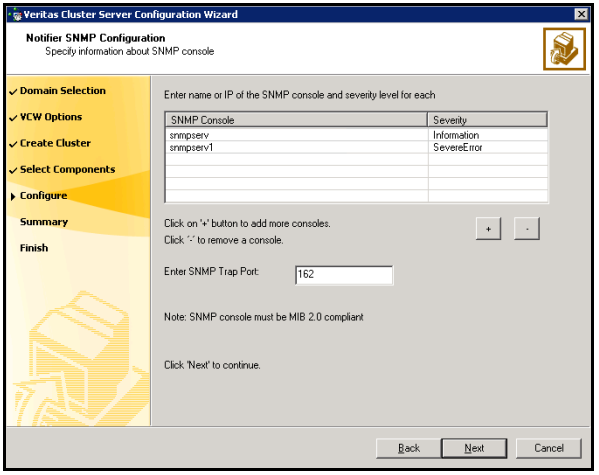
### To configure notification

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



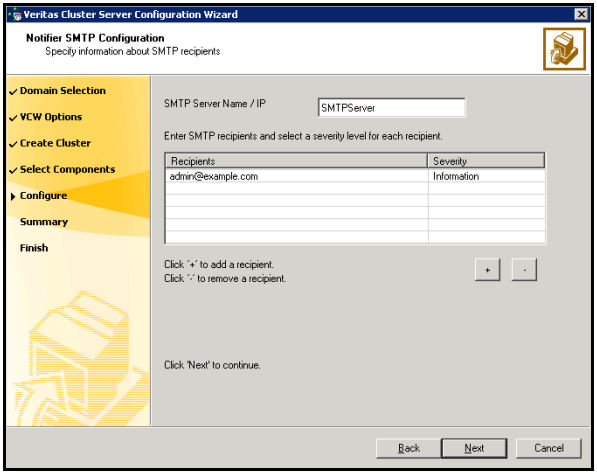

You can configure VCS to generate SNMP (V2) traps on a designated server and/or send emails to designated recipients in response to certain events.

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



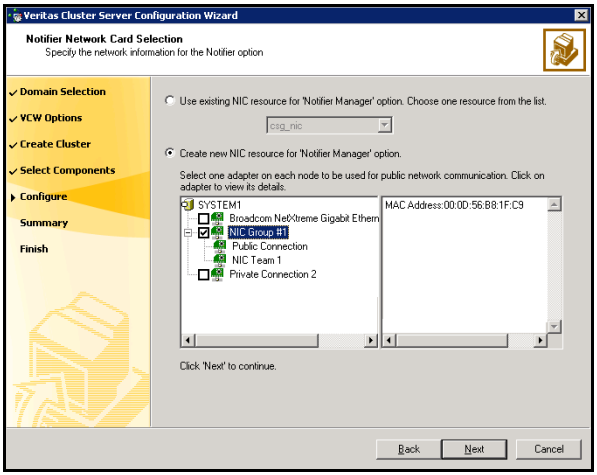

- Click a field in the SNMP Console column and type the name or IP address of the console. The specified SNMP console must be MIB 2.0 compliant.
- Click the corresponding field in the Severity column and select a severity level for the console.
- Click '**+**' to add a field; click '**-**' to remove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




- 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**.

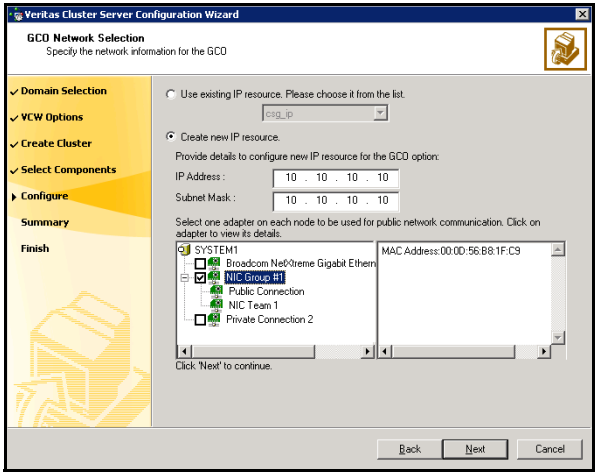
7 Click **Finish** to exit the wizard.

# Configuring Wide-Area Connector process for global clusters

Configure the wide-are 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.

Chapter 3

# Installing Microsoft Exchange

This chapter contains the following topics:

# About installing Exchange

This chapter describes how to install and configure Microsoft Exchange and its components in a VCS cluster.

---

**Note:** If you have a standalone Exchange Server setup and you want to configure it for high availability, see "Making a standalone Exchange server highly available" on page 79 for instructions.

---

# Before installing Exchange

- Verify VCS is installed on the node.
- Verify you have configured a VCS cluster using VCS Cluster Configuration Wizard (VCW).
  See "Configuring the cluster" on page 24.
- Verify the DNS and Active Directory Services are available. Make sure that a reverse lookup zone is created in the DNS. Refer to Microsoft Exchange documentation for instructions on creating a reverse lookup zone.
- Symantec recommends that the Dynamic Update option for the DNS server be set to "Secure Only."
- Verify the DNS settings for all systems on which Microsoft Exchange will be installed.
  See "Verifying DNS settings for Exchange hosts" on page 46.
- Verify that all systems on which Microsoft Exchange server is to be installed have IIS installed; the SMTP, NNTP, and WWW services must be installed on all systems. For installing Exchange on Windows Server 2003, ASP.NET service must also be installed.
- VCS requires Microsoft Exchange to be installed on the same local drive on all nodes. For example if you install Exchange on drive C of one node, installations on all other nodes must be on their respective C drives. Make sure that the same drive letter is available on all nodes and has adequate space for the installation.
- Before installing Microsoft Exchange in a VCS cluster, make sure that the forest and the domain have been prepared. See the Microsoft Exchange documentation for instructions.
- If using iSCSI, verify that the Microsoft iSCSI Initiator is configured to establish a persistent connection between the NetApp filer and the cluster nodes. See the Microsoft documentation for instructions.

- If using FC, verify that you install the NetApp FCP Attach Kit or Windows Host Utilities on all the cluster nodes. Refer to the NetApp documentation for more information.
- Symantec recommends that you create a minimum of two volumes or LUNs (virtual disks), one each for the following:
  - Exchange database
  - MTA data, transaction logs for the first storage group, and registry replication information.

## Privileges requirements

- You must be a domain user.
- You must be an Exchange Full Administrator.
- You must be a member of the Exchange Domain Servers group.
- You must be a member of the Local Administrators group on all nodes on which Microsoft Exchange will be installed. You must have write permissions for objects corresponding to these nodes in the Active Directory.
- You must have write permissions on the DNS server to perform DNS updates.
- You must be an Enterprise Administrator, Schema Administrator, Domain Administrator, or Local Administrator to run ForestPrep; you must be a Domain Administrator or Local Administrator to run DomainPrep. Refer to the Microsoft documentation for permissions requirements during Microsoft procedures that do not involve Symantec wizards.
- Make sure the VCS Helper Service domain admin user account has “Add workstations to domain” privilege enabled in the Active Directory.
- If a computer object corresponding to the Exchange virtual server exists in the Active Directory, you must have Delete permissions on the object.
- The same user, or a user with the same privileges must perform the pre-installation, installation, and post-installation phases for Microsoft Exchange.

## Verifying DNS settings for Exchange hosts

1. Open the Network Connections applet in Control Panel.
2. Double-click the adapter.
   When enabling DNS name resolution, make sure that you use the public network adapters, and not those configured for the VCS private network.
3. From the Local Area Connection Status window, click **Properties**.
4. On the **General** tab, check the **Internet Protocol (TCP/IP)** check box and click **Properties**.
5. Select the **Use the following DNS server addresses** option.
6. Verify that the correct values for the DNS server's IP address and domain name are entered.
7. Click **Advanced**.
8. On the **DNS** tab, make sure the **Register this connection's address in DNS** check box is selected.
9. Make sure the correct domain suffix is entered in the **DNS suffix for this connection** field.

## 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 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 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**.

## Preparing the Forest and the Domain

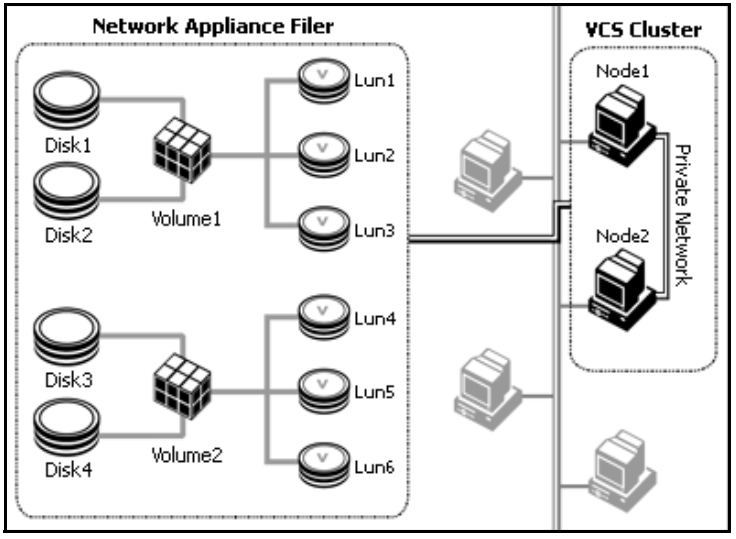
Before installing Microsoft Exchange in a VCS cluster, make sure that the forest and the domain have been prepared. See the Microsoft Exchange documentation for instructions. Do not repeat this process for additional Exchange installations.

# Managing storage using Network Appliance filer

Network Appliance manages data by creating volumes on physical disks. These volumes can further be divided into LUNs (Logical Unit Numbers.) 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 application agent for Microsoft Exchange requires two LUNs to be created on the NetApp filer, one for Exchange data and the other for MTA data, transaction logs, and registry replication information. These LUNs must be accessible from all cluster nodes.

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 NetApp filer, they must be connected (if not connected already) to the cluster nodes using NetApp 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. (**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

Steps to disconnect the virtual disks from a cluster node.

**To disconnect virtual disks**

1. Start the Computer Management MMC on the cluster node where you want to disconnect the LUN. (**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*.

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

- Reserve disks. See "Reserving disks (if you use Windows LDM)" on page 51.
- Create volumes. See "Creating volumes (if you use Windows LDM)" on page 51.
- Mount volumes. See "Mounting volumes (if you use Windows LDM)" on page 51.

## About LDM support

The following restrictions apply in this release:

- Disk Reservation and Mount agents are supported on VCS 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 Exchange.

**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 Exchange, and configuring the Exchange 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.

## Releasing disks (if you use Windows LDM)

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

```
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 may require these details to identify and reserve the disks later.

## 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.
   ```
   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.

---

# Installing Exchange on the first node

The tasks to be performed on the first node are described in three stages.

## Exchange pre-installation: first node

Use the Exchange Server Setup Wizard for Veritas Cluster Server to complete the pre-installation phase. This process changes the physical name of the node to a virtual name.

**Note:** After you have run the wizard, you will be prompted to restart the node. So, close all open applications and save your data before running the wizard.

**To perform Exchange pre-installation**

1. Verify the volumes or LUN created to store the registry replication information is mounted on or connected to this node and dismounted or disconnected from other nodes in the cluster.
2. Start the Exchange Server Setup Wizard for VCS. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange Server Setup Wizard**.
3. Review the information in the Welcome panel and click **Next**.
4. On the Available Option panel, click **Install Exchange Server for High Availability** and click **Next**.
5. On the Select Option panel, click **Create New Exchange Virtual Server** and click **Next**.
6. Specify network information for the Exchange virtual server.
   - Enter a unique virtual name for the Exchange server.
     Once you have assigned a virtual name to the Exchange server, you cannot change the virtual name later. To change the virtual name, you must uninstall Exchange Server from the VCS environment and reinstall it using the Exchange Server Setup Wizard for VCS.
   - Enter the name of a domain suffix for the Exchange server.
   - Select the appropriate public NIC from the drop-down list.
     The wizard lists the public adapters and low-priority TCP/IP enabled private adapters on the system.
   - Enter a unique virtual IP address for the Exchange server.
   - Enter the subnet mask for the virtual IP address.
   - Click **Next**.

7 Select a drive where the registry replication data will be stored and click **Next**.

8 Review the summary of your selections and click **Next**.

9 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

10 The wizard starts running commands to set up the VCS environment. Various messages indicate the status of each task. After all the commands are executed, click **Next**.

11 Click **Reboot**.

When prompted to reboot the node, click **Yes**.

After you reboot the node, the value specified for the Exchange virtual server is temporarily assigned to the node. So, all network connections to the node must be made using the temporary name. Review the information in the wizard dialog box and proceed to installing Microsoft Exchange Server.

After installing Microsoft Exchange and rebooting the node, the Exchange Setup Wizard for VCS is launched automatically. The wizard will assign the original name to the node.

See "Exchange Server installation: first node" on page 55 for instructions.

Click **Revert** to undo all actions performed by the wizard during the pre-installation procedure.

# Exchange Server installation: first node

Install Exchange on the node where the Exchange Server Setup Wizard was run for the pre-installation tasks.

### To install Exchange

1. Install Exchange Server using the Microsoft Exchange installation program. Make sure you install the Microsoft Exchange System Management Tools also. See the Microsoft Exchange documentation for instructions.
2. Reboot the node if prompted to do so.
3. For Exchange 2003, install service packs listed in the requirements.

# Exchange post-installation: first node

After completing the installation, use the Exchange Server Setup Wizard to complete the post-installation tasks. This process reverts the node name to original name and sets the startup type of the Exchange services to manual, so that they can be controlled by VCS.

### To perform Exchange post-installation

1. Make sure that the Veritas High Availability Engine (HAD) is running on the node on which you plan to perform the post-installation tasks.
   Type the following on the command line:
   ```
   C:\>hasys -state
   ```
   The state should display as RUNNING.
   If HAD is not running, start it. Type the following on the command line:
   ```
   C:\>net stop had
   C:\>net start had
   ```
2. Make sure that the volume or LUN containing the registry replication information is mounted on or connected to the node on which you will perform the post-installation.
3. If the Exchange installation did not prompt you to reboot the node, click **Continue** from the Exchange Server Setup Wizard and proceed to step 5.
   If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.
4. Review the information in the Welcome panel and click **Next**.
5. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue. This sets the node name back to its physical host name.

6 The wizard starts performing the post-installation tasks. Various messages indicate the status. After all the commands are executed, click **Next**.

7 Click **Finish**.

8 When prompted to reboot the node, click **Yes**.
Changes made during the post-installation phase do not take effect till you reboot the node.
Once the node is rebooted, move the databases created during the Exchange installation from the local drive to the shared storage.

# Moving Exchange databases to shared storage

After completing Microsoft Exchange installation on the first node, move the Exchange databases on the local drive of the first node to a location on shared storage.

Complete the following tasks before moving the databases:

- Make sure that there is no queued data on the SMTP server.
- Make sure that the volumes or LUNs created to store the Exchange database, MTA data, transaction logs, and registry replication information are connected. Disconnect the volumes or LUNs from other systems in the cluster.

### To move Exchange database to a shared storage

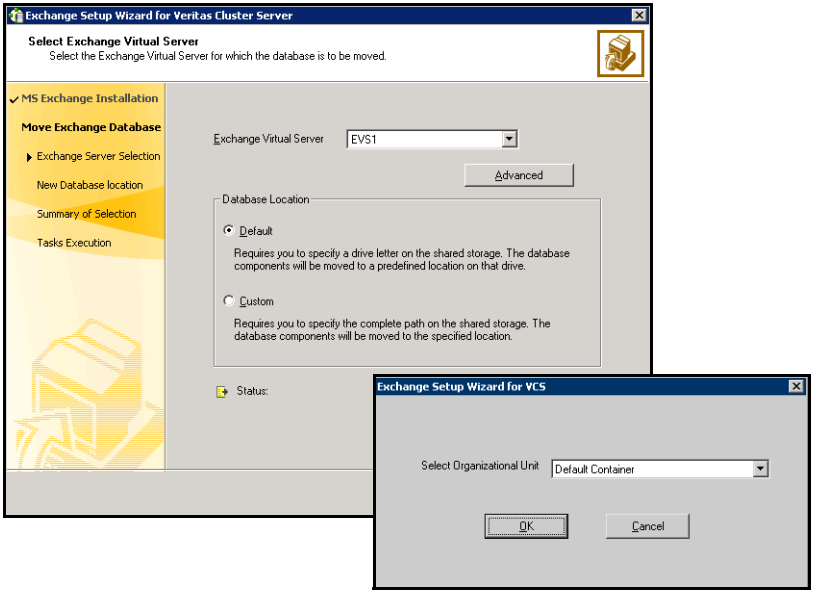
1 Start the Exchange Server Setup Wizard for VCS. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.

2 Review the information in the Welcome panel and click **Next**.

3 In the Available Option panel, click **Configure/Remove highly available Exchange Server** and click **Next**.

4 In the Select Option panel, click **Move Exchange Databases** and click **Next**.

5 In the Select Exchange Virtual Server panel, select the Exchange virtual server and specify whether you want to move the Exchange databases to a default or a custom location and click **Next**.




Exchange Virtual Server

From the drop-down list, select the Exchange virtual server for which you want to move the database components.

Advanced

To specify the Lanman resource details:

1. Click **Advanced**.
2. From the Organizational Unit drop-down list, select the distinguished name for the Exchange 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
3. Click **OK**.

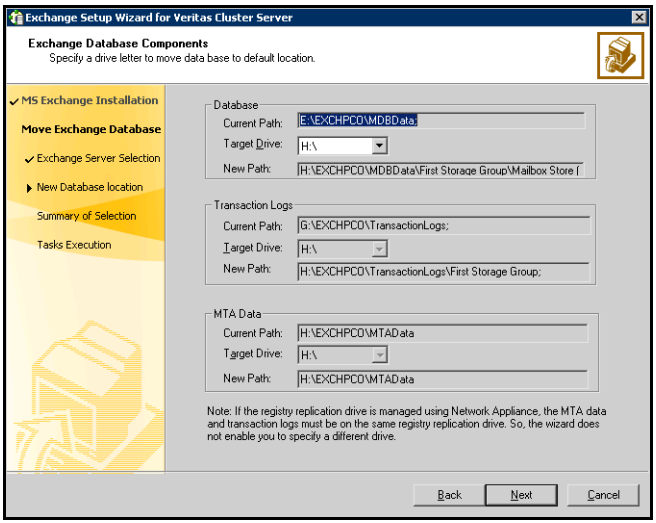
Default

Select this option if you want to move the database to a default location on the shared storage.
After you click **Next**, the wizard prompts you for the drive letter on the shared storage. The database components will be moved to a pre-defined location on the drive letter that you select.

| | |
|---|---|
| Custom | Select this option if you want to move the database to a custom location on the shared disk.<br>After you click **Next**, the wizard prompts you for the drive letter and the complete path on the shared storage. The database components will be moved to the location that you specify. |

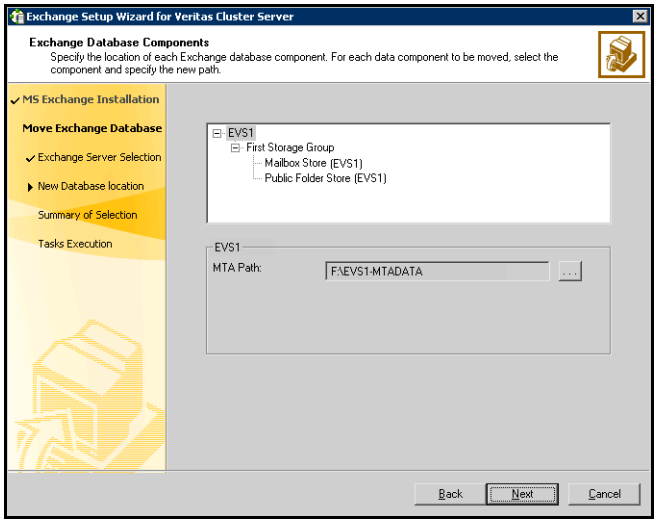
6 On the Exchange Database Components panel, complete the following and then click **Next**.

- If you chose to move the Exchange database to a default location:




- For the Exchange database, select a drive letter from the respective drop-down list.
- The Transaction Logs and MTA Data components will be moved to the drive that you specified for storing the registry replication information, during the Exchange pre-installation phase.

- If you chose to move the Exchange database to a custom location:




  - For each data component to be moved, select the component and specify the path to designate the new location of the component. Click **...** (ellipsis button) to browse for folders.

    For Transaction logs and MTA Data, you must select the drive that you specified for storing the registry replication information, during the Exchange pre-installation phase.

  Make sure the path for the Exchange database components contains only ANSI characters.

7 Review the summary of your selections and click **Next**.

8 The wizard starts performing tasks to move the Exchange databases. Various messages indicate the status of each task. After all the tasks are complete, click **Next**.

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

# Installing Exchange on additional nodes

After moving the Exchange databases to shared storage, install Exchange on additional nodes in the cluster for the same Exchange virtual server. You must run the pre-installation, installation, and post-installation procedures on each additional node.

## Exchange pre-installation: additional nodes

Use the Exchange Server Setup Wizard for Veritas Cluster Server to complete the pre-installation phase. This process changes the physical name of the node to a virtual name.

Before adding a node to the Exchange cluster, make sure you meet the prerequisites listed under "Before installing Exchange" on page 44.

### To perform Exchange pre-installation

1. Verify the volumes or LUN created to store the registry replication information is mounted or connected to this node and dismounted or disconnected from other nodes in the cluster.
2. Start the Exchange Server Setup Wizard for VCS from the node to be added to an Exchange cluster. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.
3. Review the information in the Welcome panel and click **Next**.
4. In the Available Option panel, click **Install Exchange Server for High Availability** and click **Next**.
5. In the Select Option panel, click **Create a failover node for existing Exchange Virtual Server** and click **Next**.
6. Select the Exchange virtual server for which you are adding the failover node and click **Next**.
7. The wizard validates the system for the prerequisites. Various messages indicate the validation status. Once all the validations are done, click **Next**.
8. Specify network information for the Exchange virtual server.
   The wizard discovers the Exchange virtual server name and the domain suffix from the Exchange configuration. Verify this information and provide values for the remaining text boxes.
   - Select the appropriate public NIC from the drop-down list.
     The wizard lists the public adapters and low-priority TCP/IP enabled private adapters on the system.

- Enter the virtual IP address for the Exchange virtual server. By default, the text box displays the IP address that you specified during Exchange pre-installation phase, while creating a new Exchange cluster.
- Enter the subnet mask for the virtual IP address.
- Click **Next**.

9 Review the summary of your selections and click **Next**.

10 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

11 The wizard starts running commands to set up the VCS environment. Various messages indicate the status of each task. After all the commands are executed, click **Next**.

12 Click **Reboot**.

The wizard prompts you to reboot the node. Click **Yes**.

---

**Warning:** After you reboot the node, the value specified for the Exchange virtual server is temporarily assigned to the node. So, all network connections to the node must be made using the temporary name. After installing Microsoft Exchange, you must rerun this wizard to assign the original name to the node.

---

On rebooting the node, the Exchange Server Setup Wizard is launched automatically. Review the information in the wizard dialog box and proceed to installing Microsoft Exchange Server.

See "Exchange Server installation: additional nodes" on page 62 for instructions.

Click **Revert Changes** to undo all actions performed by the wizard during the pre-installation procedure.

Do not click **Continue** at this time. Wait until after the Exchange installation is complete.

# Exchange Server installation: additional nodes

Install Exchange on the node where the Exchange Server Setup Wizard was run for the pre-installation tasks.

This is a standard Microsoft Exchange Server installation. Refer to the Microsoft documentation for details on this installation.

- Install any required service packs.
- Install the same Exchange version and components on all nodes.

The procedure below is based on Exchange 2003. This is a standard Microsoft Exchange Server installation. Refer to the Microsoft documentation for details on this installation.

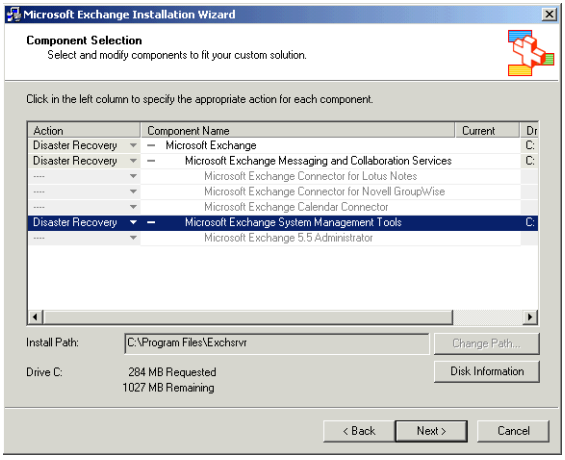
### To install Exchange

1. Begin the Exchange installation for disaster recovery at the command prompt using the /disasterrecovery option :

   ***<drive letter>***`:\SETUP\I386\setup.exe /disasterrecovery`

   where ***<drive letter>*** is the location where the Exchange software is located.

2. During the wizard, verify or select **Disaster Recovery** in the **Action** column for the Microsoft Exchange, Microsoft Exchange Messaging and Collaboration services and Microsoft Exchange System Management Tools components. Be sure to install the same components on all the nodes in the cluster.



3 When notified to restore databases from backup and reboot the node after completing the installation, click **OK** and complete the Microsoft Exchange wizard.

4 If prompted to reboot the node, click **Yes**.

5 For Exchange 2003, install the service packs listed in the requirements. When installing service packs enter the following from the command line:

```
SETUP\I386\update.exe /disasterrecovery
```

## Exchange post-installation: additional nodes

After completing the Microsoft Exchange installation, use the Exchange Server Setup Wizard to complete the post-installation tasks. This process reverts the node name to original name.

### To run the Exchange post-installation

1 Make sure that the Veritas High Availability Engine (HAD) is running on the node on which you plan to perform the post-installation tasks.

Type the following on the command line:

```
C:\>hasys -state
```

The state should display as RUNNING.

If HAD is not running, start it. Type the following on the command line:

```
C:\>net stop had
C:\>net start had
```

2 Make sure that the volumes or LUN containing the registry replication information is mounted or connected to the node on which you will perform the post-installation.

3 If the Exchange installation did not prompt you to reboot the node, click **Continue** from the Exchange Server Setup Wizard and proceed to step 5.

If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.

4 Review the information in the Welcome panel and click **Next**.

5 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

6 The wizard starts performing the post-installation tasks. After all commands are executed, click **Next**.

7 Specify whether you want to add the node to the SystemList of the service group for the EVS selected in the Exchange pre-installation step.

Select this option only if service groups are already configured for the EVS.

If you wish to add the nodes later, you can do so by using the Exchange service group Configuration Wizard.

8 Click **Finish**.

9 The wizard prompts you to reboot the node. Click **Yes**.
Changes made during the post-installation steps do not take effect till you reboot the node.

# Configuring stores to mount on start-up

Run the Exchange System Manager so that all the stores that were previously mounted are automatically mounted on start-up.

**To reconfigure mounting of stores at start-up**

1 Start Exchange System Manager.

2 In the left pane, navigate to your storage group.
If you have only one administrative group, expand **Servers >** ***Exchange Server*** **>** ***Storage Group***.
If you have more than one administrative groups, expand **Administrative Groups >** ***Your Administrative Group*** **> Servers >** ***Exchange Server*** **>** ***Storage Group***.

3 Right-click the Exchange database and choose **Properties** from the pop-up menu.

4 Click the **Database** tab.

5 Clear the **Do not mount this store at start-up** check box.

6 Click **OK**.

Repeat these steps for all the Exchange databases that were previously mounted.

Chapter 4

# Configuring the Exchange service group

This chapter contains the following topics:

# About configuring the service group

Configuring the Exchange service group involves creating the required VCS resources for Exchange. VCS provides several ways of configuring a service group, including the service group configuration wizard, Cluster Manager (Java Console), Cluster Management Console, and the command line. This chapter provides instructions on configuring an Exchange service group using the Exchange Server Configuration Wizard.

# Configuring the service group using the wizard

The Exchange Server Configuration Wizard guides you through the process of configuring an Exchange service group. You can also create and modify Exchange service groups using the wizard.

This section describes how to create a new Exchange service group using the wizard. To modify an existing service group, see "Modifying the service group configuration" on page 77.

Review the resource types and the attribute definitions of the agents before configuring the agents. See "Resource type definitions" on page 127.

For sample configuration files and resource dependency graphs of the Exchange service group, see "Sample configuration" on page 135.

## Before configuring the Exchange service group

- Verify VCS is installed on all cluster nodes. Refer to the *Veritas Cluster Server Install and Upgrade Guide*.
- Verify the cluster is configured using the VCS Cluster Configuration Wizard (VCW).
  See "Configuring the cluster" on page 24.
- Verify Exchange is installed and configured identically on all the cluster nodes.
  See Chapter 3, "Installing Microsoft Exchange" on page 43.
- Verify your DNS server settings. Make sure a static DNS entry maps the virtual IP address with the virtual computer name.
- You must be a Cluster Administrator to create and configure service groups.
- You must be a Local Administrator on the node where you run the wizard.
- You must be an Administrator for the NetApp Filer containing the LUNs created to store Exchange data components.
- Verify the Command Server is running on all systems in the cluster.

- Verify the Veritas High Availability Daemon (HAD) is running on the system from where you run the wizard.
- Verify the volumes or the virtual disks (LUNs) 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.
  - Exchange database
  - MTA data, transaction logs for the first storage group, and registry replication information.

  See "Managing storage using Network Appliance filer" on page 48 for instructions.

  See for "Managing storage using Windows Logical Disk Manager" on page 50 for instructions.
- Verify your DNS server settings. Make sure a static DNS entry maps the virtual IP address with the virtual computer name. Refer to the appropriate DNS documentation for further information.
- 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*.

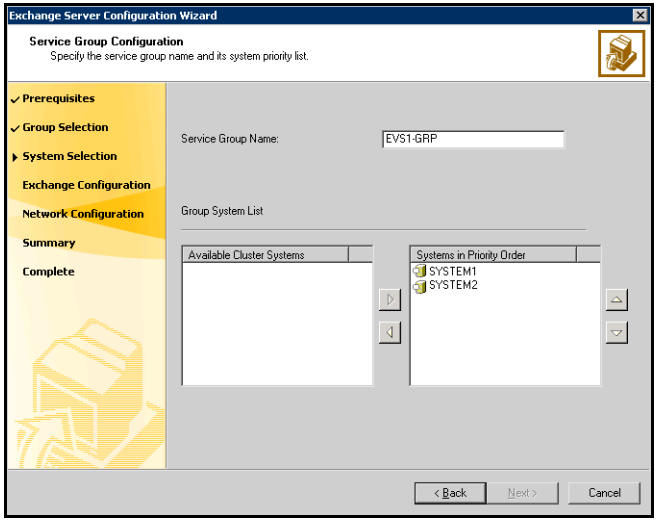
## Configuration instructions

The following steps describe how to configure an Exchange service group using the configuration wizard.

**To configure an Exchange service group**

1. Start the Exchange Server Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange Server Configuration Wizard**.
2. Review the information in the Welcome panel and click **Next**.
3. In the Wizard Options panel, click **Create service group** and click **Next**.
4. On the Service Group Configuration panel, specify the service group name and the systems that will part of the service group and click **Next**. The

wizard starts validating your configuration. Various messages indicate the validation status.

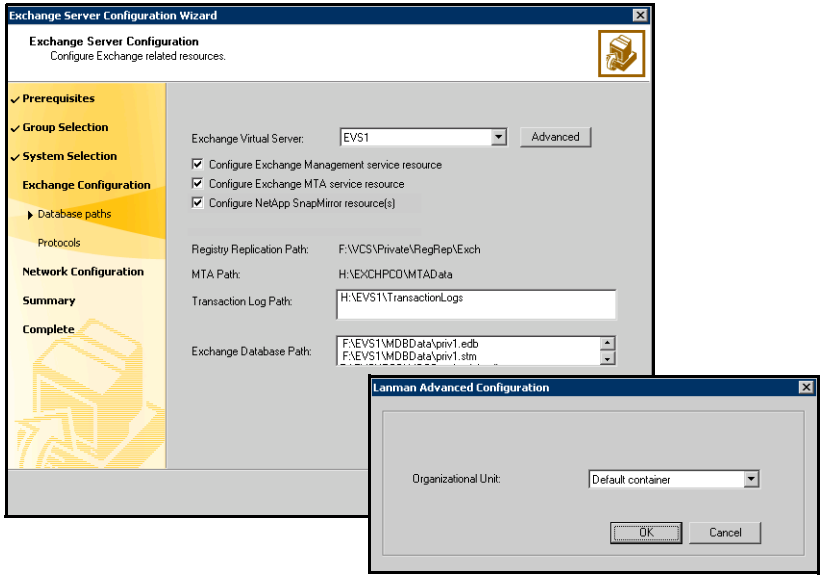



| | |
|---|---|
| Service Group Name | Type a name for the Exchange service group. If you are configuring the service group on the secondary site, ensure that the name matches the service group name on the primary site. |
| Available Cluster Systems | Select the systems on which to configure the service group and click the right-arrow to move the systems to the Systems in Priority Order box. |
| Systems in Priority Order | This list represents the service group's system list. To remove a system from the service group's system list, select the a system and click the left arrow. To change a system's priority in the service group's system list, select the system 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. |

**Note:** Microsoft Exchange Server and Microsoft SQL Server can exist in the same cluster but cannot run on or fail over to the same system. If a SQL Server service group is configured in the cluster, make sure to select a distinct set of systems in the SystemList attribute for each application's service group.

5 On the Exchange Server Configuration panel, verify the Exchange virtual server name and paths to the LUNs created to store Exchange data, and then click **Next**.

An informational message appears if you chose to configure a SnapMirror resource without configuring replication between Network Appliance filers at primary and secondary sites. Review the message and click **Yes** to continue. You must always click **Yes** if you encounter this message while configuring a service group at the secondary site.

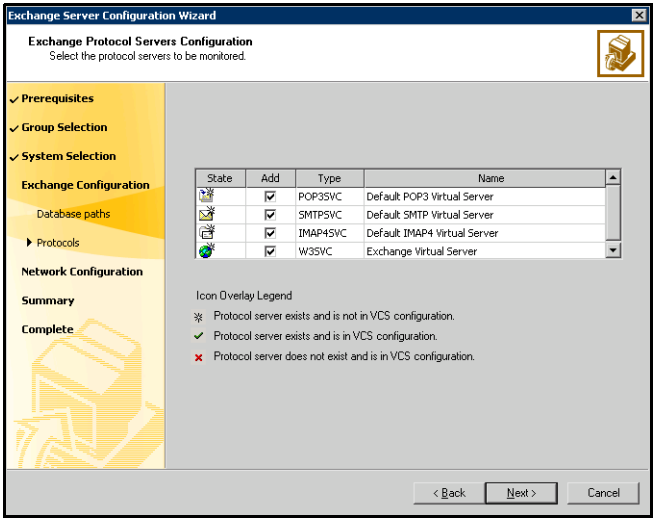



| | |
|---|---|
| Exchange Virtual Server | From the drop-down list, select the Exchange virtual server for which you wish to configure the service group. |

| | |
|---|---|
| Advanced | To specify the Lanman resource details:<br>1 Click **Advanced**.<br>2 From the Organizational Unit drop-down list, select the distinguished name for the Exchange virtual server.<br>By default, the Lanman resource adds the virtual server to the default container Computers.<br>The user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts<br>3 Click **OK**. |
| Configure Exchange Management service resource | Check this check box if you want to configure the Exchange Management service resource.<br>If you are running the wizard to modify a service group, unchecking this check box will remove the Exchange Management service resource from the service group configuration. |
| Configure Exchange MTA service resource | Check this check box if you want to configure the Exchange Message Transfer Agent (MTA) service resource.<br>If you are running the wizard to modify a service group, unchecking this check box will remove the Exchange MTA service resource from the service group configuration. |
| Configure NetApp SnapMirror resource(s) | Check this check box if you want to configure a NetApp SnapMirror resource. SnapMirror resource is required only in case of a disaster recovery configuration.<br>If you are running the wizard to modify a service group, unchecking this check box will remove the NetApp SnapMirror resource from the service group configuration. |
| Registry Replication Path | Verify the registry replication path for the selected Exchange virtual server. |
| MTA Path | Verify the MTA path for the selected Exchange virtual server. |
| Transaction Log Path | Verify the Transaction Log path for the selected Exchange virtual server. |
| Exchange Database Path | Verify the Exchange database path for the selected Exchange virtual server. |

- To configure additional storage, click **Configure...**. On the Additional Storage Configuration dialog box, complete the following:
  - In the Available Volumes box, select a volume that you wish to add and click the right-arrow button to move the volume to the Selected Volumes box.
  - To remove a volume, select the volume in the Selected Volumes box, and click the left-arrow button.
  - Click **OK**. The wizard will configure resources required for the additional storage as child resources of the Microsoft Exchange System Attendant (MSExchangeSA) service resource.

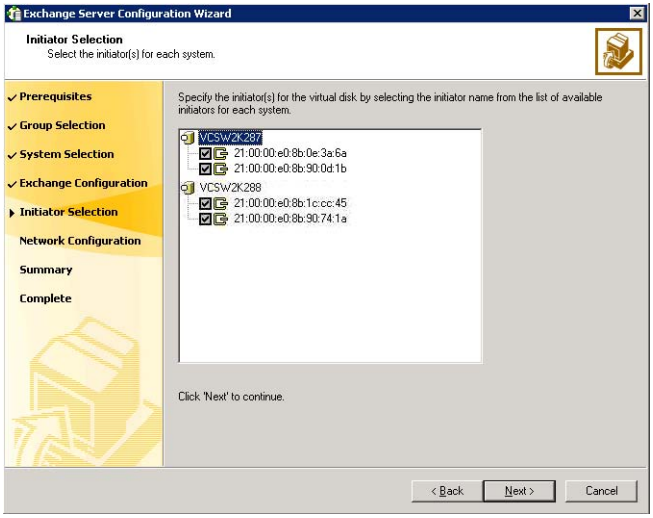
6 On the Exchange Protocols Servers Configuration panel, check the protocol check boxes next to the protocol servers to be monitored and click **Next**.



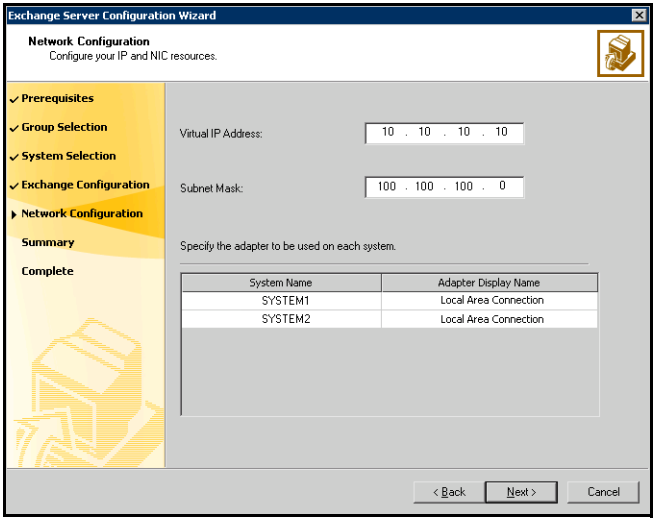

7 On the Initiator Selection panel, select the initiator(s) for the virtual disk from the list of available initiators displayed for each cluster node, and then click **Next**.

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 On the Network Configuration panel, specify the following network related information and then click **Next**.




- The Virtual IP Address and the Subnet Mask fields display the values entered while installing Exchange. You can keep the displayed values or type new values.

If you change the virtual IP address, create a static entry in the DNS server mapping the new virtual IP address to the virtual server name.

- 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 node.

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.

9 Review the service group configuration, change the resource names, if desired, and then click **Next**.

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. To edit a resource name, select the resource, click the resource or press the F2 key. Edit the resource, and press the Enter key to confirm the changes. To cancel editing a resource name, press the Esc key.

10 Click **Yes** on the message that prompts you that the wizard will run commands to modify the service group configuration. Various messages indicate the status of these commands.

11 In the Completing the Exchange Configuration panel, check the **Bring the service group online** check box to bring the service group online on the local node and click **Finish**.

After bringing the service group online, run the Exchange System Manager to modify the database settings such that all the stores are automatically mounted on start-up.

If you need to configure additional storage groups or mailbox stores on the shared storage you should do that now. Mount or connect the volumes or LUNs that have been created for the additional storage groups and mailbox stores, and then create the new storage groups and mailbox stores. Run the Exchange Configuration Wizard again to bring them under VCS control.

If you already designated the additional volumes or LUNs when you ran the configuration wizard the first time, then you can just create the storage groups and mailbox stores.

# Running SnapManager for Exchange

Run the SnapManager configuration wizard on the node on which the service group is online to complete the configuration process and to schedule backups of the Exchange database. You must adhere to the following requirements while running SnapManager for Exchange:

- Make sure the Exchange service group is online.
- Do not move the Exchange database components already moved using the Exchange Server Setup Wizard.

If you are scheduling backups in a VCS cluster, schedule them on the node on which the service group is online. If the Exchange virtual server 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 Exchange.

# Verifying the service group configuration

This section provides steps to verify a service group configuration by bringing the service group online, taking it 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 Exchange 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*)

**To bring a service group online from the Web Console**

1. On the **Service Group** page (**Cluster Summary > All Groups > Service Group**), click **Online**.
2. In the Online Group dialog box, select the system on which to bring the service group online.
3. To run PreOnline script, select the **Run PreOnline Script** check box.
4. Click **OK**.

## 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*)

**To take a service group offline from the Web Console**

1. On the **Service Group** page (**Cluster Summary > All Groups > Service Group**), click **Offline**. This opens the Offline Group dialog box.
2. Select the system on which to take the service group offline.
3. Click **OK**.

## Switching the service group

The process of switching a service group involves taking it offline on its current system and bringing it online on another system. Perform the following steps to switch the service group from the VCS Java or Web Console.

### To switch a service group 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 **Switch To**, and choose the appropriate system from the pop-up menu. (Right-click > Switch To > *system_name*)

### To switch a service group from the Web Console

1. From the Service Group page (**Cluster Summary > All Groups > Service Group**), click **Switch**.
2. On the Switch Group dialog box, select the system to switch the service group to.
3. Click **OK**.

# Modifying the service group configuration

You can dynamically modify the Exchange service group configuration in several ways, including the Exchange Server Configuration Wizard, Cluster Manager (Java Console), Cluster Management Console (Single Cluster Mode) also referred to as Web Console, and the command line. The following steps describe how to modify the service group using the configuration wizard.

## Prerequisites

- If the Exchange service group is online, you must run the wizard from the node on which the service group is online. You can then use the wizard to add and remove resources. 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 must be online on the node where you run the wizard and offline on all other nodes. So, the LUNs created to store the Exchange database, the registry replication information, the MTA data, and the transaction logs should be connected to node where you run the wizard.
- If you are running the wizard to remove a node from the service group's system list, do not run the wizard from the node being removed.

## Instructions

The following steps describe how to modify an Exchange service group using the configuration wizard. If you run the wizard to add a system to an online service group, resources having local attributes may go in an UNKNOWN state for a short duration. These resources will come out of the UNKNOWN state in the next monitor cycle.

### To modify an Exchange service group

1. Start the Exchange Server Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Configuration Wizard**.
2. Read the information in the Welcome panel and click **Next**.
3. On the Wizard Options panel, click **Modify service group**, click the service group to be modified, and click **Next**.
4. Follow the wizard instructions and make desired modifications to the service group configuration. See "Configuring the service group using the wizard" on page 66 for more information about the configuration wizard.

# Deleting the Exchange service group

The following steps describe how to delete an Exchange service group using the configuration wizard.

### To delete an Exchange service group

1. Start the Exchange Server Configuration Wizard from a cluster node. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Configuration Wizard**.
2. Review the information in the Welcome panel and click **Next**.
3. In the Wizard Options panel, click **Delete service group**, click the service group to be deleted and click **Next**.
4. In the Service Group Summary panel, click **Next**.
5. A message appears informing you that the wizard will run commands to delete the service group. Click **Yes** to delete the service group.
6. Click **Finish**.

Chapter 5

# Making a standalone Exchange server highly available

This chapter contains the following topics:

# About configuring standalone Exchange with VCS

This chapter describes how to bring a standalone Exchange server into a VCS environment. This involves installing VCS and the VCS application agent for Exchange on the Exchange server, making it cluster-ready by running the Exchange Server Setup Wizard for VCS, and adding nodes to the cluster,

This scenario considers an active/passive configuration with one to one failover capabilities.

# Installing VCS  on the Exchange server

Verify the prerequisites, and then install VCS  and the VCS application agent on the system that hosts the Exchange server. See the Veritas Cluster Server Installation and Upgrade Guide for installation information.

# Converting the standalone Exchange server into a “clustered” Exchange server

Use the Exchange Setup Wizard to convert a standalone Exchange server into a “clustered” Exchange server. In this wizard, the node name of the standalone Exchange Server becomes the name of the Exchange virtual server and the existing node is given a new physical node name.

Renaming the existing standalone Exchange server allows Active Directory entries to remain valid. For example, if your existing standalone Exchange server is called EXCH, the name of the Exchange virtual server will become EXCH and the existing node is given a new physical node name, for example, SYSTEM1.

Before proceeding, make sure you meet the following requirements:

- You have installed VCS on the system that hosts Exchange.
  See “Installing the VCS agent for Exchange” on page 21 for more information.
- The system hosting the Exchange server to be made highly available is not configured as a root broker.
- The system hosting the Exchange server does not have VCS configured.

**To convert a standalone Exchange Server into a “clustered” Exchange server**

1. Start the Exchange Server Setup Wizard for VCS from the node having the standalone Exchange server installed. Click **Start > All Programs >**

**Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.

2 Review the information in the Welcome panel and click **Next**.

3 In the Available Option panel, click **Make a standalone Exchange Server highly available** and click **Next**.

4 Specify information related to your network.

- Enter a name for the node. This name will be permanently assigned to the node on which the wizard is being run. This name for the node becomes the new name of the physical system after the process is completed. The original name of the system, for example, EXCH, is returned as the name of the Exchange virtual server so that the Active Directory entries remain valid.
- Enter the name of the domain suffix.
- Select the appropriate public NIC from the drop-down list.
  The wizard lists the public adapters and low-priority TCP/IP enabled private adapters on the system.
- Enter a unique virtual IP address for the Exchange virtual server.
  If you plan to use the IP address of the node as the virtual IP address, you must assign a new static IP address to the node.
- Enter the subnet mask for the virtual IP address.
- Click **Next**.

5 Select a drive where the registry replication data will be stored and click **Next**.
Make sure to select the volumes or the virtual disks (LUNs) to store registry replication information.

6 Review the summary of your selections and click **Next**.

7 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

8 The wizard starts running commands to set up the VCS environment.Various messages indicate the status of each task. After all the commands are executed, click **Next**.

9 Click **Finish**.
The wizard prompts you to restart the system. Click **Yes** to restart the system. Click **No** to restart the system later. You must restart the system before continuing with the next step.

# Adding the standalone Exchange server to a cluster

After converting the standalone Exchange server into a virtual server, use the VCS Cluster Configuration Wizard (VCW) to create a cluster, if one does not already exist, and then add all the nodes to the cluster.

See "Configuring the cluster" on page 24 for instructions.

# Moving Exchange databases

Use the Exchange Server Setup Wizard for VCS with the **Move Exchange Database** option to move the Exchange database from the clustered Exchange server to a shared disk.

If you have multiple SMTP virtual servers configured, the wizard changes the home directory path for default SMTP virtual server and not for the additional SMTP virtual servers. So you must delete additional SMTP servers before running the wizard. You can create them again after the database has been moved by the wizard.

See "Moving Exchange databases to shared storage" on page 56 for instructions.

# Installing Exchange on additional nodes

After moving the Exchange databases to shared storage, install Exchange on additional nodes in the cluster for the same Exchange virtual server, if required. You must run pre-installation, installation, and post-installation procedures for each additional node.

See "Installing Exchange on additional nodes" on page 60 for more information.

# Configuring the Exchange service group for VCS

Configure an Exchange service group in the cluster using the Exchange Server Configuration Wizard. Configuring the Exchange service group involves creating an Exchange service group and defining the attribute values for its resources.

See "Configuring the Exchange service group" on page 65 for instructions.

Chapter 6

# Configuring any-to-any failover

This chapter contains the following topics:

# About any-to-any configuration

This chapter describes how to set up an any-to-any failover configuration in an Exchange cluster. An any-to-any configuration could have many Exchange virtual servers in a cluster, each configured in a separate service group. Each service group can fail over to any configured node in the cluster, provided no other Exchange virtual server is online on that node.

How you configure failover nodes for Exchange instances depends on if Exchange has already been installed on the target node. In any-to-any configuration, the node you plan to use for failover may already have Exchange installed. For example, you configure an EVS1 cluster on SYSTEM1 and SYSTEM3. SYSTEM3 is the failover node for EVS1. Now you install EVS2 on SYSTEM2. You want to use SYSTEM3 as the failover node for EVS2. In this case, you do not install Exchange once again on SYSTEM3. Instead, you specify SYSTEM3 as a common node for failover.

# Installing VCS

Verify the prerequisites, and then install VCS and the VCS application agent on the system that hosts the Exchange server. See the Veritas Cluster Server Installation and Upgrade Guide for installation information.

# Configuring the cluster

After installing VCS, ensure that you have installed the VCS Application agent for Exchange and then run the VCS Cluster Configuration Wizard (VCW) to configure the components required to run the VCS cluster.

See “Installing the VCS agent for Exchange” on page 21.

See “Configuring the cluster” on page 24 for more information.

# Configuring the first Exchange virtual server

Installing Microsoft Exchange in a VCS cluster environment involves three major tasks; pre-installation, Microsoft Exchange installation, and post-installation. The Exchange Setup Wizard for VCS performs the pre-installation and post-installation tasks.

The “First Node” installation tasks need to be repeated on all of the active Exchange nodes in the any-to-any configuration.

See “Installing Microsoft Exchange” on page 43 for more information.

Ensure that you complete all the procedures mentioned.

## Configuring the Exchange service group for VCS

Configure an Exchange service group in the cluster using the Exchange Server Configuration Wizard. Configuring the Exchange service group involves creating an Exchange service group and defining the attribute values for its resources.

See “Configuring the Exchange service group” on page 65 for instructions.

# Configuring another Exchange virtual server for an any-to-any failover

Configure the second Exchange virtual server in the cluster environment. Complete the following tasks:

- Install Exchange on the first node. You must complete pre-installation, Microsoft Exchange installation, and post-installation on the first node only.
  See “Installing Exchange on the first node” on page 53 for more information.
- Move the Exchange databases to shared storage.
  See “Moving Exchange databases to shared storage” on page 56 for more information.

## Specifying a common node for failover

Exchange was installed on the node that will be the common failover node during the installation process of the first Exchange virtual server. You do not need to install Exchange a second time on the common failover node. You must run the Exchange Setup Wizard for VCS to set up the any-to-any failover configuration in the Exchange cluster.

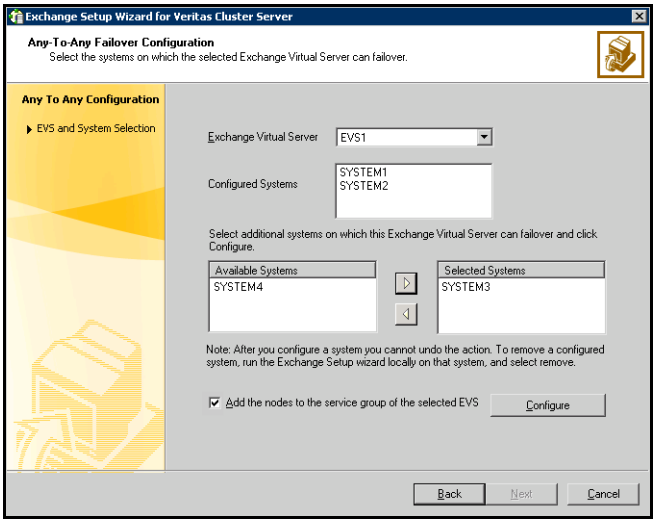
The first Exchange virtual server is already configured with the common failover node. You must run this wizard for the second Exchange virtual server only.

### To specify a common node for failover

1. Start the Exchange Server Setup Wizard for VCS from any node configured to host an Exchange service group. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.
2. Review the information in the Welcome panel and click **Next**.
3. In the Available Option panel, click **Configure/Remove highly available Exchange Server** and click **Next**.

4 In the Select Options panel, click **Configure any-to-any failover** and click **Next**.

5 Select systems to be configured for any-to-any failover. The Existing Systems box lists the nodes on which the Exchange Server service group can fail over.




- Select the Exchange virtual server to which you want to add the additional failover nodes.
- From the Available Systems box, select the systems to be configured for any-to-any failover.

  The Available Systems box lists only those systems that have the same version and service pack level of Microsoft Exchange as the selected Exchange virtual server.
- Click the right arrow to move the selected systems to the Selected Systems box. To remove a system from the box, select the system and click the left arrow.
- Specify whether you want to add the systems to the SystemList of the service group for the selected EVS.
- Click **Configure**. Repeat these steps for all the Exchange virtual servers for which you want to configure any-to-any failover.
- Click **Next**.

6 Click **Finish**.

## Configuring the Exchange service group for an additional Exchange virtual server

A new Exchange service group must be configured for the second Exchange virtual server. Configure an Exchange service group in the cluster using the Exchange Server Configuration Wizard. Configuring the Exchange service group involves creating an Exchange service group and defining the attribute values for its resources.

See “Configuring the Exchange service group” on page 65 for instructions.

Chapter 7

# Deploying agents for disaster recovery

This chapter contains the following topics:

# About disaster recovery configuration

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 primary cluster fails.

This chapter describes how to set up a disaster recovery solution for Exchange server with VCS. Symantec recommends that you configure the secondary site only after you have established a local cluster with the GCO option at the primary site.

# Verifying the primary site configuration

If you have not set up the primary site, follow the instructions in the earlier chapters in this guide. The instructions include specifying the disaster recovery configuration options that are required on a primary site. Make sure you complete the following tasks on the primary site:

- Install VCS with the GCO option and then configure the VCS cluster at the primary site. While configuring the cluster, ensure that you select the GCO option to configure the wide area connector (WAC) resource in the cluster.
  See the Veritas Cluster Server Installation and Upgrade Guide for more information on installing VCS.
  See Chapter 2, "Installing the VCS agent for Exchange" on page 21 for more information on installing the VCS application agent for Exchange and configuring the VCS cluster.
- Install Microsoft Exchange server on the primary site cluster nodes.
  See Chapter 3, "Installing Microsoft Exchange" on page 43 for more information.
- Configure the Exchange service group for VCS.
  See Chapter 4, "Configuring the Exchange service group" on page 65 for more information.

# Setting up the secondary site

Ensure the following before you proceed:

- Configure the Exchange databases for backup and restore using SnapManager for Exchange configuration wizard.
  See "Running SnapManager for Exchange" on page 74 for instructions.
- Make sure the volumes or LUNs at both sites are of the same size.

Perform the following tasks at the secondary site to set up and configure a disaster recovery environment:

- Install VCS with the GCO option and then configure the VCS cluster. While configuring the cluster, ensure that you select the GCO option to configure the wide area connector (WAC) resource in the cluster at the secondary site.
  See the Veritas Cluster Server Installation and Upgrade Guide for more information on installing VCS.
  See Chapter 2, "Installing the VCS agent for Exchange" on page 21 for more information on installing the VCS application agent for Exchange and configuring the VCS cluster.
- Install Microsoft Exchange at the secondary site using the Exchange Setup Server Wizard for VCS.
  See "Installing Microsoft Exchange at the secondary site" on page 92 for instructions.
- Copy the .CRK file from the secondary site to the primary site.
  See "Copying the .CRK file to the primary site" on page 100 for more information.
- Configure an Exchange service group with SnapMirror resources at the secondary site.
  See "Configuring the Exchange service group at the secondary site" on page 101 for instructions for instructions.
- Replicate the volumes containing data for all Exchange components using Network Appliance SnapMirror.
  See "Configuring replication using Network Appliance SnapMirror" on page 102 for instructions.
- Configure SnapMirror resources in the Exchange service group at the primary site.
  See "Configuring NetAppSnapMirror resources at the primary site" on page 102 for instructions.
- Link the clusters at primary and secondary sites.

See “Linking clusters at primary and secondary sites” on page 103 for instructions.

- Configure the Exchange service group to be a global group.
  See “Making the Exchange service group global” on page 103 for instructions.

# Installing Microsoft Exchange at the secondary site

Before installing Microsoft Exchange on the cluster nodes in the secondary site, ensure the following:

- Make sure you meet the prerequisites for installing Exchange.
  See “Before installing Exchange” on page 44 for more information.
- Make sure the Exchange service group is offline in the primary site cluster.
- Connect to the LUNs created to store the registry replication information using the same drive letters and LUN names used at the primary site.

## Installing Exchange on the first node

The tasks to be performed on the first node are described in the following stages: pre-installation, Exchange installation, and post-installation.

If you are familiar with the procedures for installing Exchange on the primary site, you will find that the procedures for installing Exchange are the same for the secondary site except for the pre-installation procedure for the first node. In the pre-installation procedure for the first node, you must select the wizard option to create a failover node for Exchange disaster recovery setup, instead of the option to create a new Exchange virtual server.

### Exchange pre-installation: first node

Use the Exchange Server Setup Wizard for VCS to complete the pre-installation phase. This process changes the physical name of the node to a virtual name.

---

**Note:** After you have run the wizard, you will be requested to restart the node. Close all open applications and save your data before running the wizard.

---

#### To perform Exchange pre-installation

1. Verify the volume or LUN created to store the registry replication information on the secondary site is mounted on or connected to this node and dismounted or disconnected from other nodes in the cluster. Assign the same drive letters and names to these LUNs as on the primary site.

2 Start the Exchange Server Setup Wizard for VCS. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.

3 Review the information in the Welcome panel and click **Next**.

4 In the Available Option panel, click **Install Exchange Server for High Availability** and click **Next**.

5 In the Select Option panel, click **Create a failover node for Exchange disaster recovery setup** and click **Next**.

6 In the Select System From Primary Site panel, enter the name of a system on the primary site on which Exchange virtual server is configured and click **Next**.

7 In the Select Exchange Virtual Server panel, select the Exchange virtual server for disaster recovery and click **Next**.
If the service group on the primary node has not been taken offline, the installer prompts you to do so without exiting the installer, or you can cancel the installation wizard and take the service group offline manually. When all requirements are validated, click **Next**.

8 Enter a name of a failover node and click **Next**.

9 Specify the information related to your network. The wizard discovers the Exchange virtual server name and the domain suffix from the Exchange configuration. Verify this information and provide values for the remaining fields.
   - Enter a unique virtual IP address for the virtual server. By default, the wizard displays the IP address assigned while installing Exchange in the primary cluster; you can assign a different IP address in the secondary cluster.
   - Enter the subnet to which the virtual IP address belongs.
   - Select the appropriate public NIC from the drop-down list.
     The wizard lists the public adapters and low-priority TCP/IP enabled private adapters on the system.
   - Click **Next**.

10 In the Registry Replication Drive panel, select a drive where the registry replication data will be stored and click **Next**. Make sure you select the same drive letter (or directory in case of folder mounts) as the one used at the primary site for registry replication.

11 Review the summary of selections and click **Next**.

12 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

If the wizard could not locate a DNS entry for the specified Exchange server and IP address, click **OK** to create one. If a DNS entry for the specified Exchange server and IP address does not exist, the wizard will display a message. Click **OK** to let the wizard create the DNS entry. If the wizard is unable to create the entry, click **OK** to continue. In this case, you will have to manually create the DNS entry.

13 The wizard starts running commands to set up the VCS environment. Various messages indicate the status of each task. After all the commands are executed, click **Next**.

14 Click **Reboot**. The wizard prompts you to reboot the node. Click **Yes**.
After you reboot the node, the value specified for the Exchange virtual server is temporarily assigned to the node. So, all network connections to the node must be made using the temporary name. After installing Microsoft Exchange, you must rerun this wizard to assign the original name to the node.
On rebooting the node, the Exchange Server Setup Wizard is launched automatically. Review the information in the wizard dialog box and proceed to installing Microsoft Exchange Server. Do not click Continue at this time. Wait until after you install Exchange installation.
See "Exchange server installation: first node" on page 94 for instructions.
If you need to undo all actions performed by the wizard during the pre-installation, click **Revert Changes**.

## Exchange server installation: first node

Install Exchange on the node where the Exchange Server Setup Wizard was run for the pre-installation tasks.

- Install any required service packs.
- Install the same Exchange version and components on all nodes.

The procedure below is based on Exchange 2003. This is a standard Microsoft Exchange Server installation. Refer to the Microsoft documentation for details on this installation.

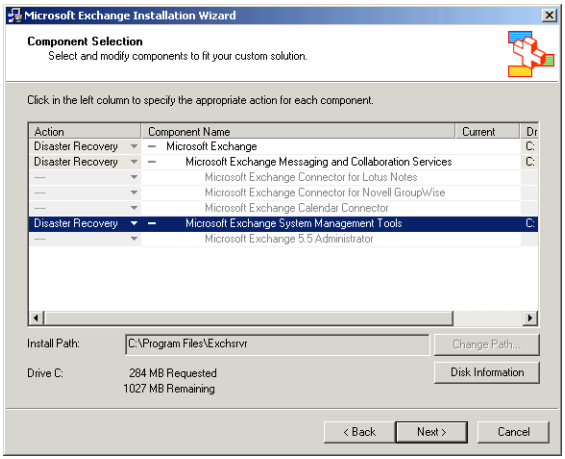
### To install Exchange

1 Begin the Exchange installation for disaster recovery at the command prompt using the /disasterrecovery option :

```
<drive letter>:\SETUP\I386\setup.exe
    /disasterrecovery
```

where *<drive letter>* is the location where the Exchange software is located.

2 During the wizard, verify or select **Disaster Recovery** in the **Action** column for the Microsoft Exchange, Microsoft Exchange Messaging and Collaboration services and Microsoft Exchange System Management Tools components. Be sure to install the same components on all the nodes in the cluster.




3 When notified to restore databases from backup and reboot the node after completing the installation, click **OK** and complete the Microsoft Exchange wizard.

4 If prompted to reboot the node, click **Yes**.

5 For Exchange 2003, install the service packs listed in the requirements. When installing service packs enter the following from the command line:

```
SETUP\I386\update.exe /disasterrecovery
```

## Exchange post-installation: first node

After completing the Microsoft Exchange installation, use the Exchange Setup Wizard for VCS to complete the post-installation phase. This process reverts the node name to the physical name, and sets the Exchange services to manual so that the Exchange services can be controlled by VCS.

### To run the Exchange post-installation

1 Make sure that the Veritas High Availability Engine (HAD) is running on the node on which you plan to perform the post-installation tasks.

Type the following on the command line:

```
C:\>hasys -state
```

The state should display as RUNNING.

If HAD is not running, start it. Type the following on the command line:

```
C:\>net stop had
C:\>net start had
```

2 Verify the volume or LUN created to store the registry replication information is mounted on or connected to this node and dismounted or disconnected from other nodes in the cluster.

3 If the Exchange installation did not prompt you to reboot the node, click **Continue** from the Exchange Server Setup Wizard and proceed to step 5 on page 96.
If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.

4 Review the information in the Welcome panel and click **Next**.

5 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

6 The wizard starts performing the post-installation tasks. Various messages indicate the status. After all commands are executed, click **Next**.

7 Click **Finish**.

8 The wizard prompts you to reboot the node. Click **Yes**.
Changes made during the post-installation steps do not take effect till you reboot the node.
If you want to add failover nodes to the Exchange cluster, proceed to "Installing Exchange on additional nodes" on page 96 for instructions. Otherwise, proceed to "Copying the .CRK file to the primary site" on page 100.

# Installing Exchange on additional nodes

Install Exchange on additional nodes in the secondary site cluster to configure the nodes as failover nodes for the same Exchange virtual server. You must run the pre-installation, Exchange installation, and post-installation procedures on each additional node.

## Exchange pre-installation: additional nodes

Use the Exchange Server Setup Wizard for VCS to complete the pre-installation phase. This process changes the physical name of the node to a virtual name.

Before adding a node to the Exchange cluster, make sure you meet the prerequisites listed under "Before installing Exchange" on page 44.

To perform Exchange pre-installation

1. Verify the volume or LUN created to store the registry replication information is mounted on or connected to this node and dismounted or disconnected from other nodes in the cluster.
2. Start the Exchange Server Setup Wizard for VCS from the node to be added to an Exchange cluster. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.
3. Review the information in the Welcome panel and click **Next**.
4. In the Available Option panel, click **Install Exchange Server for High Availability** and click **Next**.
5. In the Select Option panel, click **Create a failover node for existing Exchange Virtual Server** and click **Next**.
6. Select the Exchange virtual server for which you are adding the failover node and click **Next**.
7. Specify network information for the Exchange virtual server. The wizard discovers the Exchange virtual server name and the domain suffix from the Exchange configuration. Verify this information and provide values for the remaining text boxes.
   - Select the appropriate public NIC from the drop-down list.
     The wizard lists the public adapters and low-priority TCP/IP enabled private adapters on the system.
   - Optionally, enter a unique virtual IP address for the Exchange virtual server. By default, the text box displays the IP address assigned when the Exchange Virtual Server was created on the first node. You should not have to change the virtual IP address that is automatically generated when setting up an additional failover node for the virtual server in the same cluster.
   - Enter the subnet mask for the virtual IP address.
   - Click **Next**.
8. Review the summary of your selections and click **Next**.
9. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
10. The wizard starts running commands to set up the VCS environment. Various messages indicate the status of each task. After all the commands are executed, click **Next**.
11. Click **Reboot**.
    The wizard prompts you to reboot the node. Click **Yes**.

After you reboot the node, the value specified for the Exchange virtual server is temporarily assigned to the node. So, all network connections to the node must be made using the temporary name. After installing Microsoft Exchange, you must rerun this wizard to assign the original name to the node.

On rebooting the node, the Exchange Server Setup wizard is launched automatically. Review the information in the wizard dialog box and proceed to installing Microsoft Exchange Server.

See "Exchange Server installation: additional nodes" on page 98 for instructions.

If you want to undo all actions performed by the wizard during the preinstallation procedure, click **Revert**.

Do not click **Continue** at this time. Wait until after the Exchange installation is complete.

## Exchange Server installation: additional nodes

Install Exchange on the node where the Exchange Server Setup Wizard was run for the pre-installation task.

- Install any required service packs.
- Install the same Exchange version and components on all nodes.

The procedure below is based on Exchange 2003. This is a standard Microsoft Exchange Server installation. Refer to the Microsoft documentation for details on this installation.

### To install Exchange

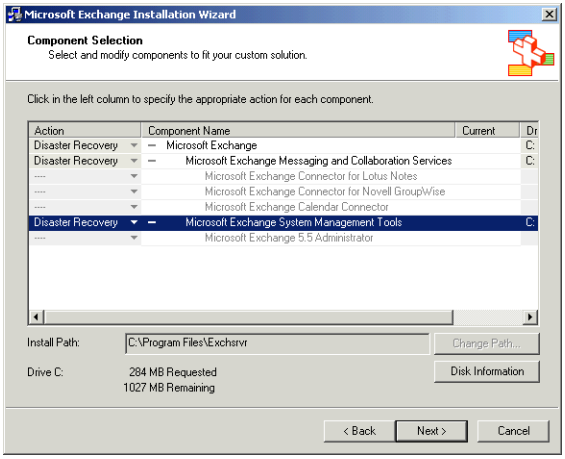
1. Begin the Exchange installation for disaster recovery at the command prompt using the /disasterrecovery option :

   ```
   <drive letter>:\SETUP\I386\setup.exe
       /disasterrecovery
   ```

   where *<drive letter>* is the location where the Exchange software is located.

2. During the wizard, verify or select **Disaster Recovery** in the **Action** column for the Microsoft Exchange, Microsoft Exchange Messaging and Collaboration services and Microsoft Exchange System Management Tools

components. Be sure to install the same components on all the nodes in the cluster.




3 When notified to restore databases from backup and reboot the node after completing the installation, click **OK** and complete the Microsoft Exchange wizard.

4 If prompted to reboot the node, click **Yes**.

5 For Exchange 2003, install the service packs listed in the requirements. When installing service packs enter the following from the command line:

```
SETUP\I386\update.exe /disasterrecovery
```

## Exchange post-installation: additional nodes

After completing the Microsoft Exchange installation, use the Exchange Server Setup Wizard to complete the post-installation tasks. This process reverts the node name to original name.

### To perform the Exchange post-installation

1 Verify the volume or LUN created to store the registry replication information is mounted on or connected to this node and dismounted or disconnected from other nodes in the cluster.

2 If the Exchange installation did not prompt you to reboot the node, click Continue from the Exchange Server Setup Wizard and proceed to step 5 on page 100.
If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.

3 Review the information in the Welcome panel and click **Next**.

4 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

5 The wizard starts performing the post-installation tasks. Various messages indicate the status. After all commands are executed, click **Next**.

6 Specify whether you want to add the node to the SystemList of the service group for the EVS selected in the pre-installation step. You must do so only if service groups are already configured for the EVS.
If you wish to add the nodes later, you can do so by using the Exchange service group configuration wizard.

7 Click **Finish**.

8 The wizard prompts you to reboot the node. Click **Yes**.
Changes made during the post-installation steps do not take effect till you reboot the node.

# Copying the .CRK file to the primary site

The .CRK file is the public cryptographic key of the Exchange virtual server. This key is regenerated every time the Exchange virtual server is installed.

The file is located on the shared disk used to store the registry replication information at the path *Drive*\VCS\Private\RegRep\Exch*EVSName*.CRK

where *Drive* represents the drive letter used to connect to the virtual disk (LUN) and *EVSName* represents the name of the Exchange virtual server.

Copy this file to the same location at the primary site. You must perform this step every time you add a node to an Exchange cluster on the secondary site.

See the Network Appliance documentation for instructions on copying files.

# Backing up and restoring the Exchange data files

A DR installation of Microsoft Exchange does not create Exchange data files. Therefore, after installing Exchange on the secondary site, you must back up the Exchange volumes or LUNs on the primary site and then restore it on the secondary site. Make sure you restore the data at the same path at the secondary site as on the primary site.

Complete the following tasks:

- On the primary site, back up all volumes or LUNs specified for Exchange data files.
- Restore the group in the corresponding location on the secondary site.

See the Network Appliance documentation for instructions on restoring data.

---

**Note:** Perform this step *only once* at the secondary site.

---

# Configuring the Exchange service group at the secondary site

Configuring the Exchange service group involves creating an Exchange service group and defining the attribute values for its resources.

See Chapter 4, "Configuring the Exchange service group" on page 65 for more information.

- Make sure the service group has the same name as in the primary site cluster.
- In case of a NetApp storage environment, make sure you configure NetApp SnapMirror resources in the service group.
- Do not bring the service group online.

Note that the service group may be partially online because the LUNs are connected to the node.

# Configuring replication using Network Appliance SnapMirror

You can replicate Exchange 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.

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.

Refer to Network Appliance documentation for more information.

# Configuring NetAppSnapMirror resources at the primary site

Configure NetAppSnapMirror resources at the primary site to monitor data replication from the primary site to the secondary site. The following steps describe how to add the resources using the Exchange Server Configuration Wizard.

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.

### To configure SnapMirror resource using Exchange Server Configuration Wizard

1. Verify the volume or LUN created to store the registry replication information is mounted on or connected to this node and dismounted or disconnected from other nodes in the cluster.
2. Start the Exchange Server Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Configuration Wizard**.
3. Review the information in the Welcome panel and click **Next**.

4 In the Wizard Options panel, click **Modify service group**, click the service group to be modified, and click **Next**.

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

6 In the Exchange Server Configuration panel, check **Configure the NetApp SnapMirror resource(s)** and click **Next**.

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

8 In the Completing the Exchange Configuration panel, uncheck the **Bring the service group online** check box and click **Finish**.

# Linking clusters at primary and secondary sites

Once all the setup tasks are completed at the primary and secondary sites, you must link the clusters at both the sites. The VCS Java Console provides a wizard to create global cluster by linking standalone clusters.

For instructions, see the chapter on Administering Global Clusters from Cluster Manager (Java Console) in the *Veritas Cluster Server Administrator's Guide* for instructions.

# Making the Exchange service group global

After linking the clusters at the primary and secondary sites, use the Global Group Configuration wizard of the Java Console to convert the Exchange service group from a local service group to a global service group. This will enable the Exchange service group to fail over across clusters.

For instructions, see the chapter on Administering Global Clusters from Cluster Manager (Java Console) in the *Veritas Cluster Server Administrator's Guide* for instructions.

# Managing failover in a disaster recovery environment

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.

Remote failover involves starting the Exchange services on a node in the remote cluster. In case of an administrative failover, this also involves reversing the direction of replication by demoting the original source to a target, and replicating from the new source.

## Managing a successful remote failover

For a successful failover, you must perform the following tasks after the service group comes online at the remote site.

**To manage a successful failover**

1. Freeze the Exchange service group at the remote site.
2. Restore Exchange data from the latest valid database snapshot using the Network Appliance SnapManager Restore utility.
3. Unfreeze the Exchange service group.

## Managing failover in response to a network outage

In the event that the public network or the private storage network at the local cluster fails, the application fails over to the remote site. Perform the following tasks to ensure a proper failover.

**To ensure a proper failover**

1. Freeze the service group at the local site.
2. Restore the network connections. You may see concurrency violation errors in the engine log. Ignore these errors.
3. Unfreeze the service group.
4. Take the service group offline at the local site.
5. Freeze the service group at the remote site.
6. Restore Exchange data from the latest valid database snapshot using the Network Appliance SnapManager Restore utility.
7. Unfreeze the Exchange service group.

# Switching the service group back to the local cluster

When the application fails over to a remote site, switching the application back to the local site involves the following additional tasks, depending on whether the failover was administrative or in response to a disaster.

## Administrative failover

In case of an administrative failover, VCS brings the service group online at the remote site and reverses the direction of replication.

### To switch the application back to the local cluster

1. Back up the Exchange data using Network Appliance SnapManager. See the Network Appliance documentation for instructions.
2. Switch the service group.
   - In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group.
   - Click **Switch To**, and click **Remote switch**.
   - Select a system at the local site and click **OK**.

## Failover in response to a disaster

In the event that a disaster strikes the local cluster and the application fails over to the remote site, data is written to the LUNs at the remote site. When the local site comes up again, the Exchange data at both sites is out-of-sync.

### To switch the application back to the local cluster

1. Synchronize the Exchange data at both sites by running the fbsync action at the site at which the service group is online.

   # **hares -action *SnapMirror_resname* fbsync -sys *node_name***

   The variable *SnapMirror_resname* represents the name of the SnapMirror resource; *node_name* represents the node on which the service group is online.

   Run the action for each SnapMirror resource.
2. Back up the Exchange data using Network Appliance SnapManager. See the Network Appliance documentation for instructions.
3. Switch the service group.
   - In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group.
   - Click **Switch To**, and click **Remote switch**.
   - Select a system at the local site and click **OK**.

Chapter 8

# Removing the software

This chapter contains the following topics:

# About removing VCS

This chapter describes steps to remove VCS.

# Before removing VCS

- From the Exchange service group SystemList, remove the node where you are removing Microsoft Exchange.
- Verify that the user mailboxes and routing group connectors are deleted from the system where you are removing Microsoft Exchange.
- Verify that the system from which Microsoft Exchange will be removed is not a Recipient Update Server.
- Verify that the system from which Microsoft Exchange will be removed is not a routing master.

See “Troubleshooting Microsoft Exchange uninstallation” on page 125 to resolve errors encountered while removing Microsoft Exchange.

# Overview of tasks

Removing VCS from a cluster node involves the following tasks:

- Remove Microsoft Exchange Server from the node using the Exchange Server Setup Wizard for VCS.
  See “Removing Microsoft Exchange” on page 109 for instructions.
- Remove the VCS configuration from the node using VCS Cluster Configuration Wizard (VCW).
  See “Removing the VCS configuration” on page 112 for instructions.
- Remove VCS.
  See “Removing the agents” on page 112 for instructions.

# Removing Microsoft Exchange

The Exchange Server Setup Wizard for VCS performs the following tasks for removing Microsoft Exchange from a node:

- If the node being removed is configured to host other Exchange virtual servers, the wizard removes the node from the SystemList of the service group for the specified Exchange virtual server. The wizard does not remove Microsoft Exchange from the node.
  See "Removing a node without removing Microsoft Exchange" on page 109 for instructions.
- If the node being removed is not configured to host other Exchange virtual servers, the wizard removes the node from the SystemList of the service group for the specified Exchange virtual server. The wizard also removes Microsoft Exchange from the node by launching the Microsoft Exchange Installation wizard.
  See "Removing a node and removing Microsoft Exchange" on page 110 for instructions.

**Note:** If you are uninstalling Microsoft Exchange from all nodes in the cluster, delete the service group after taking it offline.

## Removing a node without removing Microsoft Exchange

These steps describe how to remove a node without removing Microsoft Exchange.

**To remove a node without removing Microsoft Exchange**

1. Start the Exchange Server Setup Wizard for VCS. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server Setup Wizard**.
2. Review the information in the Welcome panel and click **Next**.
3. In the Available Option panel, click **Configure/Remove highly available Exchange Server** and click **Next**.
4. In the Select Option panel, click **Remove Exchange Server** and click **Next**.
   If an Exchange service group is configured on the node, the wizard prompts you to remove the system from the service group's SystemList attribute. Resolve the error and rerun the Exchange Server Setup Wizard.
5. Select the Exchange virtual server for which you are removing the failover node and click **Next**.

6 The wizard starts running commands to set up the VCS environment for removing the node from the Exchange service group. Various messages indicate the status of each command. Once all the commands are executed, click **Next**.

7 Click **Finish**.
Proceed to "Removing the agents" on page 112 for instructions on uninstalling the VCS agent for Exchange.

## Removing a node and removing Microsoft Exchange

These steps describe how to remove a node and remove Microsoft Exchange.

**To remove a node and remove Microsoft Exchange**

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

2 Review the information in the Welcome panel and click **Next**.

3 In the Available Option panel, click **Configure/Remove highly available Exchange Server** and click **Next**.

4 In the Select Option panel, click **Remove Exchange Server** and click **Next**. If an Exchange service group is configured on the node, the wizard prompts you to remove the system from the service group's SystemList attribute. Resolve the error and rerun the Exchange Server Setup Wizard.

5 Select the Exchange virtual server for which you are removing the failover node and click **Next**.

6 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

7 The wizard starts running commands to set up the VCS environment for removing the node from the Exchange service group. Once all the commands are executed, click **Next**.
If the node is the last node in the Exchange service group, the wizard prompts you to choose whether you want to retain the entry for the EVS in the Active Directory. Click **Yes** to remove the entry or **No** to retain the entry.

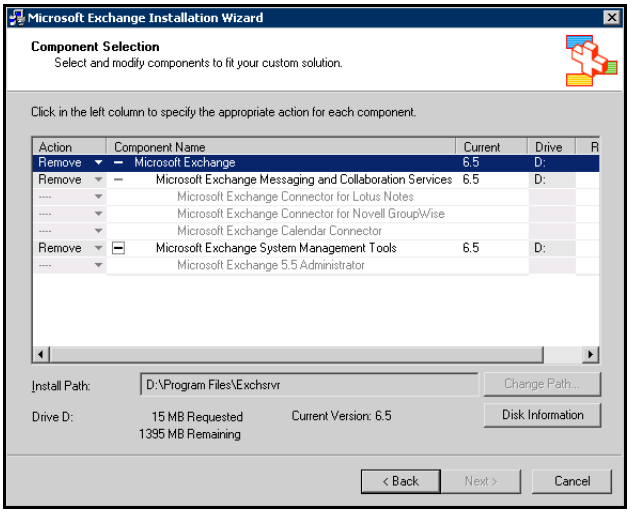
8 Click **Reboot**. The wizard prompts you to restart the node. Click **Yes** to restart the node.
If you have other applications running, click **No**, close all applications, and restart the node manually.

9 Restarting the node automatically launches the Exchange Server Setup Wizard for VCS. Review the information in the Welcome dialog box and click **Next**.

10 A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.

11 In the Microsoft Exchange Installer Welcome panel, read the welcome information and click **Next**.

12 In the Component Selection panel, click the **Action** column against each Exchange component, select **Remove** from the drop-down list, and click **Next**.




13 In the Installation Summary panel, review the information presented and click **Next**. The Component Progress panel displays the status of the uninstallation.

14 In the completion panel, click **Finish**.
Do not reboot the node at this stage. The Exchange Server Setup Wizard for VCS must complete its operations before the node is rebooted.

15 The Exchange Server Setup Wizard for VCS will be launched automatically. The wizard performs the post-uninstallation tasks. Once all the tasks are complete, click **Next**.

16 Click **Finish**. The wizard prompts you to restart the node. Click **Yes** to restart the node.
If you have other applications running, click **No**, close all applications, and restart the node manually.

# Removing the VCS configuration

Before you remove the VCS , use the VCS Configuration Wizard (VCW) to delete the VCS configuration from all nodes where Microsoft Exchange Server was uninstalled using the Exchange Server Setup Wizard for VCS.

For instructions, see the chapter on Modifying the Cluster Configuration in the *Veritas Cluster Server Administrator's Guide*.

# Removing the agents

This section describes steps for uninstalling VCS  using the Veritas Product Installer.

You can also perform a silent uninstallation of the software from the command prompt. For more information, including the command syntax, see the Veritas Cluster Server Installation and Upgrade Guide.

## Prerequisites

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

## Instructions

Follow these steps to removing VCS .

**To remove VCS**

1. In the **Add/Remove Programs** applet, click VCS (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 removal. 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**. The installer displays the status.

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

8 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 **VCS (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**.

Chapter 9

# Troubleshooting the agents

This chapter contains the following topics:

# About troubleshooting VCS agents

This chapter describes how to troubleshoot common problems in the VCS agents for Network Appliance and Microsoft Exchange. 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 Symantec product logs the message. For VCS application agent for Microsoft Exchange, 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, CIRITCAL, 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 ExchService agent would resemble: `V-16-20024-13`
  Originator ID for all VCS products is 'V-16.' Category ID for ExchProtocol agent is 20023 while that for ExchService agent is 20024. 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:

```
2006/12/19 15:09:22 VCS INFO V-16-20024-13
ExchService:d1-ExchService-MSExchangeIS:online:Service
(MSEXCHANGEIS) is taking longer to start. Timeout = 10 seconds
```

## VCS Cluster Configuration Wizard (VCW) 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:

```
00005540-00000064: 5540: STARTING - Discovering NICs on the
selected machines...
00009956-00000064: 9956: STARTING - Generating private network
related files...
00009956-00000048: 9956: COMPLETED - Gererating 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 9-1** Network Appliance agents error messages

| Message | Description |
|---|---|
| Failed to open connection to filer *%s*. | Make sure that the VCS Helper Service account has is a domain user and is part of the administrator's group on the local host and the filer.<br>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. |
| Failed to initialize ONTAPI on system | The agent could not find the file NTAPADMIN.DLL on the system. Verify the file exists in the `%VCS_HOME%\bin` directory |
| Invalid attributes exist in the configuration | Some agent attributes have not been defined or have been defined incorrectly. Verify the configuration definition for the agent. |
| *ONTAP API* called failed for *object_name* on *filer_name*. | The specified API failed on the specified object. See the NetApp ONTAP API documentation for information about the associated error message |
| Volume *%s* on filer *%s* is not a SnapMirror replicated volume | Verify replication is set up on the specified volume. |
| 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 | There should be only one destination per source volume. |

**Table 9-1** Network Appliance agents error messages (continued)

| Message | Description |
|---|---|
| Initialize VLibNetAppHost::Initialize() failed. (error_type: *%s*, error_code: *0x%s*) | The agent could not detect the iSCSI or the FC Initiator on the host.<br>Make sure that you have installed and configured Microsoft iSCSI Initiator or an FC Initiator on each node. |
| 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:<br>■ Filer name<br>■ Volume name/LUN name<br>■ Share name<br>■ Storage IP<br>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. |

# Exchange Protocol agent error messages

This section describes the error messages for the Exchange Protocol agent.

**Table 9-2** Exchange Protocol agent error messages

| Message | Description |
|---|---|
| Failed to find the service object. Please check the 'Protocol' attribute | The value specified for “Protocol” attribute is incorrect.<br>Solution: Provide a valid value for the attribute. |
| Failed to get the Lanman resource state *Error Type*, *Error Code*. Please check the 'LanmanResName' attribute. | The value specified for the Lanman resource is incorrect.<br>Solution: Provide a valid value for the Lanman resource. If the value is correct, see error type and error code for further information. |
| Configuration error. 'Protocol' attribute is not configured. | No value specified for the “Protocol” attribute.<br>Solution: Specify a valid value for the attribute. |
| Configuration error. 'VirtualServer' attribute is not configured. | No value specified for the “Virtual Server” attribute.<br>Solution: Specify a valid value for the attribute. |
| Configuration error. 'LanmanResName' attribute is not configured. | No value specified for the “LanManResName” attribute.<br>Solution: Specify a valid value for the attribute. |
| Failed to find the specified exchange server (*server name*) in the active directory. *Error Type*, *Error Code*. | The value specified for the Exchange server name (lanman resource name) does not pertain to the Exchange server service group.<br>Solution: Provide a valid value for the Lanman resource that pertains to the Exchange server service group. |

**Table 9-2** Exchange Protocol agent error messages (continued)

| Message | Description |
|---|---|
| Failed to get protocol virtual servers (Type = *protocol type*).*Error Type*, *Error Code*. | The value specified for the protocol type and protocol server do not match.<br>Solution: Provide a valid combination of protocol type and protocol server. |
| Failed to find the specified protocol virtual server (*server name*) *Error Type*, *Error Code*. Please check the 'VirtualServer' attribute. | The value specified for the protocol virtual server is incorrect. See the associated Windows error type and error code for more information. |
| Failed to initialize active directory protocol object. *Error Type*, *Error Code*. | The agent fails to initialize the Active Directory protocol object. See the associated Windows error type and error code for more information. |
| Failed to access the active directory. *Error Type*, *Error Code*. | The agent fails to access the Active Directory. See the associated Windows error type and error code for more information. |
| ADsOpenObject() for *obj_name* returned *Error Code* | The agent fails to open the Active Directory object. See the associated Windows error code for more information. |
| The Lanman resource (Virtual name = *resource name*) is offline. | The Lanman resource is offline.<br>Solution: Bring the Lanman resource online. |
| Failed to start the protocol virtual server (*virtual server name*). *Error Type*, *Error Code*. | The agent failed to start the protocol virtual server. See the associated Windows error type and error code for more information. |
| Failed to stop the protocol virtual server (*virtual server name*). *Error Type*, *Error Code*. | The agent failed to stop the protocol virtual server. See the associated Windows error type and error code for more information. |
| Failed to determine the state of the protocol virtual server (*virtual server name*). *Error Type*, *Error Code*. | The agent failed to determine the state of the protocol virtual server. See the associated Windows error type and error code for more information. |

# Exchange Service agent error messages

This section describes the error messages for the Exchange Service agent.

**Table 9-3** Exchange Service agent error messages

| Message | Description |
|---|---|
| Failed to find the service object. Please check the 'Service' attribute. | The value specified for the “Service” attribute is incorrect.<br>Solution: Provide a valid value for the Lanman resource. If the value is correct, see error type and error code for further information. |
| Configuration error. 'Service' attribute is not configured. | No value specified for the “Service” attribute.<br>Solution: Specify a valid value for the attribute. |
| Configuration error. 'LanmanResName' attribute is not configured. | No value specified for the “LanManResName” attribute.<br>Solution: Specify a valid value for the attribute. |
| Failed to get the Lanman resource state *Error Type*, *Error Code*. Please check the 'LanmanResName' attribute. | The value specified for the Lanman resource is incorrect.<br>Solution: Provide a valid value for the Lanman resource. If the value is correct, see error type and error code for further information. |
| The Lanman resource (Virtual name = *resource name*) is offline. | The Lanman resource is offline.<br>Solution: Bring the Lanman resource online. |
| Failed to stop the service (*service name*). *Error Type*, *Error Code*. | The agent failed to stop the service. See the associated Windows error type and error code for more information. |
| Failed to start the service (*service name*) *Error Type*, *Error Code*. | The agent failed to start the specified service. See the associated Windows error type and error code for more information. |

**Table 9-3** Exchange Service agent error messages (continued)

| Message | Description |
|---|---|
| Failed to open the service object.(Service = *service name*). *Error Type*, *Error Code*. | The agent failed to open the service object. See the associated Windows error type and error code for more information. |
| Failed to initialize the CExchServer object. *Error Type*, *Error Code*. | The agent failed to initialize the Exchange server object. |
| Failed to query the service status. (Service = *service name*). Error = *Error Type* | The agent failed to query the service object. See the associated Windows error type and error code for more information. |
| Failed to terminate the service (*service name*). *Error Type*, *Error Code*. | The agent failed to terminate the service. See the associated Windows error type and error code for more information. |
| Failed to open the service object (Service = *service name*). *Error Type*, *Error Code*. | The agent failed to open the service object. See the associated Windows error type and error code for more information.?? |

# Troubleshooting Microsoft Exchange uninstallation

You might encounter errors while removing Microsoft Exchange if any of the following requirements are not adhered to:

- User mailboxes exist.
- The Exchange Server to be uninstalled is a Recipient Update Server.
- The Exchange Server to be uninstalled is a Routing Group Master.
- The Exchange Server to be uninstalled has routing group connectors configured.

In any of the above scenarios, complete the following steps to resolve the error:

1. Start the following Exchange services manually using the Service Control Manager:
   - MSExchangeSA
   - MSExchangeIS
   - MSExchangeMTA
   - MSExchangeMGMT
   - RESvc
   - POP3
   - IMAP4
2. Delete user mailboxes by running the **Active Directory Users and Computers** MMC wizard. Click **Start > All Programs > Microsoft Exchange > Active Directory Users and Computers**.
3. Delete the routing group connector by running the **Exchange System Manager** MMC wizard. Click **Start > All Programs > Microsoft Exchange > Exchange System Manager**.
4. Change the Routing Group Master by running the **Exchange System Manager** MMC wizard.
5. Change the Recipient Update Server by running the **Exchange System Manager** MMC wizard.
6. Stop all Exchange services started in Step 1.
7. Start the Exchange Server Setup Wizard for VCS and select the **Remove Exchange** option. Note that you must uninstall Exchange only by using the Exchange Server Setup Wizard for VCS.

# Troubleshooting Exchange Setup Wizard issues

This section describes some of the issues related to the Exchange Setup Wizard for VCS.

## Exchange Setup Wizard may fail to rename the node

When adding a failover node to an existing Exchange cluster, the Exchange Setup Wizard may fail to rename the node during the pre-installation phase, and report the following error message:

```
Failed to rename the node. Refer to the log file for
further details.
```

This can happen if the Exchange Setup Wizard is unable to delete the Exchange Virtual Server computer object in the Active Directory.

To resolve this issue, you must manually delete the Exchange Virtual Server computer object from the AD, and run the wizard again.

Appendix A

# Resource type definitions

This chapter contains the following topics:

# 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.

# NetApp Filer agent

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

## Resource type definition

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

## Attribute definitions

**Table A-1** NetApp Filer agent attributes

| Attribute | Type - Dimension | Description |
|---|---|---|
| FilerName | string-scalar | DNS-resolvable name or IP address of the locally attached filer. |
| StorageIP | string -scalar | The private storage IP address of the filer. |

# NetApp SnapDrive agent

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

| Attribute | Type - Dimension | Description |
|---|---|---|
| FilerResName | string-scalar | Name of the VCS NetAppFiler-type resource in the service group. |
| VolumeName | string-scalar | Name of the volume containing the virtual disk. Define the volume name in the same case as on the filer. |
| ShareName | string-scalar | Name of the CIFS share containing the virtual disk. |
| LUN | string-scalar | 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. |
| MountPath | string-scalar | Drive letter to be assigned to the virtual disk. |
| Initiator | string-vector | Name of iSCSI or FC initiator the host uses to connect virtual disks. You can retrieve this value from the Disk Management console. |

# NetApp SnapMirror agent

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

## Resource type definition

```
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 A-3** NetApp SnapMirror agent attributes

| Attribute | Type - Dimension | Description |
|---|---|---|
| FilerResName | string-scalar | Name of the VCS NetAppFiler-type resource in the group. |
| VolumeName | string-scalar | Name of the volume containing the virtual disk. Define the volume name in the same case as on the filer. |
| SnapMirrorArguments | string-scalar | Specifies the SnapMirror arguments such as maximum transfer speed and restart mode. |
| SnapMirrorSchedule | string-scalar | Specifies the schedule the destination uses for updating data. Do not assign a value for this attribute if you use SnapManager.<br>By default, this attribute does not have any value. |

**Table A-3** NetApp SnapMirror agent attributes (continued)

| Attribute | Type - Dimension | Description |
|---|---|---|
| AppResName | string-scalar | Name of the resource configured to monitor the application being made highly available. When used with Exchange Server, set this value to the name of the ExchService resource configured to monitor the Exchange Information Store. |

# Exchange Service agent

The Exchange Service agent is configured as a resource of type ExchService.

## Resource type definition

```
type ExchService (
    static i18nstr ArgList[] = { Service,
    "LanmanResName:VirtualName",DetailMonitor }
    str Service
    str LanmanResName
    int DetailMonitor = 0
    static keylist SupportedActions = {autoMountDB}
)
```

## Attribute definitions

**Table A-4** Exchange Service agent required attributes

| Required Attributes | Type - Dimension | Definition |
|---|---|---|
| Service | string-scalar | The name of the Exchange service to be monitored. This attribute could take any of the following values:<br>■ MSExchangeIS<br>■ MSExchangeMTA<br>■ MSExchangeMGMT<br>■ MSExchangeSA<br>■ RESvc |
| LanmanResName | string-scalar | The name of the LANMAN resource on which the ExchService resource depends. |

**Table A-5** Exchange Service agent optional attributes

| Optional Attribute | Type - Dimension | Definition |
|---|---|---|
| DetailMonitor | integer-scalar | A flag that determines whether the agent monitors the MSExchangeIS service in detail. The value 1 indicates that the agent monitors the service in detail; the value 0 indicates it does not.<br>Set this attribute only for resources configured to monitor the MSExchangeIS service; the attribute is ignored for other services. |

# Exchange Protocol agent

The Exchange Protocol agent is configured as a resource of type ExchProtocol.

## Resource type definition

```
type ExchProtocol (
    static i18nstr ArgList[] = { Protocol, VirtualServer,
    "LanmanResName:VirtualName",DetailMonitor }
    str Protocol
    i18nstr VirtualServer
    str LanmanResName
    int DetailMonitor = 0
)
```

## Attribute definitions

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

**Table A-6** Exchange Protocol agent required attributes

| Required Attributes | Type - Dimension | Definition |
|---|---|---|
| VirtualServer | string-scalar | The name of the Exchange protocol server to be monitored. This attribute can take localized values. |
| LanmanResName | string-scalar | The name of the LANMAN resource on which the ExchProtocol resource depends. |

**Table A-6** Exchange Protocol agent required attributes

| Required Attributes | Type - Dimension | Definition |
|---|---|---|
| Protocol | string-scalar | The Exchange protocol for which the Exchange protocol server is configured. This attribute could take any of the following values:<br>■ POP3SVC<br>■ W3SVC<br>■ IMAP4SVC<br>■ SMTPSVC |

**Table A-7** Exchange Protocol agent optional attributes

| Optional Attribute | Type - Dimension | Definition |
|---|---|---|
| DetailMonitor | integer-scalar | For internal use. |

Appendix B

# Sample configuration

This chapter contains the following topics:

# About sample configurations

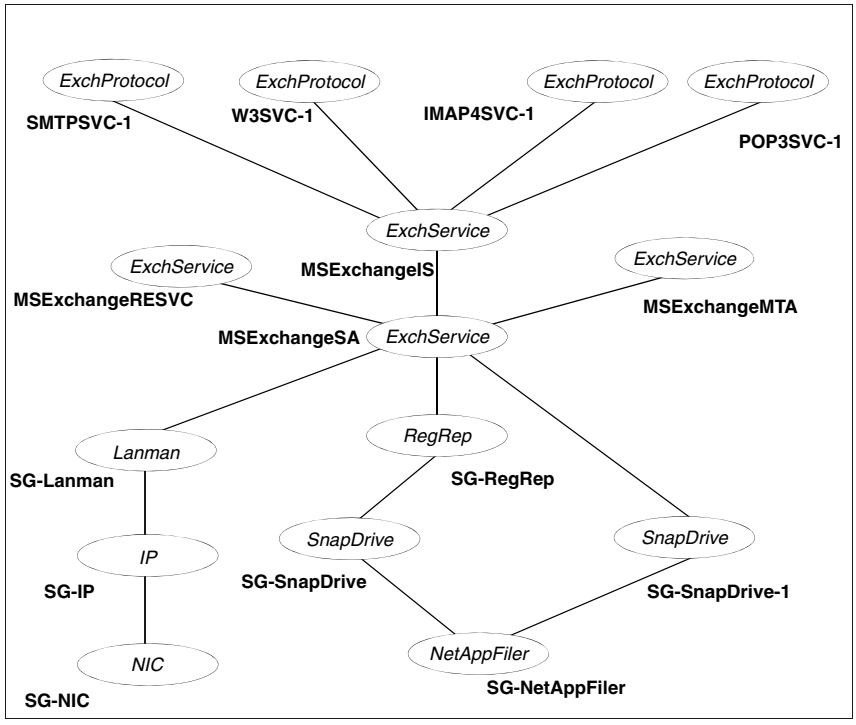
The sample configurations in this appendix describe typical service groups configured to monitor the state of the Exchange Server in a VCS cluster. The appendix lists the sample configuration for clusters using Network Appliance filers to manage shared storage.

The sample configuration graphically depicts the resource types, resources, and resource dependencies within the service group. The sample configuration files (main.cf) are also included for your reference. For more information about these resource types, see the chapter *Veritas Cluster Server Bundled Agents Reference Guide*.

# Dependency graph (local cluster configuration)

The following dependency graph shows a VCS service group that has Network Appliance related resources.

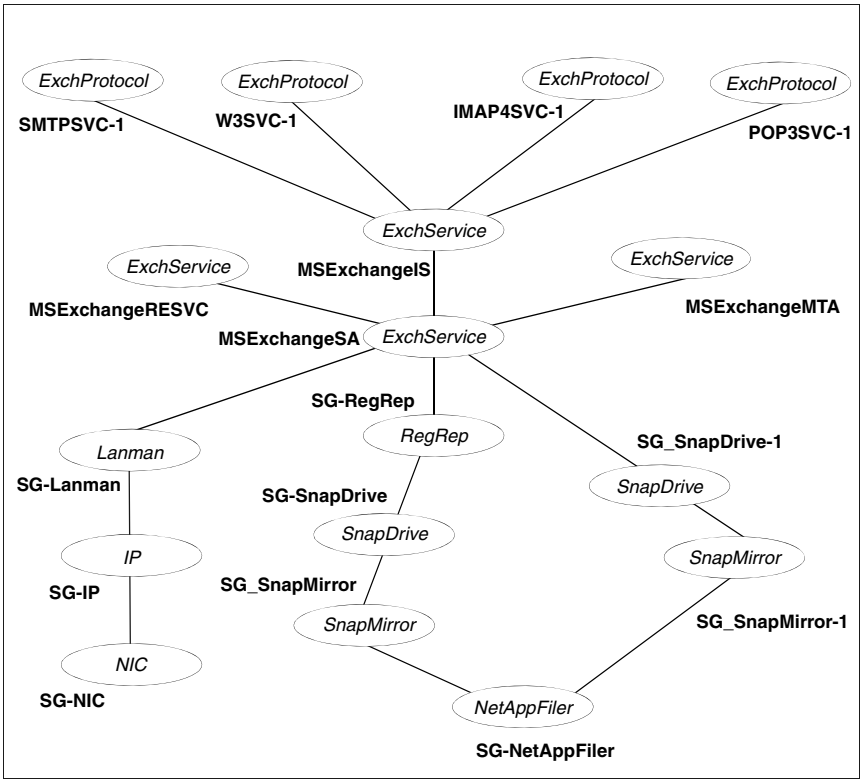
**Figure B-1** Local cluster configuration dependency graph



# Dependency graph (disaster recovery configuration)

The following dependency graph shows a VCS service group in a cluster that is a part of a global cluster.

**Figure B-2** Disaster Recovery configuration dependency graph



# Sample configuration (local cluster configuration)

```
include "types.cf"

cluster cl50_51 (
    UserNames = { "Administrator@zen" = ch }
    ClusterAddress = "10.121.60.165"
    Administrators = { "Administrator@zen" }
    SecureClus = 1
    )
remotecluster secondary (
    ClusterAddress = "10.121.119.90"
    )

heartbeat Icmp (
    ClusterList = { secondary }
    AYATimeout = 30
    Arguments @secondary = { "10.121.119.90" }
    )

system VCSW2K250 (
    Limits = { ExchLoad = 10 }
    )

system VCSW2K251 (
    Limits = { ExchLoad = 10 }
    )

group ClusterService (
    SystemList = { VCSW2K250 = 0, VCSW2K251 = 1 }
    AutoStartList = { VCSW2K250, VCSW2K251 }
    )

    IP csg_ip (
        Address = "10.121.60.165"
        SubNetMask = "255.255.253.0"
        MACAddress @VCSW2K250 = "00:0D:56:B8:1F:76"
        MACAddress @VCSW2K251 = "00:0D:56:B8:1F:82"
        )

    NIC csg_nic (
        MACAddress @VCSW2K250 = "00:0D:56:B8:1F:76"
        MACAddress @VCSW2K251 = "00:0D:56:B8:1F:82"
        )

    Process wac (
        StartProgram @VCSW2K250 = "C:\\Program
        Files\\Veritas\\Cluster Server\\bin\\wac.exe"
        StartProgram @VCSW2K251 = "C:\\Program
        Files\\Veritas\\Cluster Server\\bin\\wac.exe"
```

```
        StopProgram @VCSW2K250 = "C:\\Program
        Files\\Veritas\\Cluster Server\\bin\\wacstop.exe"
        StopProgram @VCSW2K251 = "C:\\Program
        Files\\Veritas\\Cluster Server\\bin\\wacstop.exe"
        MonitorProgram @VCSW2K250 = "C:\\Program
        Files\\Veritas\\Cluster Server\\bin\\wacmonitor.exe"
        MonitorProgram @VCSW2K251 = "C:\\Program
        Files\\Veritas\\Cluster Server\\bin\\wacmonitor.exe"
        )

    csg_ip requires csg_nic
    wac requires csg_ip

    // resource dependency tree
    //
    //  group ClusterService
    //  {
    //  Process wac
    //      {
    //      IP csg_ip
    //          {
    //          NIC csg_nic
    //          }
    //      }
    //  }

group EX1 (
    SystemList = { VCSW2K251 = 1, VCSW2K250 = 0 }
    Authority = 1
    Prerequisites = { ExchLoad = 10 }
    )

    ExchProtocol EX1-ExchProtocol-POP3SVC-1 (
        Protocol = POP3SVC
        VirtualServer = "Default POP3 Virtual Server"
        LanmanResName = EX1-Lanman
        )

    ExchProtocol EX1-ExchProtocol-SMTPSVC-1 (
        Protocol = SMTPSVC
        VirtualServer = "Default SMTP Virtual Server"
        LanmanResName = EX1-Lanman
        )

    ExchProtocol EX1-ExchProtocol-IMAP4SVC-1 (
        Protocol = IMAP4SVC
        VirtualServer = "Default IMAP4 Virtual Server"
        LanmanResName = EX1-Lanman
        )

    ExchProtocol EX1-ExchProtocol-W3SVC-1 (
        Protocol = W3SVC
```

```
    VirtualServer = "Exchange Virtual Server"
    LanmanResName = EX1-Lanman
    )

ExchService EX1-ExchService-MSExchangeSA (
    Service = MSExchangeSA
    LanmanResName = EX1-Lanman
    )

ExchService EX1-ExchService-MSExchangeIS (
    Critical = 0
    Service = MSExchangeIS
    LanmanResName = EX1-Lanman
    )

ExchService EX1-ExchService-MSExchangeMTA (
    Service = MSExchangeMTA
    LanmanResName = EX1-Lanman
    )

ExchService EX1-ExchService-RESVC (
    Service = RESVC
    LanmanResName = EX1-Lanman
    )

ExchService EX1-ExchService-MSExchangeMGMT (
    Service = MSExchangeMGMT
    LanmanResName = EX1-Lanman
    )

IP EX1-IP (
    Address = "10.121.60.169"
    SubNetMask = "255.255.253.0"
    MACAddress @VCSW2K251 = "00-0D-56-B8-1F-82"
    MACAddress @VCSW2K250 = "00-0D-56-B8-1F-76"
    )

Lanman EX1-Lanman (
    VirtualName = NEW
    IPResName = EX1-IP
    DNSUpdateRequired = 1
    ADUpdateRequired = 1
    ADCriticalForOnline = 1
    )

NIC EX1-NIC (
    MACAddress @VCSW2K251 = "00-0D-56-B8-1F-82"
    MACAddress @VCSW2K250 = "00-0D-56-B8-1F-76"
    )

NetAppFiler EX1-NetAppFiler (
    FilerName = vcsnetapp1
```

```
    StorageIP = "10.121.60.156"
    )

NetAppSnapDrive EX1-NetAppSnapDrive (
    Critical = 0
    FilerResName = EX1-NetAppFiler
    VolumeName = vol7
    ShareName = data07
    LUN = "d71.lun"
    MountPath = J
    Initiator @VCSW2K251 = { "21:00:00:e0:8b:10:05:f3",
         "21:00:00:e0:8b:8f:a3:a8" }
    Initiator @VCSW2K250 = { "21:00:00:e0:8b:10:50:9e",
         "21:00:00:e0:8b:90:db:1b" }
    )

NetAppSnapDrive EX1-NetAppSnapDrive-1 (
    Critical = 0
    FilerResName = EX1-NetAppFiler
    VolumeName = vol7
    ShareName = data07
    LUN = "d70.lun"
    MountPath = I
    Initiator @VCSW2K251 = { "21:00:00:e0:8b:10:05:f3",
         "21:00:00:e0:8b:8f:a3:a8" }
    Initiator @VCSW2K250 = { "21:00:00:e0:8b:10:50:9e",
         "21:00:00:e0:8b:90:db:1b" }
    )

NetAppSnapMirror EX1-NetAppSnapMirror (
    Critical = 0
    FilerResName = EX1-NetAppFiler
    VolumeName = vol7
    AppResName = EX1-ExchService-MSExchangeIS
    )

RegRep EX1-RegRep (
    MountResName = EX1-NetAppSnapDrive
    ReplicationDirectory = "\\VCS\\Private\\RegRep\\Exch"
    Keys = {
         "HKLM\\SYSTEM\\CurrentControlSet\\Services\\IMAP4Svc" =
        "",
        "HKLM\\SYSTEM\\CurrentControlSet\\Services\\
        MSExchangeDSAccess" = "",
        "HKLM\\SYSTEM\\CurrentControlSet\\Services\\
        MSExchangeIS" = "",
        "HKLM\\SYSTEM\\CurrentControlSet\\Services\\
        MSExchangeMTA" = "",
        "HKLM\\SYSTEM\\CurrentControlSet\\Services\\
        MSExchangeSA" = "",
        "HKLM\\SYSTEM\\CurrentControlSet\\Services\\
        POP3Svc" = "",
```

```
"HKLM\\SOFTWARE\\Network Appliance\\
SnapManager for Exchange\\Client" = "",
"HKLM\\SOFTWARE\\Network Appliance\\
SnapManager for Exchange\\Server" = "" }
    RestoreLocally = 1
    )

EX1-ExchProtocol-POP3SVC-1 requires
EX1-ExchService-MSExchangeIS
EX1-ExchProtocol-SMTPSVC-1 requires
EX1-ExchService-MSExchangeIS
EX1-ExchProtocol-IMAP4SVC-1 requires
EX1-ExchService-MSExchangeIS
EX1-ExchProtocol-W3SVC-1 requires EX1-ExchService-MSExchangeIS
EX1-ExchService-MSExchangeSA requires EX1-NetAppSnapDrive-1
EX1-ExchService-MSExchangeSA requires EX1-RegRep
EX1-ExchService-MSExchangeSA requires EX1-Lanman
EX1-ExchService-MSExchangeIS requires
EX1-ExchService-MSExchangeSA
EX1-ExchService-MSExchangeMTA requires
EX1-ExchService-MSExchangeSA
EX1-ExchService-RESVC requires EX1-ExchService-MSExchangeSA
EX1-ExchService-MSExchangeMGMT requires
EX1-ExchService-MSExchangeSA
EX1-IP requires EX1-NIC
EX1-Lanman requires EX1-IP
EX1-NetAppSnapDrive requires EX1-NetAppFiler
EX1-NetAppSnapDrive requires EX1-NetAppSnapMirror
EX1-NetAppSnapDrive-1 requires EX1-NetAppFiler
EX1-NetAppSnapDrive-1 requires EX1-NetAppSnapMirror
EX1-NetAppSnapMirror requires EX1-NetAppFiler
EX1-RegRep requires EX1-NetAppSnapDrive
```

# Index

## W