Veritas™ Cluster Server for NetApp SnapMirror Installation and Configuration Guide for Microsoft Exchange

Windows 2000, Windows Server 2003

5.0

11293746

symantec.

Veritas Cluster Server for NetApp SnapMirror Installation and Configuration Guide for Microsoft Exchange

VCS for NetApp SnapMirror 5.0

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

VCS for NetApp SnapMirror is a licensed product. See the Licensing section in this guide for license installation instructions.

Technical support

For technical assistance, visit http://entsupport.symantec.com 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

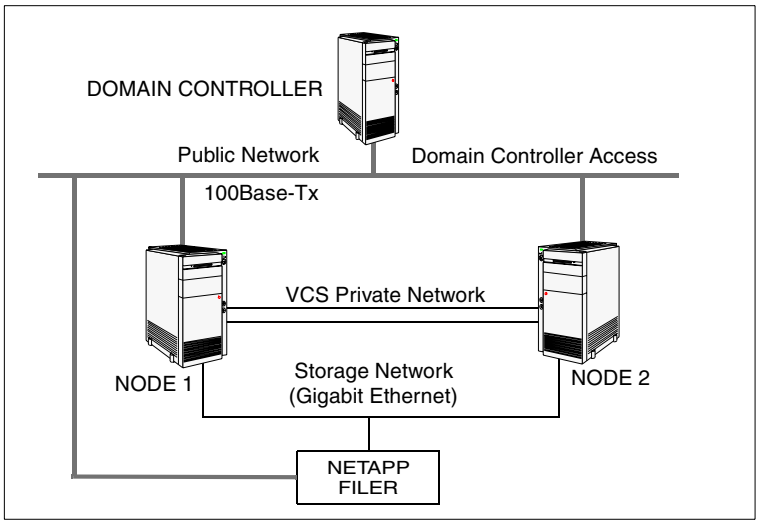
Introduction

The VCS enterprise agent for Microsoft Exchange Server provides high availability to Exchange Server. The VCS enterprise agent for Network Appliance SnapMirror enables configuring Network Appliance filers in a VCS 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.

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



VCS nodes are physically attached to the Network Appliance filer via an ethernet cable supporting iSCSI as the transport protocol.

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 125.

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 enterprise agent for Microsoft Exchange contains two 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 provided 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 Information Store (MSExchangeIS): The Exchange storage used to hold messages in users' mailboxes and in public folders.
- Microsoft Exchange System Attendant (MSExchangeSA): The Exchange component responsible for maintenance and ensuring that operations run smoothly.
- 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 operations

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

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 operations

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

VCS enterprise agent for Network Appliance

The VCS enterprise 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 protocol.
- NetAppSnapMirror agent—Determines the role of the filer volumes with respect to replication and promotes a read-only snapmirrored volume to a read-write source volume during a wide-area failover.

NetApp Filer agent

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

Agent operation

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

NetApp SnapDrive agent

The NetApp SnapDrive agent monitors, connects, and disconnects filer volumes. The agent uses the iSCSI protocol.

Agent operations

- Online—Connects a virtual disk (LUN) using an iSCSI 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 the iSCSI service is running on the filer. If the service is not running, the entry point starts the service.
- Clean—Attempts to forcibly disconnect a virtual disk (LUN).

NetApp SnapMirror agent

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

Agent operations

- Online—If the state of the local filer device is SOURCE, the agent creates a lock file to indicate that the resource can come online. This effectively makes the devices writable for the application.
  If the state of the local filer is TARGET, 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. The Online entry point touches a lock file if Read Write access is enabled successfully.
- Offline—Removes the lock file. The agent does not perform any filer operations because an offline entry point does not necessarily indicate an intention to give up the devices.
- Monitor—Verifies the lock file exists. If the lock file exists, the monitor entry point reports the status of the resource as online. If the lock file does not exist, the monitor entry point reports the status of the resource as offline.
- Open—Removes the lock file, thereby preventing potential concurrency violation if the group fails over to another node.

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

- Clean—Removes the lock file. No filer operations are performed since offlining this resource is no indication of a pending role swap.

How the agents make Microsoft Exchange highly available

The VCS enterprise 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 103 for more information.

Typical Exchange configurations in a VCS cluster

The VCS enterprise agent for Microsoft Exchange does not support an Active/Active configuration for Exchange. It supports the Active/Passive and the Any-to-Any configurations. It also supports the Disaster Recovery configuration.

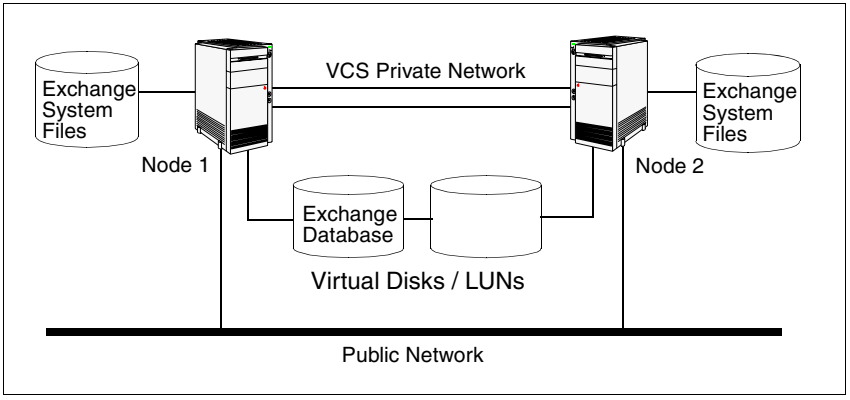
Active/Passive failover configuration

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 enterprise agent for Microsoft Exchange are installed on both nodes. The Exchange database is on shared storage. The shared storage can be managed using the Network Appliance suite of products.

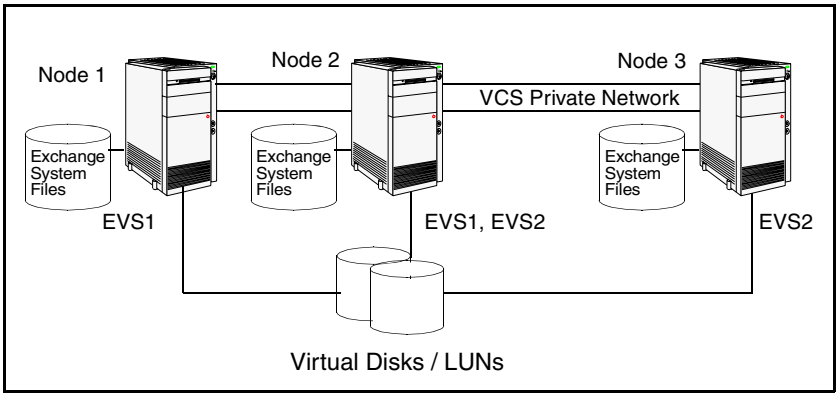
Figure 1-2 Active Passive fail over configuration



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

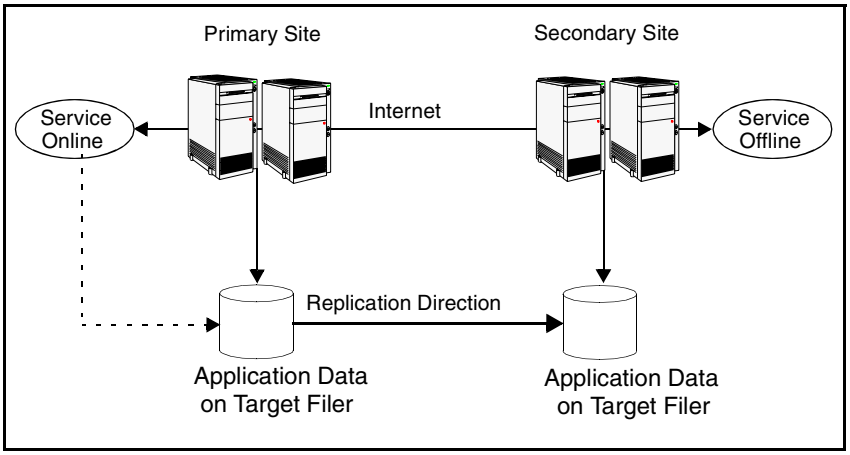


For example, consider a three-node cluster hosting two Exchange virtual servers, EVS1 and EVS2. The virtual servers are configured in VCS in two service groups such that nodes 1 and 2 host the EVS1 service group and nodes 2 and 3 host the EVS2 service group. If node 1 (or node 3) fails, the service group 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 an environment that is prepared for a disaster with a DR solution. 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 software

This chapter describes how to install the software and presents key considerations. For information on upgrading from a previous version, see “Upgrading VCS for Network Appliance SnapMirror” on page 32.

Licensing

Licensing is based on the Microsoft Windows 2000 Server or Windows Server 2003 operating systems in use on a specific server. For each system that runs any of the Symantec products, you need a license.

Note: License keys for previous releases (4.2 or 4.3) are not supported in release 5.0 of VCS for NetApp SnapMirror.

Evaluation license key

An evaluation license key is embedded in the product. To use this key click Next at the license key entry screen of the product installer. This license key is valid for a limited evaluation period only.

You must purchase the product to obtain a permanent license key.

Virtual Server license policy

Each copy of the VCS for NetApp SnapMirror including all options and agents, whether used on a physical server or within a virtual machine must be separately licensed. Each Licensed Software license specifies the number of instances of the Licensed Software you may run on a particular server at one time.

License management

The product installer allows you to add and remove specific licenses. Adding a license for an option does not install the option. Use the Add/Remove function to install an option. License keys support installation on multiple systems.

Symantec License Inventory Manager

The Symantec License Inventory Manager is an enterprise asset management tracking tool. It determines all the Symantec software products and licenses being used in your network. The Symantec License Inventory Manager is available separately. To order a Symantec License Inventory Manager license and media kit, contact your Symantec sales representative.

See "Configuring the Symantec License Inventory Agent" on page 141.

Vxlicrep

Vxlicrep is a command line tool that generates a report of the licenses in use on your system.

To use Vxlicrep to display a license report:

Open the command prompt.

Enter **vxlicrep** without any options to generate a default report.

Optionally, use one of the following options to produce the type of report needed:

-g default report

-s short report

-e enhanced/detailed report

-h display this help

Prerequisites

Before you install VCS for NetApp SnapMirror, verify that your configuration meets the following criteria. Refer to the Hardware Compatibility List on the Symantec Support Web site at http://entsupport.symantec.com to determine the approved hardware for SFW HA.

Supported software

- Microsoft Exchange servers and their operating systems. Note that all systems must be running the same operating system:
  - Microsoft Exchange Server 2003 Standard Edition or Enterprise Edition (SP2 required)
    with
    Windows 2000 Server, Advanced Server, or Datacenter Server (all require Service Pack 4 with Update Rollup1)
    or
    Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) (SP 1 required for all editions)
    or
    Windows Server 2003 R2 (Standard Edition, Enterprise Edition, or Datacenter Edition)

  or

  - Microsoft Exchange 2000 Server or
    Microsoft Exchange 2000 Enterprise Server (SP3 with August 2004 rollup patch required for both editions)
    with
    Windows 2000 Server, Advanced Server, or Datacenter Server (all require Service Pack 4 with Update Rollup1)

  Note: Microsoft support for Exchange Server 2003 is limited to 32-bit versions of the Windows 2003 operating system.

- Veritas Cluster Server (VCS) for Windows with Veritas Cluster Server Application Agent for Microsoft Exchange
- Network Appliance Data ONTAP 7.0.4
- Network Appliance SnapDrive 3.2
- Network Appliance SnapManager for Exchange version 3.1
- Microsoft iSCSI software initiator version 2.0

System requirements

- Verify that all systems have adequate resources to run Exchange Server and VCS.
- VCS requires administrator privileges to install the software.
- Verify the systems on which you install the software are part of a Windows 2000 or Windows 2003 domain.

Software requirements

- The following software must be installed on each node:
  - Microsoft iSCSI Initiator.
  - Network Appliance SnapDrive.
    When installing SnapDrive, you must specify a user account in the **SnapDrive Service Credentials** dialog box. The user account must be a domain user and part of the Administrators group of the local system and the filer.
  - Network Appliance SnapManager for Exchange.
- If you use Windows 2003 systems, install ONTAP 7.0.4 on the filers.
- You must have licenses for Network Appliance SnapMirror and SnapRestore (for Disaster Recovery configurations).

Configuration requirements

- Make sure the filers reside in the same domain as the systems.
- Make sure the filers can replicate in both directions.
- The user account for the VCS Helper service must be a member of the administrators group on the filers.
- If you plan to set up a disaster recovery configuration, make sure the volumes at both sites are of the same size.
- Set up a private network for the shared storage. Assign an IP address to each adapter in the private network.
- Configure the Common Internet File System (CIFS) for each volume. See the Network Appliance documentation for instructions.
- Disable the Windows Firewall on systems running Windows Server 2003 SP1.

Installing the software using the product installer

Before installing the software on remote systems running Windows 2003, you must modify the driver signing options to ignore warning messages about software authentication.

To modify driver signing options for Windows 2003

1. Open the Driver Signing Options dialog box by using either of the following methods:
   - From Windows Explorer, right-click **My Computer,** and click **Properties**. On the **Hardware** tab, click **Driver Signing** in the Device Manager box.
     or
   - Open the Control Panel and double-click **System**. On the **Hardware** tab, click **Driver Signing** in the Device Manager box.
2. In the Driver Signing Options dialog box, check **Ignore**, and click **OK**.

To install the products using the installer

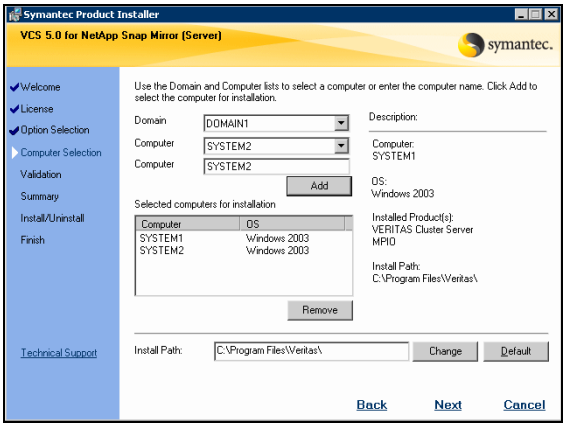
The examples in the following procedure are based on a Custom/Complete installation.

1. From Windows Explorer, navigate to the root directory of the VCS for Network Appliance CD and double-click **Setup.exe**.
2. From the Select a language drop-down list, select **English** as the language and click **OK**.
3. Click **Product Installation** in the left pane, then click the product name.
4. Click **Complete/Custom**.
   The Complete/Custom installation installs server components and optional client components. Click **Administrative Console** if you wish to install only the client components. This will install the VCS Java Console.
5. Review the information on the Welcome panel and click **Next**.
6. Read the License Agreement by using the scroll arrows in the view window. If you agree to the license terms, click **I accept the terms of the license agreement** and then click **Next**.
7. In the Enter a license key and click Add field, type the license key, click **Add**, and then click **Next**. The License Key Details section displays more information about the selected key. To delete a license key, select the key from the key list and click **Remove**.

8 On the Option Selection panel, check the following product options and click **Next**:

- **VCS 5.0 for NetApp Snap Mirror (Server)**
- **Global Clustering Option** - if you plan to configure a disaster recovery environment.
- **High Availability Hardware Replication Agents**
- **High Availability Application Agents**
- **VCS 5.0 for NetApp Snap Mirror (Client)** - This will install the VCS Java Console on the same nodes where the server components are installed.

9 On the Computer Selection panel, specify the domain and nodes for the installation and click **Next**.



Domain	Select the domain from the drop-down list.
Computer	Select the computer name from the dropdown list. This may take some time to populate depending on the domain and network size, speed, and activity. Alternatively, if you know the computer name, type the name in the Computer field.
Add	Click **Add** to add the computer for installation.
Selected computers for installation	The Selected computers for installation section displays the list of computers that you have added for installation. To remove a computer, click a computer name and click **Remove**.

Install Path

The Install Path field displays the default path for installation. To specify a different installation path for a computer:

1. Select the computer name from the Selected computers for installation list.
2. Type the path in the Install Path field.
3. Click **Change** and then click **Yes** to confirm the changes.

To restore the default installation path for a computer: Select the computer name from the Selected computers for installation list and then click **Default**.

10. After the installer validates the systems for the installation, click **Next**. If an error occurs, address the problem described in the Details box, click **Validate Again**, and click **Next**.
11. Review the summary information and click **Install**. If necessary, click **Back** to make changes.
12. If an installation is not successful on any of the systems, the status screen shows a failed installation. If the installation is successful on all systems, click **Next** after the progress indicator shows the installation is completed.

    If a security alert asks you to accept the Veritas driver software, click **Yes**.
13. Review the installation report and click **Next**.
14. Reboot the remote nodes:
    - Select the remote nodes on which the installation took place.
    - Click **Reboot**.
    - Click **Next**.
15. Click **Finish**.
16. Click **Yes** to reboot the local node.

To ensure a secure system environment, change the driver signing options for the remote Windows 2003 systems to the original state of **Warn** or **Block**.

Installing the software from the command line

You can perform a silent installation from the command prompt using the `Setup.exe` command. See the examples at the end of this section for reference.

To start the installation from the command window

1. Insert the product software disc into a drive connected to the system.
2. Click **Start** > **Run.**
3. Enter **cmd** in the Open field and click **OK**.
4. From the command window, navigate to the root directory of the product software disc.
5. Use the following command to install the software:

```
Setup.exe /s [INSTALL_MODE=InstallMode] [SOLUTION=Solution]
    LICENSEKEY="LicenseKey" [OPTIONS="a,b,c,..."]
    [INSTALLDIR="InstallDirPath"] [REBOOT=RebootMode]
```

Where the total length of the argument string is 512 characters.

Parameters for Setup.exe

Information about the possible parameter values follows:

InstallMode	Set to indicate an installation or uninstallation. ***1*** = To install ***5*** = To uninstall The default setting is ***1*** to install. Example: **INSTALL_MODE=*1***
Solution	Set to the type of installation. ***6*** = VCS for Network Appliance (Server Components) ***7*** = VCS for Network Appliance (Client Components) The default setting is ***6*** for server components. Example: **SOLUTION=*6***

Note: To install the server and matching client components, run two `Setup.exe /s` commands, one with the SOLUTION parameter set for the server component and the other set for the client component. If you use a script to install the server and client, consider first installing the client and then the server, so that the script can reboot the system after server installation.

LicenseKey	Set the license key for the installation. Enter multiple keys by separating them with a comma (e.g. 123-345-567-789-123,321-543-765-789-321, etc.) The license key must start and end with a quotation mark ("). *LicenseKey* has no default setting. Example: **LICENSEKEY="*123-234-123-234-345*"**
Options	Set the desired options, if any. The option must start and end with a quotation mark ("). There are no default settings. The options for VCS for Network Appliance are: ■ **ntap** ■ **GCO** ■ **exchange** ■ **sql** Example: **OPTIONS="*GCO*"**
InstallDirPath	Set the path of the installation directory. The path must start and end with a quotation mark ("). The default setting is *SystemDrive*:\Program files\Veritas Example: **INSTALLDIR="*C:\InstallationDirectory*"**
RebootMode	Setting for the automatic reboot of the system at the completion of the installation. ***0*** = No reboot ***1*** = Reboot The default setting is 0 for no system reboot. Example: **REBOOT=*1***

Note: Reboot the system at the end of installation to ensure that the software drivers for the server component are installed correctly. You do not have to reboot after installing the client.

Example for Setup.exe: Client Installation

This command installs the client components at the specified installation path and tells the system not to reboot at the end of the installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=7
    INSTALLDIR="C:\InstallationDirectory"
```

Example for Setup.exe: Server Installation

This command installs the server components with a license key of 123-234-123-234-345, and with the GCO option. Determines where the installation path is `C:\InstallationDirectory` and tells the system to reboot at the end of the installation.

```
Setup.exe /s INSTALL_MODE=1 SOLUTION=6
    LICENSEKEY="123-234-123-234-345" OPTIONS="GCO"
    INSTALLDIR="C:\InstallationDirectory" REBOOT=1
```

Configuring Veritas Cluster Server

After installing the software, set up the components required to run Veritas Cluster Server. The VCS Configuration Wizard 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.
- When configuring a user account for the VCS Helper service, choose the administrative account set up on the filer.

For instructions, see the chapter on Getting Started with VCS in the *Veritas Cluster Server Administrator's Guide*.

Upgrading VCS for Network Appliance SnapMirror

Upgrading an Exchange configuration in a VCS cluster involves:

- Upgrading previous versions (4.2 or 4.3) of VCS for Network Appliance SnapMirror to version 5.0.
- Upgrading Microsoft Exchange 2000 SP3 to Microsoft Exchange 2003.

Run the Exchange Upgrade wizard to upgrade Microsoft Exchange Server. After you have upgraded Microsoft Exchange in the VCS cluster, make sure that all failover nodes for an Exchange virtual server have the same version of Microsoft Exchange. All failover nodes must also have the same version of the VCS Application agent for Exchange.

Upgrade scenarios

The following table presents possible scenarios for upgrading to a VCS 5.0 for Network Appliance SnapMirror cluster with Microsoft Exchange.

Table 2-1 VCS for NetApp SnapMirror upgrade scenarios

Scenarios	Upgrade From			Upgrade To		
	VCS for NetApp SnapMirror Version	Operating System	Exchange Version	VCS for NetApp SnapMirror Version	Operating System	Exchange Version
Upgrade tasks for scenario A	4.2 or 4.3	Windows 2000 SP4	Exchange 2000 SP3	*5.0*	Windows 2000 SP4	Exchange 2000 SP3
Upgrade tasks for scenario B	4.2 or 4.3	Windows 2000 SP4	Exchange 2000 SP3	*5.0*	Windows 2000 SP4	*Exchange 2003 SP1*
Upgrade tasks for scenario C	4.2 or 4.3	Windows Server 2000 SP4	Exchange 2003	*5.0*	Windows Server 2000 SP4	*Exchange 2003 SP1*
Upgrade tasks for scenario D	4.2 or 4.3	Windows Server 2003	Exchange 2003	*5.0*	Windows Server 2003	*Exchange 2003 SP1*

Note: After you have upgraded Microsoft Exchange in the VCS cluster, make sure that all failover nodes for an Exchange virtual server have the same version of Microsoft Exchange. All failover nodes must also have the same enterprise agent version.

Upgrade tasks for scenario A

- Stop VCS Services before upgrading. See "Preparing to upgrade VCS for Network Appliance SnapMirror" on page 36.
- Upgrade VCS for NetApp SnapMirror to version 5.0. See "Upgrading to VCS 5.0 for Network Appliance SnapMirror" on page 37.

Upgrade tasks for scenario B

- Perform the pre-upgrade tasks before upgrading Microsoft Exchange Server. See "Performing the pre-upgrade tasks" on page 34 for instructions.
- Upgrade Microsoft Exchange Server. See "Upgrading Microsoft Exchange" on page 35 for instructions.
- Perform the post-upgrade tasks for Microsoft Exchange Server. See "Performing the post-upgrade tasks" on page 35 for instructions.
- Stop VCS Services before upgrading. See "Preparing to upgrade VCS for Network Appliance SnapMirror" on page 36.
- Upgrade VCS for NetApp SnapMirror for Exchange to version 5.0. See "Upgrading to VCS 5.0 for Network Appliance SnapMirror" on page 37 for instructions.

Upgrade tasks for scenario C

- Stop VCS Services before upgrading. See "Preparing to upgrade VCS for Network Appliance SnapMirror" on page 36.
- Upgrade VCS for NetApp SnapMirror to version 5.0. See "Upgrading to VCS 5.0 for Network Appliance SnapMirror" on page 37.

Upgrade tasks for scenario D

- Stop VCS Services before upgrading. See "Preparing to upgrade VCS for Network Appliance SnapMirror" on page 36.
- Upgrade VCS for NetApp SnapMirror to version 5.0. See "Upgrading to VCS 5.0 for Network Appliance SnapMirror" on page 37.

Performing the pre-upgrade tasks

Run the Exchange Upgrade wizard on all nodes where you want to upgrade the Microsoft Exchange server.

To run the Exchange Upgrade wizard

1. Navigate to the `Tools\netapp_agent\Exchange` folder and double-click **Upgrade.exe**.
2. Review the welcome information and click **Next**.
3. Select an Exchange virtual server and click **Next**.
   The Exchange virtual server box lists the servers that are:
   - configured to run on the node where you run the wizard.
   - to be upgraded from Microsoft Exchange 2000 SP3 to Microsoft Exchange 2003.
4. Click **Finish**.
5. A message appears telling you that the system must be restarted after you quit the wizard. Click **Yes** to continue.
6. The wizard starts running commands to set up the VCS environment.
   After you reboot the node, the Exchange virtual server name is temporarily assigned to the node. The wizard restores the original name when you rerun the wizard after upgrading Microsoft Exchange. During this period, all network connections to the node must be made using the temporary name.
   On reboot, VCS prompts you to upgrade Microsoft Exchange. Proceed to the next section for information on updating Microsoft Exchange.

Upgrading Microsoft Exchange

Follow these steps to upgrade Microsoft Exchange.

To upgrade Microsoft Exchange

1. Insert the Microsoft Exchange 2003 installation CD into a CD drive connected to the node.
2. From the command prompt, navigate to the file Setup.exe on the CD and type:
   ```
   <cd_drive>:\Setup\I386> Setup
   ```
3. Follow the wizard instructions to upgrade Exchange. The ActiveDirectory object of the Exchange Virtual Server selected in the pre-upgrade steps is also upgraded.
   Refer to Microsoft Exchange documentation for further information.
4. Reboot the node, if prompted to do so.

Performing the post-upgrade tasks

Run the Exchange Upgrade wizard for post-upgrade steps on all nodes where Microsoft Exchange server is upgraded.

To run the Exchange Upgrade wizard

1. Navigate to the `Tools` folder and double-click **Upgrade.exe**.
2. Read the information on the Welcome panel and click **Next**.
3. At the VCS warning dialog, click **Yes** to continue.
4. The wizard starts running commands to set up the VCS environment. Various messages indicate the status of each task. After all the commands have been executed, click **Next**.
5. Click **Finish**.
6. The wizard prompts you to reboot the node. Click **Yes** to reboot the node.

Changes made during the post-upgrade task do not take effect until you reboot the node.

Preparing to upgrade VCS for Network Appliance SnapMirror

Before starting the upgrade process, use the VCS Java Console to “save and close” the configuration. This operation involves saving the latest configuration to disk and changing the configuration state to read-only mode. You must also stop VCS before attempting the upgrade process.

To save and close the configuration

- From the VCS Java Console, click **Save and Close Configuration** on the Cluster Explorer toolbar.

To take the Exchange Server service group offline

1. From the command prompt, type:

   ```
   C:\> hagrp -offline group_name -sys system_name
   ```

   Where *group_name* is the name of the Exchange Server service group and *system_name* is the node where the group is online.
2. Repeat this command for all service groups that are online.

To stop VCS services

1. One one node, stop HAD on all the cluster nodes. Type:

   ```
   C:\> hastop -all -force
   ```
2. On each node, stop the Veritas VCSComm Startup service on all the cluster nodes. Type:

   ```
   C:\> net stop vcscomm
   ```
3. On each node, stop GAB and LLT on all the cluster nodes. Type:

   ```
   C:\> net stop gab
   C:\> net stop llt
   ```

Upgrading to VCS 5.0 for Network Appliance SnapMirror

Make sure to select the same agents and options while upgrading the software. If you do not want to include the enterprise agents and options in the upgraded cluster, uninstall the agents from the cluster before proceeding.

Changing driver signing options

When upgrading on systems running Windows Server 2003, you must set the Windows driver signing option to ignore software authentication warning messages.

To change the driver signing options

1. Open the Control Panel and click **System**.
2. Click the **Hardware** tab and click **Driver Signing**.
3. In the Driver Signing Options dialog box, note the current setting, and select **Ignore**.
4. Click **OK**.
5. Repeat for each node in the cluster.

If you do not change these options, the installer rejects the node at validation and halts the upgrade. After you complete the upgrading, you should reset the driver signing options to their previous state.

To upgrade the product using the installer

1. Allow the autorun feature to start the installation or double-click **Setup.exe.**
2. Choose the default language for your installation and click **OK**. The product selection screen appears.
3. Click **VCS 5.0 for Network Appliance SnapMirror**.
4. If asked, click **Complete/Custom** to begin installation, otherwise continue to the next step.
5. Review the welcome message and click **Next**.
6. If you agree to the terms of the license agreement, click **Next**.
7. Enter the product license key before adding license keys for features.
   - Enter the license key in the top field and click **Add.**
   - Repeat for additional license keys.
     - To remove a license key, click the key to select it and click **Remove**.
     - To see the license key's details, click the key.
   - Click **Next**.

8 Select the appropriate product options and click **Next**.

9 Select the appropriate installation options and click **Next**.
If any previous VCS agents and options are installed on the node, make sure you select the same agents and options while upgrading. If you do not want to include the agents and options in the upgraded cluster, uninstall them from the cluster before proceeding.

10 To install the client components on all the nodes in your installation, verify that the check box is checked.
Click **Next**.

11 Specify the domain and nodes for the upgrade.
- Select the domain and the node. These lists can take some time to populate depending on domain and network size, speed, and activity.
- To add a computer for installation, click **Add**. You can also type the computer's name in the Computer field.
  To remove a computer, click the computer in the Selected Computers for Installation field, and click **Remove**.
- Optionally, change or restore the default installation path.
  - To change the path, select a computer, add the new path in the Install Path field, and click **Change**.
  - To restore the default path, `C:\Program Files\Veritas`, click **Default**.
- Repeat step b and step c for each node.
  Click a computer's name to see its description.
- Click **Next**.

12 The installer checks the prerequisites for the selected computers and displays the results. Review the information and click **Next**.
Note that the Install Type for the nodes is listed as **Upgrade**. If an error occurs, address the problem described in the **Details** box.

13 If the installer has detected problems, review the messages, taking action where necessary, and click **Yes**.

14 Review the information and click **Install**. Click **Back** to make changes.

15 If the installation is successful on all nodes, the installer automatically proceeds to the installation report. Click **Next**.
If an installation fails, click **Next** to review the report and address the reason for failure. You may have to either repair the upgrade or uninstall and re-install the upgrade to continue.
If a security alert asks you to accept the Veritas driver software, click **Yes**.

16 Reboot the remote nodes. Note that you cannot reboot the local node now, and that failed nodes are unchecked by default.
   - Click the check box next to the remote nodes that you want to reboot.
   - Click **Reboot**.
   - When the nodes have finished rebooting successfully, the Reboot Status shows Online and the **Next** button is available.
   - Click **Next**.
17 Review the log files and click **Finish**.
18 Click **Yes** to reboot the local node.

To ensure a secure system environment, change the driver signing options for the remote Windows Server 2003 systems to the original state of **Warn** or **Block**.

To reset the driver signing options

1 Open the Control Panel, and click **System**.
2 Click the **Hardware** tab and click **Driver Signing**.
3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.
4 Click **OK** and repeat for each upgraded system.

Chapter 3

Installing Microsoft Exchange Server

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 set up, and you want to configure it for high availability, see "Making a standalone Exchange Server highly available" on page 81 for instructions.

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

Overview of tasks

- Meet the prerequisites for installing Microsoft Exchange. See "Prerequisites" on page 42 for more information.
- Install Microsoft Exchange on the first node. See "Installing Exchange on the first node" on page 47 for more information.
- Move Microsoft Exchange database to a shared disk. See "Moving Exchange databases to shared storage" on page 51 for more information.
- Install Microsoft Exchange on additional nodes. See "Installing Exchange on additional nodes" on page 55 for more information.

Prerequisites

- Verify VCS for Network Appliance SnapMirror is installed on the node.
- Verify you have configured a VCS cluster using VCS Configuration Wizard (VCW). See the *Veritas Cluster Server Administrator's Guide* for instructions.
- 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 44 for instructions.
- 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 Application Agent for Microsoft Exchange requires the operating system to be installed on the same local drive on all nodes. For example if you install Windows 2003 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.
- 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.
- Verify that the Microsoft iSCSI Initiator is configured to establish a persistent connection between the Network Appliance filer and the cluster nodes. See the Microsoft documentation for instructions.
- Symantec recommends that you have a minimum of two LUNs (or 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 Veritas wizards.
- Make sure the HAD Helper domain 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

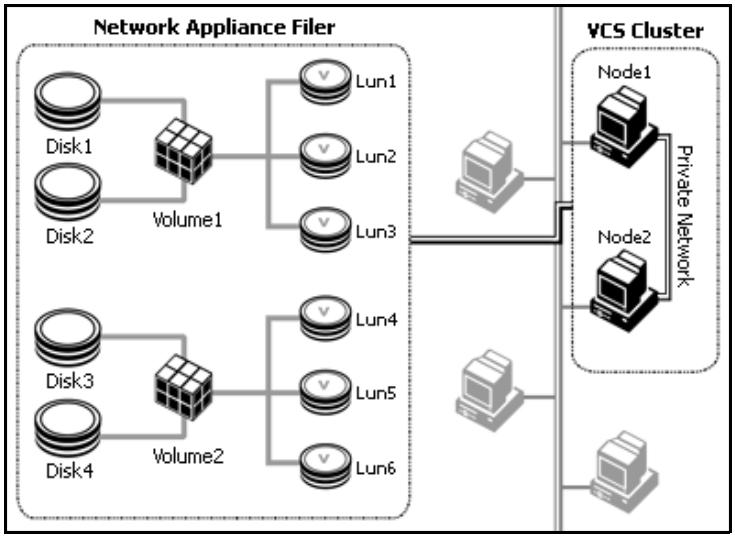
1. Make sure the Microsoft iSCSI Initiator software version 2.0 is installed on all cluster nodes. Refer to Microsoft documentation for further information.
2. Start the Microsoft iSCSI initiator. Double-click the Microsoft iSCSI Initiator icon from the desktop.
3. Click the **Target Portals** tab, if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

Managing storage using Network Appliance filer

Network Appliance manages data by creating volumes on physical disks. These volumes can further be divided into LUNs (Logical Unit Numbers.) The LUNs are accessible from the cluster nodes, provided the nodes have Microsoft iSCSI Initiator and Network Appliance SnapDrive installed.

Note: Symantec does not support volumes created using qtree.

Figure 3-1 VCS cluster in a NetApp storage environment



The VCS enterprise agent for Microsoft Exchange requires two LUNs to be created on the Network Appliance 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 Network Appliance Filer and to make them accessible from cluster nodes:

- Create volumes on the Network Appliance Filer.
- Share the volumes.
- Create LUNs on the shared volumes.

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

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 LUNs created to store the registry replication information and the Exchange database are connected to this node and 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 Wizards > Application Agent for Exchange Server > 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. The wizard validates the system for the prerequisites. Various messages indicate the validation status. Once all the validations are done, click **Next**.
7. 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**.

8 Select a drive where the registry replication data will be stored and 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**.

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. 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: first node" on page 49 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. If you installed Exchange Server 2000, make sure you install Service Pack 3 with August 2004 rollup patch. For Exchange 2003, make sure you install Service Pack 2.
4. Proceed to “Exchange post-installation: first node” on page 50 for instructions on performing the post-installation tasks.

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.

To perform Exchange post-installation

1. If the Exchange installation did not prompt you to reboot the node, click **Continue** from the Exchange Server Setup Wizard and proceed to step 3.
   If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.
2. Review the information in the Welcome panel and click **Next**.
3. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
4. The wizard starts performing the post-installation tasks. Various messages indicate the status. After all the commands are executed, click **Next**.
5. Click **Finish**.
6. When prompted to reboot the node, click **Yes**.
   Changes made during the post-installation phase do not take effect till you reboot the node.

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.

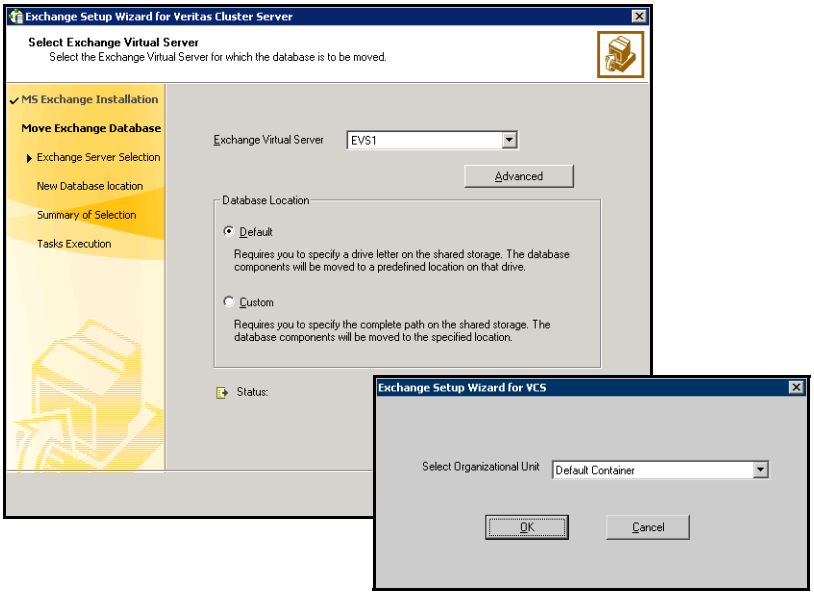
Complete the following tasks before moving the databases:

- Make sure that there is no queued data on the SMTP server.
- Make sure that the LUNs created to store the Exchange database, MTA data, transaction logs, and registry replication information are connected. Disconnect the 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 Wizards > Application Agent for Exchange Server > 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 Select the Exchange virtual server and specify whether you want to move the Exchange databases to a default or 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**.

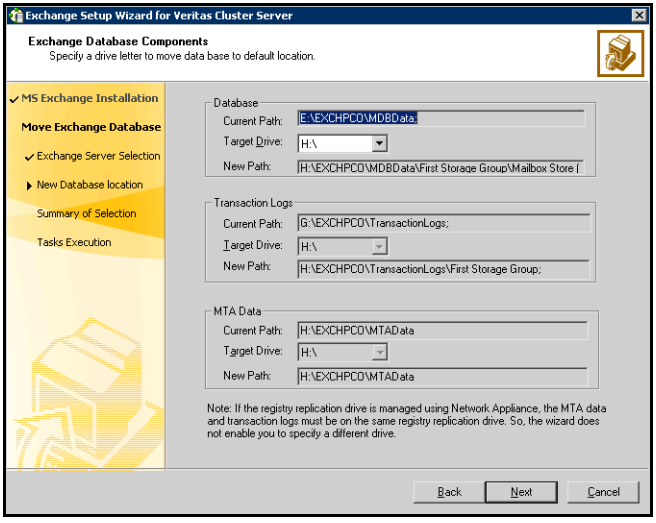
2 From the Organizational Unit drop-down list, select the distinguished name for the Exchange virtual server.
By default, the Lanman resource adds the virtual server to the default container Computers.
The user account for VCS Helper service must have adequate privileges on the specified container to 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. 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.

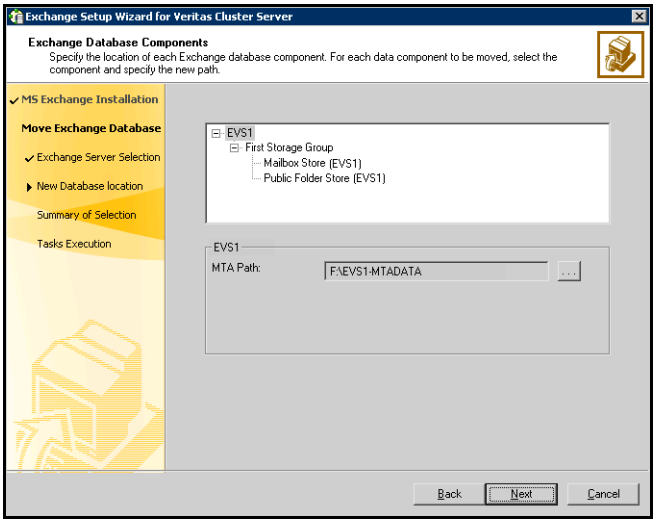
6 On the Exchange Database Components panel, complete the following and then click **Next**.

- 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:



  - The wizard displays disk managed using Windows Disk Management and virtual disks (LUNs). Ensure that you select virtual disks (LUNs) to store the data components.
  - 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.

   To install Microsoft Exchange on additional nodes, proceed to "Installing Exchange on additional nodes" on page 55.

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.

Note: Before adding a node to the Exchange cluster, make sure you meet the prerequisites listed under "Prerequisites" on page 42.

To perform Exchange pre-installation

1. Verify the LUNs created to store the registry replication information and the Exchange database are connected to this node and 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 Wizards > Application Agent for Exchange Server > 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**.
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 57 for instructions.
Click **Revert Changes** to undo all actions performed by the wizard during the pre-installation procedure.

Exchange Server installation: additional nodes

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

To install Exchange Server

1. Install Exchange Server using the Microsoft Exchange installation program. Make sure you install the Microsoft Exchange System Management Tools also. You must install the same components installed on the first node. See the Microsoft Exchange documentation for instructions.
   Make sure to select **Disaster Recovery** in the **Action** column for **Microsoft Exchange System Management Tools**.
2. Reboot the node if prompted to do so.
3. If you installed Exchange Server 2000, make sure that you install Service Pack 3 with August 2004 rollup patch. For Exchange 2003, make sure you install Service Pack 2.
4. Proceed to "Exchange post-installation: additional nodes" on page 58 for instructions on performing the post-installation tasks.

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. If the Exchange installation did not prompt you to reboot the node, click Continue from the Exchange Server Setup Wizard and proceed to step 3.
   If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.
2. Review the information in the Welcome panel and click **Next**.
3. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
4. The wizard starts performing the post-installation tasks. Various messages indicate the status. After all commands are executed, click **Next**.
5. Specify whether you want to add the node to the SystemList of the service group for the EVS selected in step 6 on page 55. 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.
6. Click **Finish**.
7. 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.

After installing Exchange Server on all systems that will participate in the service group, proceed to “Configuring the service group” on page 59 for instructions on how to configure the service group.

Chapter 4

Configuring the service group

Configuring the Exchange service group involves creating resources for the Network Appliance and Exchange resources. 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. The wizard creates and modifies Exchange service groups.

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 70.

Symantec recommends reviewing the resource types and the attribute definitions of the agents before configuring the agents. You can find this information in the appendix “Resource type definitions” on page 125. For sample configuration files and resource dependency graphs of the Exchange service group, see “Sample configuration” on page 133.

Prerequisites

- Verify VCS for Network Appliance SnapMirror is installed on all cluster nodes.
- Verify Exchange is installed and configured identically on all the cluster nodes.
- Verify the cluster is configured using the VCS configuration wizard (VCW).
- 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 virtual disks (LUNs) created to store the following data components are connected to the node where you run the wizard and 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 46 for instructions.
- Make sure to note the list of the Exchange services and Exchange protocol servers to be monitored; the wizard will prompt you for this information.

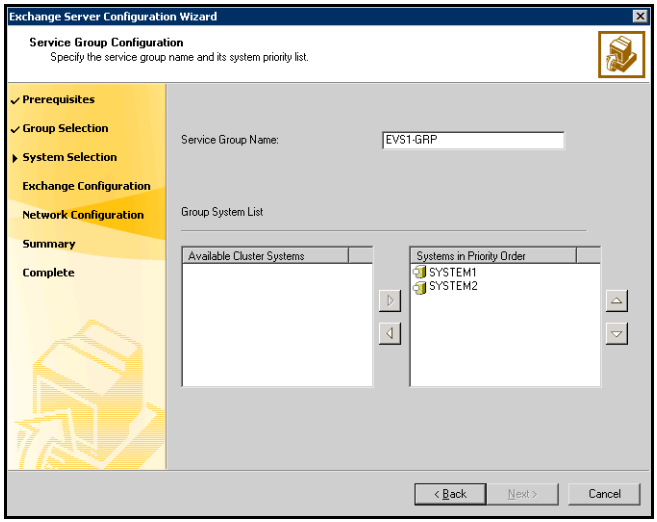
Configuration instructions

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 Wizards > Application Agent for Exchange Server > 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 system priority list and click **Next**. The wizard starts validating your configuration. Various messages indicate the validation status.

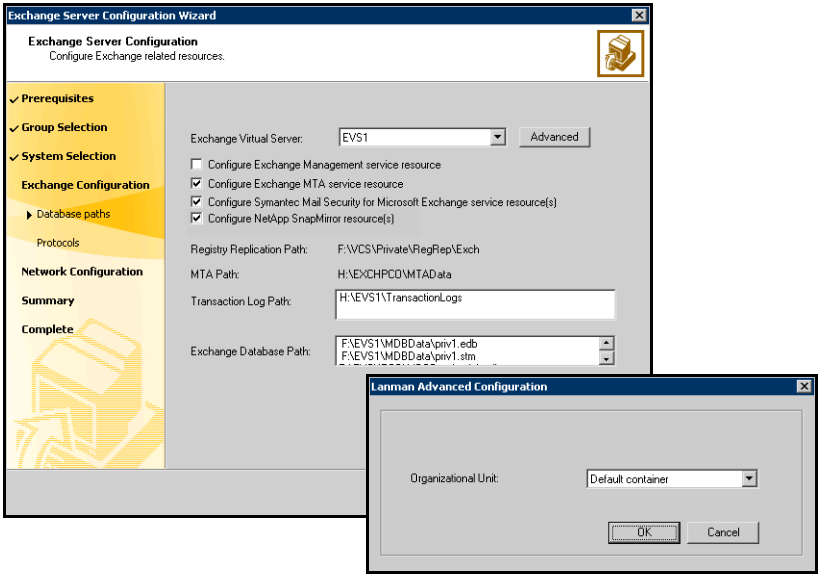


Service Group Name	Type a name for the Exchange service group.
Available Cluster Systems	Select the systems on which to configure the service group and click the right-arrow to move the systems to the Systems in Priority Order box.
Systems in Priority Order	This list represents the service group's system 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.

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

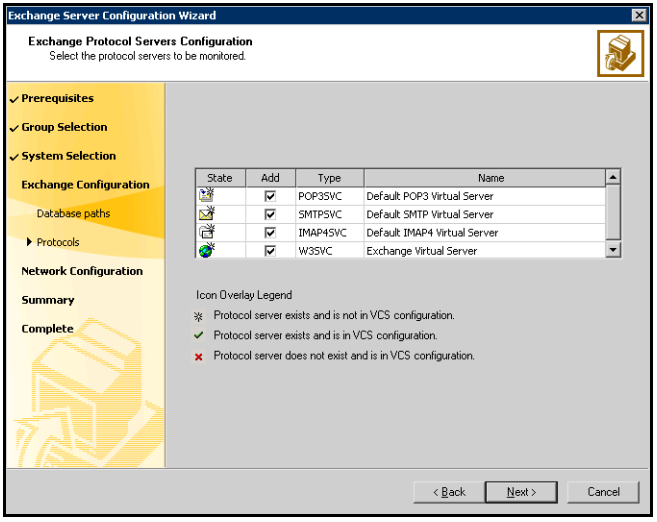
To specify the Lanman resource details:

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**.

Configure Exchange Management service resource	Check this check box if you want to configure the Exchange Management service resource. 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. 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 Symantec Mail Security for Microsoft Exchange service resource(s)	Check this check box if you want to configure the resources for the Symantec Mail Security for Microsoft Exchange services. This option is available only if you have installed Symantec Mail Security for Microsoft Exchange on the system. The wizard will configure resources of type GenericService for the following services: ■ smsmse - Symantec Mail Security for Microsoft Exchange ■ SAVFMSESpamStatsManager - Symantec Mail Security Statistics smsmse resource will be the child of the SAVFMSESpamStatsManager resource and SAVFMSESpamStatsManager resource will be the child of the Microsoft Exchange Information Store (MSExchangeIS) resource. VCS does not replicate data or registry entries related to the Symantec Mail Security for Microsoft Exchange services. You must install and apply the same configuration settings for Symantec Mail Security for Microsoft Exchange, on each failover node in the cluster. If you are running the wizard to modify a service group, unchecking this check box will remove the resources for the Symantec Mail Security for Microsoft Exchange services, from the service group configuration.

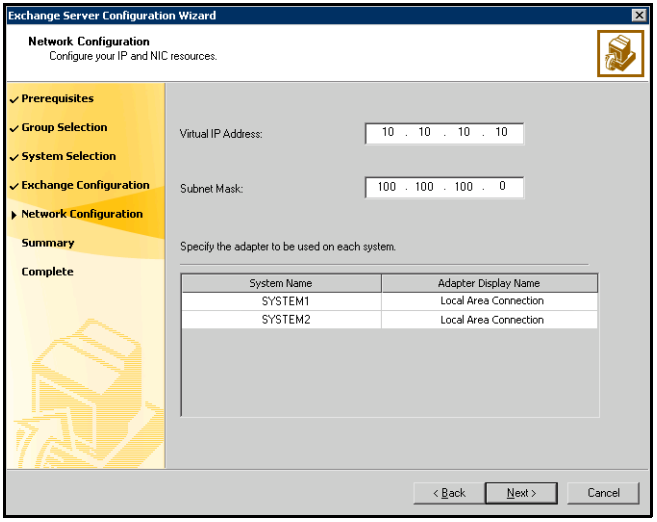
Configure NetApp SnapMirror resource(s)	Check this check box if you want to configure a NetApp SnapMirror resource. SnapMirror resource is required only in case of a disaster recovery configuration. If you are running the wizard to modify a service group, unchecking this check box will remove the NetApp 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.

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 NetApp Filer Configuration panel, click the Storage IP field and select the storage IP address for the NetApp filer and then click **Next**.

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**.

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 volumes 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.

To modify an Exchange service group

1. Start the Exchange Server Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Application Agent for Exchange Server > 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 59 for more information about 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.

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 Wizards > Application Agent for Exchange Server > 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

Adding a node to an Exchange cluster

This chapter describes how to add a failover node to an existing Exchange virtual server in an Exchange cluster, either on the primary site or on the secondary site, using the Exchange Server Setup Wizard for VCS.

Prerequisites

- Make sure the Microsoft Exchange Server was installed in the cluster using the Exchange Server Setup Wizard for VCS.
- Make sure the node to be added was configured using the VCS Configuration Wizard (VCW). Refer to *Veritas Cluster Server Administrator's Guide* for more information.
- Make sure the system has adequate resources to run Microsoft Exchange Server and VCS.
- If the node to be added will be configured as a failover node for an Exchange service group, make sure the service group is offline.
- VCS requires the Microsoft Exchange installation be identical on all nodes in the cluster. So, you must install Microsoft Exchange at the same path on this node as on other nodes in the cluster. Also, you must install all Exchange components that are installed on other nodes in the cluster.

Overview of tasks

Complete the following steps to add a new node to an Exchange cluster:

- Install VCS on the node along with the agents for Network Appliance and Exchange Server. See “Installing the software using the product installer” on page 25 for more information.
- Run VCS Configuration Wizard (VCW) to configure VCS on the node. Refer to the *Veritas Cluster Server Administrator’s Guide* for instructions.
- Run the Exchange Server Setup Wizard for VCS for Exchange pre-installation steps. See “Exchange pre-installation: additional nodes” on page 75 for more information.
- Install Microsoft Exchange. See “Exchange Server installation: additional nodes” on page 77 for more information.
- Run the Exchange Server Setup Wizard for VCS for Exchange post-installation. See “Exchange post-installation: additional nodes” on page 78 for more information.

Installing Exchange on additional nodes

The tasks to be performed on the additional nodes are described in three stages.

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.

Note: Before adding a node to the Exchange cluster, make sure you meet the prerequisites listed under "Prerequisites" on page 42.

To perform Exchange pre-installation

1. Verify the LUNs created to store the registry replication information and the Exchange database are connected to this node and 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 Wizards > Application Agent for Exchange Server > 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 field displays the IP address assigned 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**.
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 77 for instructions.
Click **Revert Changes** to undo all actions performed by the wizard during the pre-installation procedure.

Exchange Server installation: additional nodes

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

To install Exchange Server

1. Install Exchange Server using the Microsoft Exchange installation program. Make sure you install the Microsoft Exchange System Management Tools also. You must install the same components installed on the first node. See the Microsoft Exchange documentation for instructions.
   Make sure to select **Disaster Recovery** in the **Action** column for **Microsoft Exchange System Management Tools**.
2. Reboot the node if prompted to do so.
3. If you installed Exchange Server 2000, make sure you install Service Pack 3 and the August 2004 rollup patch. For Exchange Server 2003, make sure you install Service Pack 2.
4. Proceed to "Exchange post-installation: additional nodes" on page 78 for instructions on performing the post-installation tasks.

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. If the Exchange installation did not prompt you to reboot the node, click Continue from the Exchange Server Setup Wizard and proceed to step 3.
   If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.
2. Review the information in the Welcome panel and click **Next**.
3. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
4. The wizard starts performing the post-installation tasks. Various messages indicate the status. After all commands are executed, click **Next**.
5. Specify whether you want to add the node to the SystemList of the service group for the EVS selected in step 6 on page 75. 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. See "Modifying the service group configuration" on page 70 for instructions.
6. Click **Finish**.
7. 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 the agent on the new node

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

Before proceeding, make sure the Exchange service group is online. See "Bringing the service group online" on page 67 for instructions.

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 6

Making a standalone Exchange Server highly available

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

You can use the same Exchange server name, so users need not reconfigure their mailboxes.

Overview of tasks

Configuring a standalone Exchange Server for high availability involves the following tasks:

- Installing VCS for Network Appliance SnapMirror. See “Installing the software using the product installer” on page 25 for more information.
- Preparing the standalone Exchange Server to be brought under VCS control. See “Preparing the standalone Exchange Server for high availability” on page 83 for more information.
- Bringing the standalone Exchange Server in a VCS environment. See “Bringing the standalone Exchange Server in VCS control” on page 84 for more information.
- Moving the Exchange database to a shared storage. See “Moving Exchange databases” on page 84 for more information.
- Configuring the Exchange agent. See “Configuring the agent” on page 85 for more information.

Preparing the standalone Exchange Server for high availability

Before proceeding, make sure you meet the following requirements:

- The system hosting the Exchange virtual server to be made highly available is not configured as a root broker.
- The system hosting the Exchange virtual server does not have VCS configured.

To prepare a standalone Exchange Server for high availability

1. Verify that the LUNs containing the Exchange database and the registry replication information are connected to this node and disconnected from other nodes in the cluster.
2. 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 Wizards > Application Agent for Exchange Server > Exchange Server Setup Wizard**.
3. Review the information in the Welcome panel and click **Next**.
4. In the Available Option panel, click **Make a standalone Exchange Server highly available** and click **Next**.
5. 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.
   - 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**.
6. Select a drive where the registry replication data will be stored and click **Next**.
   The wizard lists disks managed using Windows Disk Management and virtual disks (LUNs). Make sure to select virtual disks (LUNs) to store registry replication information.

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

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

9 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**.

10 Click **Finish**.
The wizard prompts you to restart the system. Click **Yes** to restart the system. Click **No** to restart the system later.

Bringing the standalone Exchange Server in VCS control

Use the VCS Configuration Wizard (VCW) to configure VCS on the standalone Exchange server. Refer to *Veritas Cluster Server System Administrator's Guide* for more information.

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 51 for instructions.

Configuring the agent

Create an Exchange service group in the cluster using the Exchange Server Configuration Wizard. See “Configuring the service group” on page 59 for instructions.

Your single-node Exchange cluster is ready. You can add nodes to this cluster, and then install Microsoft Exchange on the new nodes. Do not forget to run the Exchange Server Setup Wizard for VCS before installing Microsoft Exchange in a VCS cluster.

For information on adding a node to the cluster, see “Adding a node to an Exchange cluster” on page 73. For information on setting up an any-to-any configuration, see “Configuring any-to-any failover” on page 87.

Chapter 7

Configuring any-to-any failover

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.

Prerequisites

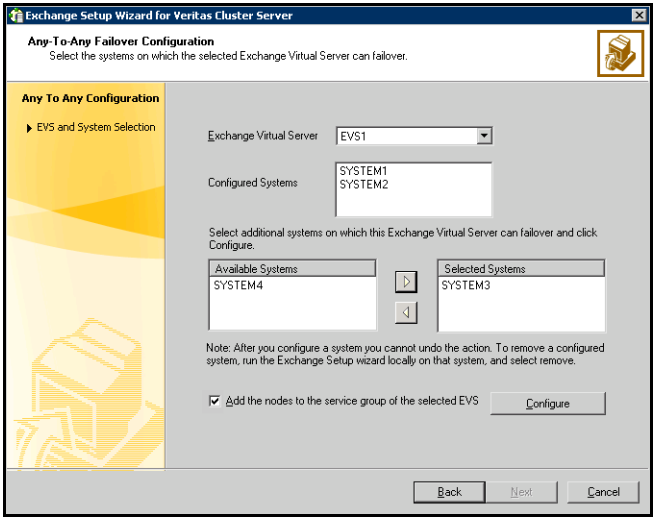
- Make sure you have at least two Exchange virtual servers in the cluster.
- Set up the Exchange cluster in the Active/Passive failover configuration. See previous chapters of this book for more information.

Configuration instructions

These steps describe how to set up an any-to-any failover configuration in an Exchange cluster.

To set up an any to any configuration in an Exchange cluster

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 Wizards > Application Agent for Exchange Server > 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**.

Chapter 8

Deploying agents for disaster recovery

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 using the VCS enterprise agents for Network Appliance SnapMirror and Microsoft Exchange.

Symantec recommends that you configure the secondary site only after you have established a local cluster with the GCO option at the primary site.

Prerequisites

- Configure the ClusterService group, with a WAC resource, at the primary site. Refer to *Veritas Cluster Server Administrator's Guide* for more information.
- Configure the Exchange databases for backup and restore using SnapManager for Exchange configuration wizard. See "Running SnapManager for Exchange" on page 67 for instructions.
- Make sure the volumes at both sites are of the same size.

Overview of tasks

Perform the following tasks to set up a disaster recovery environment:

- Install VCS for Network Appliance SnapMirror with the GCO option at the secondary site. See "Installing the software" on page 21 for more information.
- Use the VCS Configuration Wizard (VCW) to configure a VCS cluster at the secondary site. Configure a ClusterService group with a WAC resource in the cluster at the secondary site. Refer to the *Veritas Cluster Server Administrator's Guide* for more information.
- Meet the prerequisites for installing Microsoft Exchange. See "Prerequisites" on page 42 for more information.
- 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 93 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 101 for more information.
- Configure an Exchange service group with SnapMirror resources at the secondary site. See "Configuring the 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 101 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 in the second cluster, take the Exchange service group offline in the primary cluster.

- Make sure you meet the prerequisites listed under “Prerequisites” on page 42 before proceeding with Exchange installation.
- Make sure the Exchange service group is offline in the primary cluster.
- Connect to the LUNs, created to store the registry replication information and the Exchange database, 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, installation, and post-installation.

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.

To perform Exchange pre-installation

1. Verify the LUNs created to store the registry replication information and the Exchange database on the secondary site are connected to this node and 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 Wizards > Application Agent for Exchange Server > 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. Select the Exchange virtual server for disaster recovery and click **Next**.

8 The installer verifies that the selected node meets the Exchange requirements. When all requirements are validated, 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 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 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.
- Click **Next**.

10 Select a drive where the registry replication data will be stored. Make sure you select the same drive letter as the one used at the primary site for registry replication. Click **Next**.
The wizard lists disks managed using Windows Disk Management and virtual disks (LUNs). Make sure to select virtual disks (LUNs) to store registry replication information.

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.

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. See “Exchange Server installation: first node” on page 95 for instructions.

Click **Revert Changes** 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 Server

1. Install Exchange Server using the Microsoft Exchange installation program. Make sure you install the Microsoft Exchange System Management Tools also. You must install the same components installed on the first node. See the Microsoft Exchange documentation for instructions.

   Make sure to select **Disaster Recovery** in the **Action** column for **Microsoft Exchange System Management Tools**.
2. Reboot the node if prompted to do so.
3. If you installed Exchange Server 2000, make sure you install Service Pack 3 and the August 2004 rollup patch. For Exchange Server 2003, make sure that you install Service Pack 2.
4. Proceed to “Exchange post-installation: first node” on page 95 for instructions on performing the post-installation tasks.

Exchange post-installation: first node

Use the Exchange Server Setup Wizard for Veritas Cluster Server to complete the post-installation tasks. This process reverts the node name to original name.

To run the Exchange post-installation

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

   If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.
2. Review the information in the Welcome panel and click **Next**.
3. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
4. The wizard starts performing the post-installation tasks. Various messages indicate the status. After all commands are executed, click **Next**.
5. Click **Finish**.

6 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 97 for instructions. Otherwise, proceed to “Copying the .CRK file to the primary site” on page 101.

Installing Exchange on additional nodes

Install Exchange on additional nodes in the cluster to configure failover nodes 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.

Note: Before adding a node to the Exchange cluster, make sure you meet the prerequisites listed under "Prerequisites" on page 42.

To perform Exchange pre-installation

1. Verify the LUNs created to store the registry replication information and the Exchange database are connected to this node and 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 Wizards > Application Agent for Exchange Server > 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 assigned in step n on page 94 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**.
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 99 for instructions.
Click **Revert Changes** to undo all actions performed by the wizard during the pre-installation procedure.

Exchange Server installation: additional nodes

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

To install Exchange Server

1. Install Exchange Server using the Microsoft Exchange installation program. Make sure you install the Microsoft Exchange System Management Tools also. You must install the same components installed on the first node. See the Microsoft Exchange documentation for instructions.

   Make sure to select **Disaster Recovery** in the **Action** column for **Microsoft Exchange System Management Tools**.
2. Reboot the node if prompted to do so.
3. If you installed Exchange Server 2000, make sure you install Service Pack 3 and the August 2004 rollup patch. For Exchange Server 2003, make sure that you install Service Pack 2.
4. Proceed to "Exchange post-installation: additional nodes" on page 99 for instructions on performing the post-installation tasks.

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

   If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard is launched automatically.
2. Review the information in the Welcome panel and click **Next**.
3. A message appears informing that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
4. The wizard starts performing the post-installation tasks. Various messages indicate the status. After all commands are executed, click **Next**.
5. Specify whether you want to add the node to the SystemList of the service group for the EVS selected in step 6 on page 97. 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.

6 Click **Finish**.

7 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.

Configuring the service group at the secondary site

See "Configuring the service group using the wizard" on page 59 for instructions on configuring an Exchange service group at the secondary site.

- Make sure the service group has the same name as in the primary cluster.
- Make sure you configure 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 LUNs created to store the registry replication information and the Exchange database are connected to this node and disconnected from other nodes in the cluster.
2. Start the Exchange Server Configuration Wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Application Agent for Exchange Server > 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 9

Removing the software

This chapter describes steps to remove VCS for Network Appliance SnapMirror.

Prerequisites

- 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 123 to resolve errors encountered while removing Microsoft Exchange.

Overview of tasks

Removing VCS for Network Appliance SnapMirror 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 Configuration wizard (VCW). See “Removing the VCS configuration” on page 112 for instructions.
- Remove VCS for Network Appliance SnapMirror. 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 Wizards > Application Agent for Exchange Server > 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 agent.

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 Wizards > Application Agent for Exchange Server > 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. Various messages indicate the status of each command. Once all the commands are executed, click **Next**. 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**.

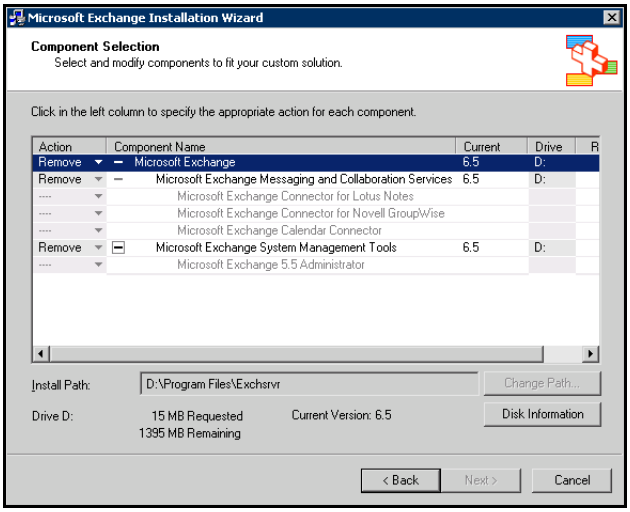
9 The wizard prompts you to restart the node. Click **Yes** to restart the node. If you have other applications running, click **No**, close all applications, and restart the node manually.

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

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

12 In the Microsoft Exchange Installation Wizard Welcome panel, read the welcome information and click **Next**.

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



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

15 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.

16 The Exchange Server Setup Wizard for VCS is launched. The wizard performs the post-uninstallation tasks. Various messages indicate the status of each task. Once all the tasks are complete, click **Next**.

17 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 for Network Appliance SnapMirror, 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 for Network Appliance SnapMirror 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 "Installing the software from the command line" on page 28.

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 for Network Appliance SnapMirror.

To remove VCS for Network Appliance SnapMirror

1. In the **Add/Remove Programs** applet, click VCS for Network Appliance (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**.

License management

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

To add or remove license keys

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

2 Select **VCS for Network Appliance (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 10

Troubleshooting the agents

This chapter describes how to troubleshoot common problems in the VCS enterprise 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

A typical agent log resembles:

```
2003/12/19 15:09:22 VCS INFO V-16-20024-13
ExchService:d1-ExchService-MSExchangeIS:online:Service
(MSEXCHANGEIS) is taking longer to start. Timeout = 10 seconds
```

Here,

- 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.

Network Appliance agents error messages

This section describes the error messages for the NetApp agents.

Table 10-1 Network Appliance agents error messages

Message	Description
Failed to open connection to filer *%s*.	Make sure that the HAD Helper account is part of the administrator's group on the local host and the filer. Make sure the private network is functioning properly. Verify you can ping the IP used for the private storage network. This is the IP defined the StorageIP attribute of the NetAppFiler resource.
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 10-1 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 Initiator on the host. Make sure that you have installed and configured Microsoft iSCSI 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: ■ Filer name ■ Volume name/LUN name ■ Share name ■ Storage IP Verify the configuration definition of the resource. Make sure each attribute is defined correctly.
Unable to create/delete online lock file *%s*. Error code *%s*,	Make sure you have write permissions on the specified directory.

Exchange Protocol agent error messages

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

Table 10-2 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. 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. 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. Solution: Specify a valid value for the attribute.
Configuration error. 'VirtualServer' attribute is not configured.	No value specified for the “Virtual Server” attribute. Solution: Specify a valid value for the attribute.
Configuration error. 'LanmanResName' attribute is not configured.	No value specified for the “LanManResName” attribute. 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. Solution: Provide a valid value for the Lanman resource that pertains to the Exchange server service group.

Table 10-2 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. 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. 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 10-3 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. 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. Solution: Specify a valid value for the attribute.
Configuration error. 'LanmanResName' attribute is not configured.	No value specified for the “LanManResName” attribute. 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. 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. 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 10-3 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, carry out 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.

Appendix A

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.

VCS enterprise agent for Network Appliance

NetApp Filer agent

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

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
}
        str FilerResName
        str VolumeName
        str ShareName
        str LUN
        str MountPath
        str Initiator
)
```

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-scalar	*Name of iSCSI initiator the host uses to connect virtual disks. You can retrieve this value from the Disk Management console.*

NetApp SnapMirror agent

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 filer volume that is to be mounted via iSCSI. 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. Default = - - - -

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.

VCS enterprise agent for Microsoft Exchange

Exchange Service agent

Type definition

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

Attribute definitions

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

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: ■ MSExchangeIS ■ MSExchangeMTA ■ MSExchangeMGMT ■ MSExchangeSA ■ 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. Set this attribute only for resources configured to monitor the MSExchangeIS service; the attribute is ignored for other services.

Exchange Protocol agent

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.
Protocol	string-scalar	The Exchange protocol for which the Exchange protocol server is configured. This attribute could take any of the following values: ■ POP3SVC ■ W3SVC ■ IMAP4SVC ■ SMTPSVC

Table A-7 Exchange Protocol agent optional attributes

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

Appendix B

Sample configuration

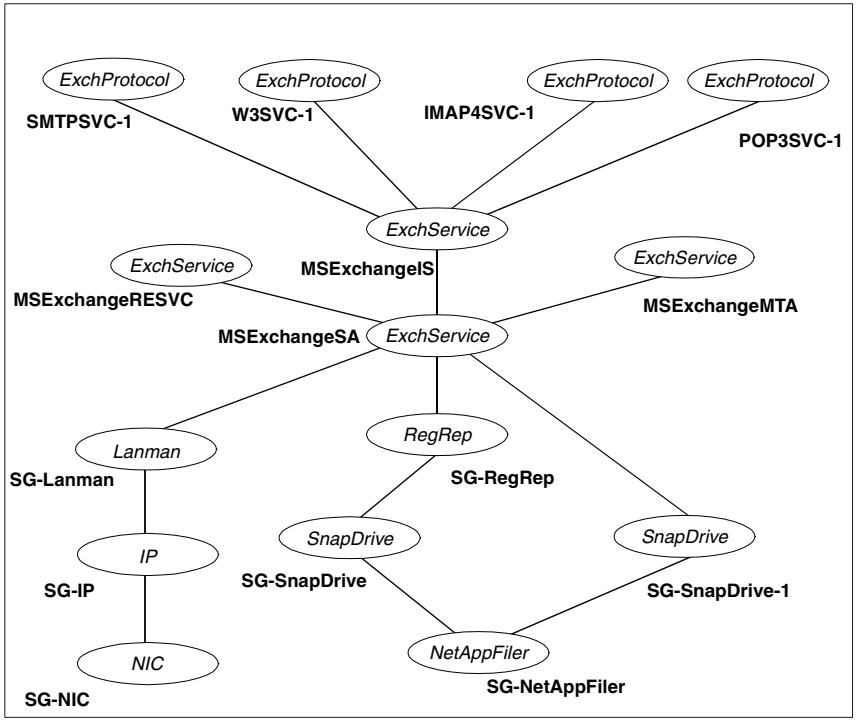
The sample configurations in this appendix describe typical service groups configured to monitor the state of the Exchange Server in a VCS cluster. The appendix lists the sample configuration for clusters using Network Appliance filers to manage shared storage.

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.

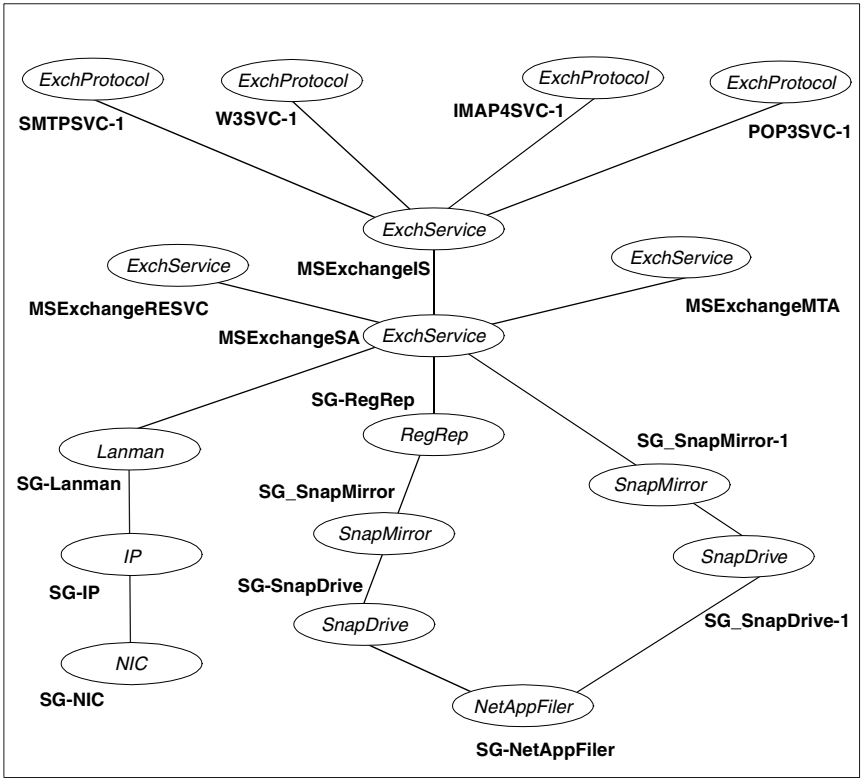
Figure B-1 Local cluster configuration dependency graph



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 NTAP (
    UserNames = { admin = HMNfMHmJNiNNlVNhMK }
    Administrators = { admin }
    CredRenewFrequency = 0
    CounterInterval = 5
)

system THORPC119 (
    Limits = { ExchLoad = 10 }
)

system THORPC120 (
    Limits = { ExchLoad = 10 }
)

group MAILSVR_SG (
    SystemList = { THORPC119 = 1, THORPC120 = 2 }
    Prerequisites = { ExchLoad = 10 }
)

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

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

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

```
ExchProtocol W3SVC-1 (
    Protocol = W3SVC
    VirtualServer = "Exchange Virtual Server"
    LanmanResName = SG-Lanman
)
ExchService MSExchangeSA (
    Service = MSExchangeSA
    LanmanResName = SG-Lanman
)

ExchService MSExchangeIS (
    Service = MSExchangeIS
    LanmanResName = SG-Lanman
)

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

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

IP SG-IP (
    Address = "10.182.147.119"
    SubNetMask = "255.255.252.0"
    MACAddress @THORPC119 = "00-0F-1F-66-C2-17"
    MACAddress @THORPC120 = "00-0F-1F-66-BA-BA"
)

Lanman SG-Lanman (
    VirtualName = MAILSVR
    IPResName = SG-IP
    DNSUpdateRequired = 1
    ADUpdateRequired = 1
    ADCriticalForOnline = 1
)

NIC SG-NIC (
    MACAddress @THORPC119 = "00-0F-1F-66-C2-17"
    MACAddress @THORPC120 = "00-0F-1F-66-BA-BA"
)



NetAppFiler SG-NetAppFiler (
    FilerName = "netapp2.vcsqa.veritas.com"
    StorageIP = "10.10.10.235"
)
```

```
NetAppSnapDrive SG-SnapDrive (
    FilerResName = SG-NetAppFiler
    VolumeName = exchlog
    ShareName = exchlog
    LUN = "e2k3log.lun"
    MountPath = L
    Initiator @THORPC119 =
        "iqn.1991-05.com.microsoft:THORPC119.VCSQA.VERITAS.COM"
    Initiator @THORPC120 =
        "iqn.1991-05.com.microsoft:THORPC120.VCSQA.VERITAS.COM"
)

NetAppSnapDrive SG-SnapDrive-1 (
    FilerResName = SG-NetAppFiler
    VolumeName = exchdb
    ShareName = exchdb
    LUN = "e2k3data.lun"
    MountPath = S
    Initiator @THORPC119 =
        "iqn.1991-05.com.microsoft:THORPC119.VCSQA.VERITAS.COM"
    Initiator @THORPC120 =
        "iqn.1991-05.com.microsoft:THORPC120.VCSQA.VERITAS.COM"
)

RegRep SG-RegRep (
    MountResName = SG-SnapDrive
    ReplicationDirectory = "\\VCS\\Private\\RegRep\\Exch"
    Keys = {
         "HKLM\\SYSTEM\\CurrentControlSet\\Services\\MSExchangeSA",
         "HKLM\\SYSTEM\\CurrentControlSet\\Services\\MSExchangeIS",
         "HKLM\\SYSTEM\\CurrentControlSet\\Services\\MSExchangeMTA",
         "HKLM\\SYSTEM\\CurrentControlSet\\Services\\POP3Svc",
         "HKLM\\SYSTEM\\CurrentControlSet\\Services\\IMAP4Svc" }
)
```

```
SG-RegRep requires SG-SnapDrive
SG-SnapDrive requires SG-NetAppFiler
SG-Lanman requires SG-IP
SG-SnapDrive-1 requires SG-NetAppFiler
MSExchangeSA requires SG-SnapDrive-1
MSExchangeSA requires SG-RegRep
MSExchangeSA requires SG-Lanman
MSExchangeIS requires MSExchangeSA
MSExchangeMTA requires MSExchangeSA
RESVC requires MSExchangeSA
POP3SVC-1 requires MSExchangeIS
SMTPSVC-1 requires MSExchangeIS
IMAP4SVC-1 requires MSExchangeIS
W3SVC-1 requires MSExchangeIS
SG-IP requires SG-NIC
```

Appendix C

Configuring the Symantec License Inventory Agent

This appendix includes the following topics:

About the Symantec License Inventory Manager

The Symantec License Inventory Manager (license inventory manager) is an enterprise asset management tracking tool. It inventories Symantec Information Availability products in your network and consolidates critical information on the deployment of these products. You can use the information to:

- Determine all the Symantec software products and licenses being used in your enterprise
- Achieve easier license self-compliance management
- Know your Enterprise License Agreement deployment status
- Reduce administrative overhead for managing license compliance
- Renew the support and maintenance agreements that are based on the licenses you have deployed
- Gain more control over your Symantec software usage
- Manage the department chargebacks based on actual software usage

- Use more flexible licensing and pricing models
- Exploit detailed deployment data to perform return on investment analyses for purchased software

The license inventory manager is a three-tiered system that consists of a server tier, access point tier, and an agent tier. The server tier is the Symantec License Inventory Server, which consolidates and stores the information that it gathers from the agents and access points.

The optional access point tier includes Symantec License Inventory Access Points and serves as a consolidation layer between the agents and server.

The agent tier includes Symantec License Inventory Agents, which are deployed on individual hosts in a network. Each agent gathers product information on the supported Symantec products that are installed on the agent's host. The agents then send the information they have gathered to an access point or the server.

When the Symantec License Inventory Agent is installed

The Symantec License Inventory Manager is installed using installation media available separately. To order a Symantec License Inventory Manager license and installation media kit, contact your Symantec sales representative.

The installation media provides online documentation for the Symantec License Inventory Manager. You can order printed copies of the documentation from your sales representative. The documents you can order include:

- *Symantec License Inventory Manager Installation and Configuration Guide*
- *Symantec License Inventory Manager Administrator's Guide*
- *Symantec License Inventory Manager User's Guide*

The installation media provides online documentation with details on all of the topics that are discussed in this appendix.

For the latest information on updates, patches, and software issues regarding this product, read the release notes located at:

http://entsupport.symantec.com/docs/285602

The Symantec product installer installs or upgrades the agent on the host with the Symantec product. The agent is installed in the following folder:

`C:\Program Files\Veritas\License Inventory Manager\Agent`

The agent is installed with a default configuration that minimizes its impact on a running system. The minimum configuration prevents remote communication with the agent to keep its data and interfaces secure.

When the server and access points are installed

The server and access points are not installed automatically. If you want to use the Symantec License Inventory Manager, you must manually install the server and, optionally, the access points. After you install the server and access points, the agents can gather information and you can create inventory reports.

You can install the server and access points from the Symantec License Inventory Manager installation media.

What you can do with the agent

After the agent is installed, you can use it to track Symantec products on the system on which it was installed. You can remove the agent if you choose not to use it.

To use the agent, however, you must manually configure it to enable remote communication between the agent and its server or access point. Complete instructions for reconfiguring the agent are provided in the *Symantec License Inventory Manager 4.2 Release Notes*. You can download this document from the following URL:

http://entsupport.symantec.com/docs/285602

How to remove the agent

If you do not want to use the Symantec License Inventory Manager, you can remove the agent using Add/Remove Programs. It is listed as the Symantec License Inventory Agent program in Add/Remove Programs.

Later, you can reinstall the agent with the Symantec License Inventory Manager installation disc. This disc is available in the Symantec License Inventory Manager kit.

Index