NetApp
Go further, faster

Technical Report

Implementation Guide for Veritas Cluster Server and NetApp SnapMirror for Microsoft Exchange Server 2007

Saji Joseph, Amarnath Rampratap, Ratheesh Ramachandran, NetApp

February 2010 | TR-3642

Microsoft
GOLD CERTIFIED
Partner

TABLE OF CONTENTS

1 INTRODUCTION

Today's business requirements, such as high availability, business continuity, and disaster recovery, are more extensive than ever before. Because Microsoft® Exchange has become a mission-critical application in recent years, Microsoft Exchange Server downtime costs companies millions of dollars per year. IT organizations work hard to eliminate or lessen the impact of both planned and unplanned downtime through implementation of high-availability strategies and disaster recovery solutions.

NetApp and Symantec have worked together to extend their reach to increase productivity and keep information close at hand, flexible enough to meet your organization's administrative model.

This technical report serves as an implementation guide for deploying Veritas™ Cluster Server and NetApp® solutions with Microsoft Exchange Server 2007.

2 PURPOSE AND SCOPE

The purpose of this technical report is to present a guide for implementing Veritas Cluster Server and NetApp SnapMirror® integrated with NetApp SnapManager® for Exchange and NetApp SnapDrive® for Windows® with Microsoft Exchange Server 2007 to achieve high availability and recovery in a disaster scenario.

The scope of the solution discussed in this technical report is limited to the following:

- An operational high-availability and disaster recovery solution recommendation for Microsoft Exchange Server 2007, with local and remote switchover options with the help of Veritas Cluster Server and NetApp SnapMirror
- A fully integrated solution can be based on iSCSI SAN or FC SAN

The FC SAN implementation will use Fibre Channel HBAs in the local and remote hosts participating in the Veritas Cluster Server cluster. FCP and iSCSI solutions may optionally use multipath I/O using Data ONTAP® DSM.

iSCSI SAN implementation will use software iSCSI initiators to connect to NetApp storage.

2.1 IMPORTANT NOTES

1. This solution is supported by PVR only. Please file a PVR through CustomerEdge and assign it to NSBU-Rapid Response.
2. VCS entries in IMT are only for Veritas Storage Foundation HA for Windows support. This product is a different bundle and is called VCS Application Package. VCS Application Package is not listed in IMT because this is a solution rather than a product.
3. There is a strict requirement that the specific product version listed in "Software Requirements" be met. Any deviation from this will void support.

3 INTENDED AUDIENCE

This technical report is intended for information technology professionals and storage professionals responsible for corporate messaging infrastructure management. For methods and procedures discussed in this technical report, NetApp assumes that the reader has working knowledge of the following:

- Exchange 2007 architecture
- Exchange Server storage architecture and administration
- Service-level expertise of Microsoft Exchange recovery operations
- Data ONTAP
- NetApp SnapDrive for Windows
- NetApp SnapManager for Exchange backup and restore procedures
- NetApp SnapMirror
- Veritas Cluster Server
- Fibre Channel or iSCSI

4 BUSINESS CONTINUITY AND HIGH AVAILABILITY

Business continuity and high availability are not a specific technology and should integrate a variety of strategies and technologies to address all potential causes of outage, balancing cost versus acceptable risk, resulting in a resilient infrastructure. As a first step in business continuity, high-availability planning is deciding which of the organization's functions must be available and operational during a crisis. Once you identify the crucial/mission-critical components, it is essential that you identify your RPOs and RTOs for the identified crucial/mission-critical apportioning in terms of cost and acceptable risk. To appropriately architect a disaster recovery solution, one must be familiar with the following terms:

- **Availability**: Generally, this is a degree to which a system, subsystem, service, or equipment is in an operable state for a proportion of time in a functional condition. It refers to the ability of the user community to access the system.
- **Disaster recovery (DR)**: This is the process of regaining access to the data, hardware, and software necessary to resume critical business operations after a disaster. A disaster recovery plan should also include methods or plans for copying necessary mission-critical data to a recovery site to regain access to such mission-critical data after a disaster.
- **High availability (HA)**: This is a system design protocol and associated implementation that provide a certain absolute degree of operational continuity of a system, service, or equipment during a given measurement period. High-availability planning should include strategies to prevent single points of failure that could potentially disrupt the availability of mission-critical business operations.
- **Recovery point objective (RPO)**: The RPO describes a point in time to which data must be restored/recovered in order to be acceptable to the organization's process supported by the data.
- **Recovery time objective (RTO)**: The RTO is the frontier of time and service level within which service availability must be accomplished to avoid undesirable consequences associated with a break in continuity of a service/process.
- **Service-level agreement (SLA)**: This is a formal negotiated agreement between a service provider and a user (typically customers) specifying the levels of availability, serviceability, performance, and operation of a system, service, or application.

5 HIGH AVAILABILITY AND DISASTER RECOVERY MODEL

When architecting a disaster recovery/high-availability solution for Microsoft Exchange Server 2007, it is important to review your current SLA to derive RTO/RPO objectives. Below we discuss multiple components that were used in this solution to achieve a highly available Exchange environment.

5.1 TECHNOLOGY COMPONENTS

5.1.1 NetApp SnapMirror

NetApp SnapMirror delivers the disaster recovery and data replication solution that today's global enterprises need. By replicating data at high speeds over LAN and WAN, SnapMirror provides extremely high data availability and the fastest recovery for mission-critical applications.

5.1.2 NetApp SnapDrive for Windows

NetApp SnapDrive for Windows is an enterprise-class storage and data management solution for Microsoft Windows Server environments. SnapDrive enables storage and system administrators to quickly and easily manage, map, and migrate data.

5.1.3 NetApp SnapManager for Exchange

NetApp SnapManager for Exchange has achieved the certified Windows logo for Windows Server 2003. SnapManager for Exchange is a simple SAN-designated Windows Server 2003 certified for backup and recovery solutions for Microsoft Exchange Server. SnapManager for Exchange tightly integrates with Microsoft Exchange, which allows consistent online backup for Microsoft Exchange environments while leveraging NetApp Snapshot™ copy and SnapMirror technologies. These technologies are critical in protecting Microsoft Exchange Server data, allowing Exchange Server administrators to quickly back up and mirror Exchange data faster and efficiently.

5.1.4 Veritas Cluster Server for NetApp SnapMirror

Veritas Cluster Server is the industry's leading cross-platform clustering solution for minimizing application downtime. Through central management tools, automated failover, features to test disaster recovery plans without disruption, and advanced failover management based on server capacity, Cluster Server allows IT managers to maximize resources by moving beyond reactive recovery to proactive management of application availability.

6 ARCHITECTURE

The architecture used in this model to provide high availability and disaster recovery for Microsoft Exchange Server 2007 contains a primary site for production and a secondary DR site for recovery of Microsoft Exchange Server 2007 in the event of a disaster. The Veritas Cluster Server application agent for Microsoft Exchange Server is used to provide high availability for the Exchange Servers, and the Veritas Cluster Server application agent for NetApp enables configuring NetApp storage via iSCSI or FC in a Veritas Cluster Server clustered environment. Both the agents work together to provide a highly available environment for Microsoft Exchange Server and provide disaster recovery configurations when set up using the Veritas Cluster Server global cluster option and NetApp SnapMirror for data replication. The following agents are used to make sure this solution works well.

6.1 VCS HARDWARE REPLICATION AGENT FOR NETAPP

The VCS hardware replication agent for NetApp provides failover support and recovery in environments employing NetApp appliances for storage and NetApp SnapMirror for replication. The agent monitors and manages the state of replicated storage devices and enables only one system to have safe and exclusive access to the configured devices. The agent can be used in local clusters, single VCS replicated data clusters, and multicluster environments set up using the VCS Global Cluster Option (GCO). The VCS agents for NetApp include the NetApp storage agent, the NetApp SnapDrive agent, and the NetApp SnapMirror agent.

6.1.1 NetApp Storage Agent

The NetApp storage agent monitors the state of the storage device. The agent is represented by the NetApp storage resource type in VCS. NetApp storage resources are persistent, meaning that they are not brought online or taken offline. The agent function includes the following:

Monitor: Verifies the state of the appliance attached to the host by sending an `ICMP ping` command to the appliance. If the appliance does not respond, the agent reports the state of the storage as faulted.

6.1.2 NetApp SnapDrive Agent

The NetApp SnapDrive agent monitors, connects, and disconnects storage volumes. You can configure the agent to use the iSCSI or the FC protocol. Specific agent functions include the following:

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

6.2 VCS APPLICATION AGENT FOR MICROSOFT EXCHANGE SERVER

The Veritas Cluster Server application agent for Microsoft Exchange monitors Exchange services in a Veritas Cluster Server cluster, brings them online, and takes them offline.

6.3 HOW THE AGENTS MAKE MICROSOFT EXCHANGE SERVER HIGHLY AVAILABLE

The Veritas Cluster Server application agent for Microsoft Exchange detects an application failure if a configured Exchange service is not running or if a configured virtual server is not available. The NetApp agents enable 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.

6.3.1 Local Cluster Configuration

When the Exchange agent detects an application or a host failure, Veritas Cluster Server attempts to fail over the Exchange service group to the next available system in the service group's system list.

The NetApp SnapDrive agent disconnects the virtual disks (LUNs) containing Exchange data from the current node and connects them to the new node. The configured Exchange services and virtual servers are started on the new node, thus providing continuous availability for Exchange data, including configured mailboxes.

6.3.2 Disaster Recovery Configuration

In a disaster recovery configuration, Veritas Cluster Server 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, Veritas Cluster Server attempts to fail over the application to the remote site. This involves the following steps:

1. Disconnecting the virtual disks (LUNs) from the current host (using the NetApp SnapDrive agent)
2. Updating SnapMirror volumes (only if both source and destination storages are available with connectivity between them)
3. Performing a mirror break, which enables write access to the target (using the NetApp SnapMirror agent)
4. Reversing the direction of replication by demoting the original source to a target and beginning replicating from the new source (using the NetApp SnapMirror agent)
5. Connecting the virtual disks (LUNs) to the target hosts (using the NetApp SnapDrive agent)
6. Starting the Exchange services on the remote node (using the Veritas Cluster Server agents for Exchange Server)

6.4 TOPOLOGY DIAGRAM

Figure 1 shows the basic architecture used in both iSCSI and FCP scenarios.

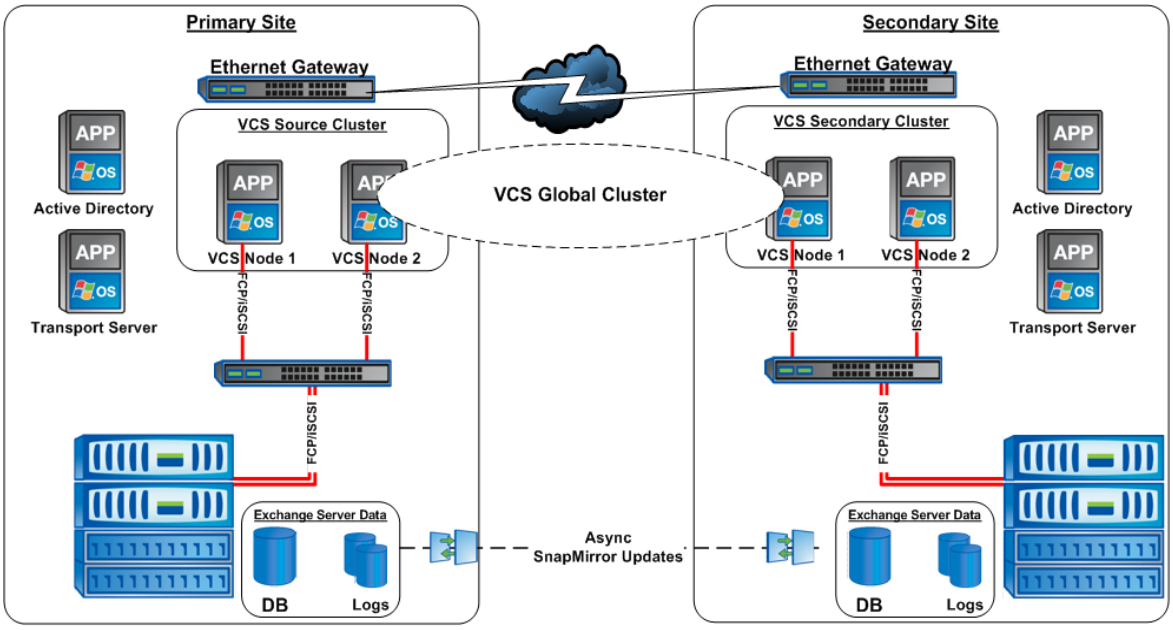

Figure 1) Veritas Cluster Server and SnapMirror for Exchange setup using FCP/iSCSI.

7 HARDWARE AND SOFTWARE REQUIREMENTS

7.1 HARDWARE REQUIREMENTS

- Server platform: x86_64
- HBA: Emulex 2Gb, 4Gb, 8Gb and QLogic 2Gb, 4Gb, 8Gb HBAs from support matrix
- Storage: NetApp FAS900, FAS3000, and FAS6000 series storage systems
- FC switch as supported in IMT

7.2 SOFTWARE REQUIREMENTS

- Data ONTAP
- Microsoft software iSCSI initiator
- NetApp SnapManager for Exchange
- NetApp SnapDrive for Windows
- Windows Server 2003
- Microsoft Exchange
- NetApp Host Utilities for Windows version for iSCSI or FC
- NetApp Data ONTAP DSM (in case of multipath)
- FC HBA driver as supported in IMT
- FC switch OS as supported in IMT

8 IMPLEMENTATION

This section provides a list of prerequisites and implementation details for implementing Exchange Server 2007 on NetApp storage systems. It also presents best practices to make the Exchange Server 2007 environment highly available and disaster recovery capable with the help of Symantec™ Veritas Cluster Server agent for NetApp SnapMirror along with NetApp SnapMirror, SnapDrive, and SnapManager for Exchange.

8.1 IMPLEMENTATION TASKS

This section outlines the tasks to successfully implement Exchange Server with Symantec Veritas Cluster Server and NetApp solutions. Supported versions of all software are listed in Appendix B. These tasks must be performed in the order in which they are listed.

8.1.1 Primary Site

1. Install software iSCSI initiator package on all hosts (or configurable Fibre Channel HBA if using FC SAN).
2. Install Windows Host Utilities for iSCSI or FC on all hosts.
3. Install NetApp Data ONTAP DSM (in case of multipath).
4. Install NetApp SnapDrive for Windows on all hosts.
5. Install Veritas Cluster Server for NetApp SnapMirror on all hosts.
6. Complete installation and create a cluster.
7. Install Microsoft Exchange Server on first node and then additional nodes.
8. Create Exchange service group in Veritas Cluster Server.
9. Install SnapManager for Exchange on all nodes.
10. Complete SnapManager for Exchange configuration on all hosts.

8.1.2 Secondary DR Site

1. Install software iSCSI initiator package on the hosts (or configurable Fibre Channel HBA if using FC SAN).
2. Install Windows Host Utilities for iSCSI or FC on all hosts.
3. Install NetApp Data ONTAP DSM (in case of multipath).
4. Install NetApp SnapDrive for Windows on all hosts.
5. Install Veritas Cluster Server for NetApp SnapMirror on all hosts.
6. Complete installation and create a cluster.
7. Install Microsoft Exchange Server on first node and then additional nodes.
8. Create Exchange service group in VCS with the **same name** as in the source cluster.
9. Install SnapManager for Exchange on all hosts.
10. Complete SnapManager for Exchange configuration on all hosts.

8.1.3 Primary Sites

1. Establish an asynchronous SnapMirror relationship for database and log volumes between the primary and secondary DR site.
2. Link Veritas Cluster Server clusters at the primary and the secondary DR sites.
3. Make the Exchange service resource group global.
4. Take a backup with SnapManager for Exchange and do a SnapMirror update.
5. Optionally plan for the SME backup schedule and create it in SME.

Note:

Set VCS service timeout as described in Appendix C**.**

Refer to the FC or iSCSI Host Utilities documentation and make sure appropriate timeout settings are established for your environment.

8.2 LIMITATIONS

Veritas Cluster Server support for Exchange Server includes the following features:

- **High availability for mailbox server role only**: High-availability support for Exchange Server is available for the mailbox server role only. While installing Exchange, ensure that you do not install any other server role on the system on which you install the mailbox server role. If you have already installed the mailbox server role along with the other server roles on the same server, you will have to remove the other server roles before configuring Exchange in a Veritas Cluster Server environment.
- **Exchange management shell in the virtual server context**: The Exchange management shell provides a command-line interface that enables automation of administrative tasks for Exchange Server. Veritas Cluster Server provides a shortcut to launch the Exchange management shell under the context of the virtual server name.

8.3 INSTALLING AND CONFIGURING VCS SOFTWARE

Make sure the following prerequisites are met before beginning software installation:

- Make sure the storage controllers are members of the same domain as the Exchange Servers.
- Make sure that the storage controllers are reachable using DNS names.
- Make sure that storage controllers can replicate bidirectionally.
- If you plan to set up disaster recovery, make sure the volumes in both the sites are of the same size.
- Set up the private network for the shared storage.
- If Fibre Channel is used for connectivity to the storage LUNs, type hba_info on the command prompt and verify that the FC initiators are displayed. If the FC initiators are not displayed, install the miniport driver provided by the vendor and then run the command again to verify that the FC initiators are displayed.
- Ensure that the LUNs are mounted. In the case of MPIO, ensure that the LUNs are mounted and using the required initiators.

USING THE PRODUCT INSTALLER

This section outlines the procedures for installing Veritas Cluster Server.

1. Run `setup.exe`, located in the root directory of Veritas Cluster Server for NetApp from the installation media.

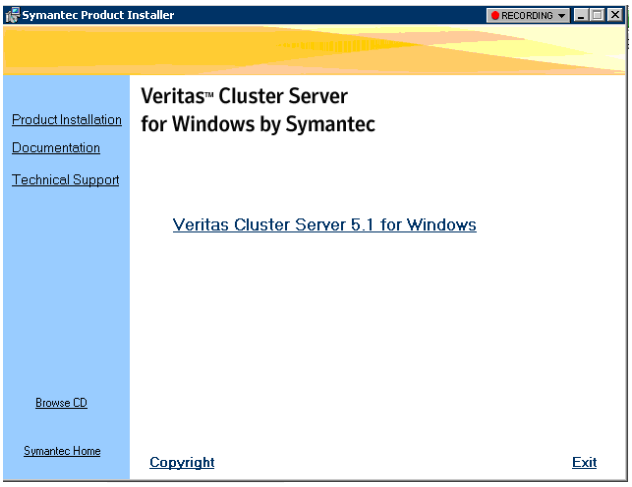

Figure 2) Veritas Cluster Server product installer (page 1).

2. On the product installation pane, click **Veritas Cluster Server 5.1 for Windows**.

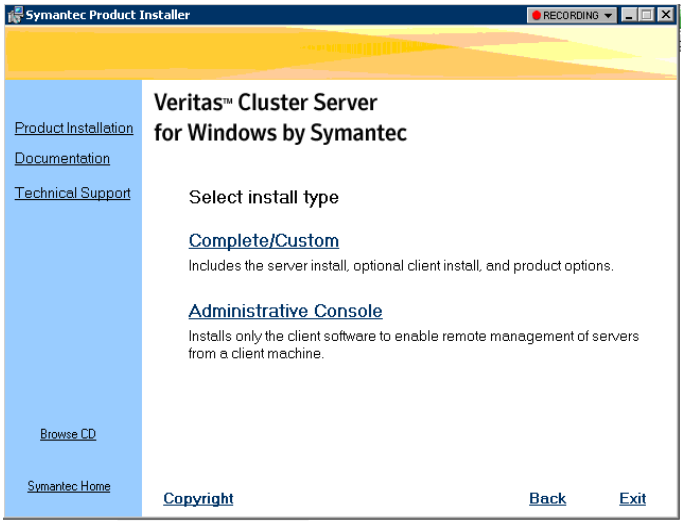

Figure 3) Veritas Cluster Server product installer (page 2).

3. Click the **Complete/Custom** option to install server components and optional client components.
   Note: Click **Administrative Console** if you wish to install only the client components.

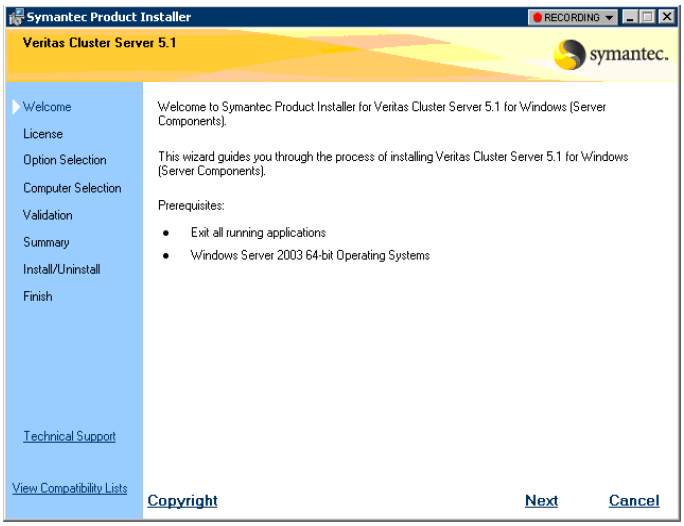

Figure 4) Veritas Cluster Server product installer (page 3).

4. Review information on the Welcome pane and click **Next.**

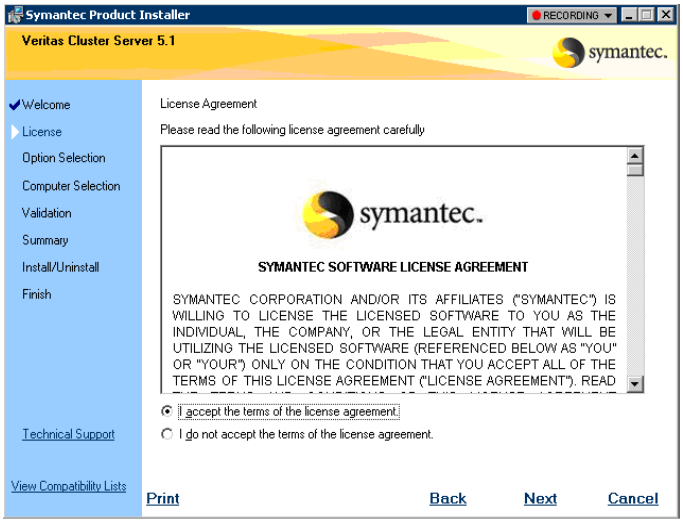

Figure 5) Veritas Cluster Server product installer (page 4).

5. Accept the license agreement.

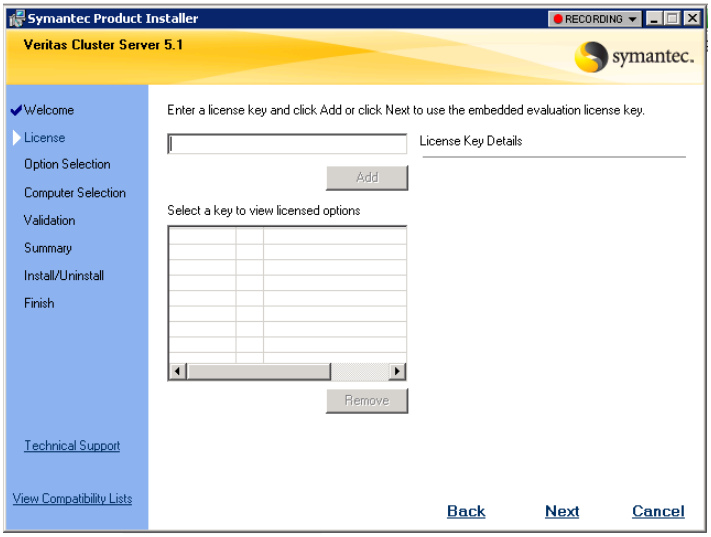

Figure 6) Veritas Cluster Server product installer (page 5).

6. Complete licensing information, and click **Next.**

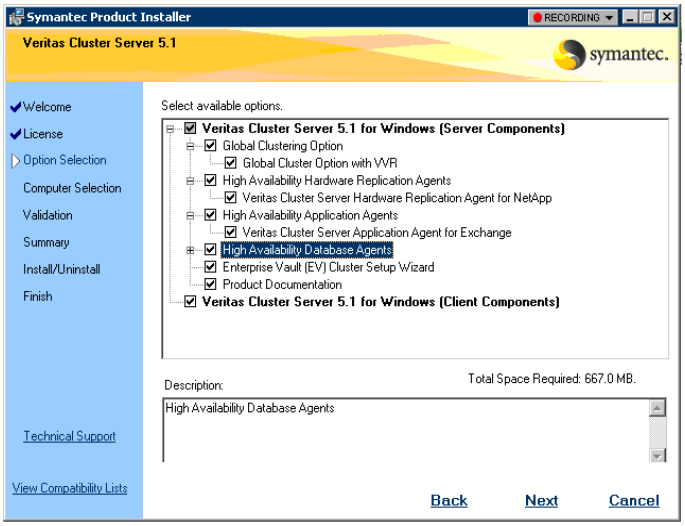

Figure 7) Veritas Cluster Server product installer (page 6).

7. On the option selection pane check the following product options and click **Next**:
   - **Veritas Cluster Server 5.1 for Windows (Server Components)**
     - **Global Clustering Option (if you plan to configure a disaster recovery environment)**
     - **High-Availability Hardware Replication Agents**
     - **Veritas Cluster Server Hardware Replication Agent for NetApp**
     - **High-Availability Application Agents**
     - **Veritas Cluster Server Application Agent for Exchange**
   - **Veritas Cluster Server 5.1 for Windows (Client Components)**

     Note: This will install the Veritas Cluster Server Java™ console on the same nodes on which the server components are installed.

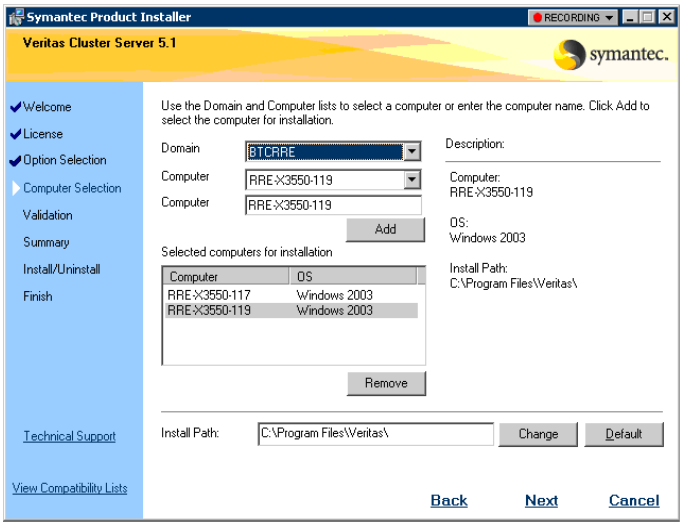

Figure 8) Veritas Cluster Server product installer (page 7).

8. On the Computer Selection pane, specify the domain and the nodes for the installation and click **Next.**

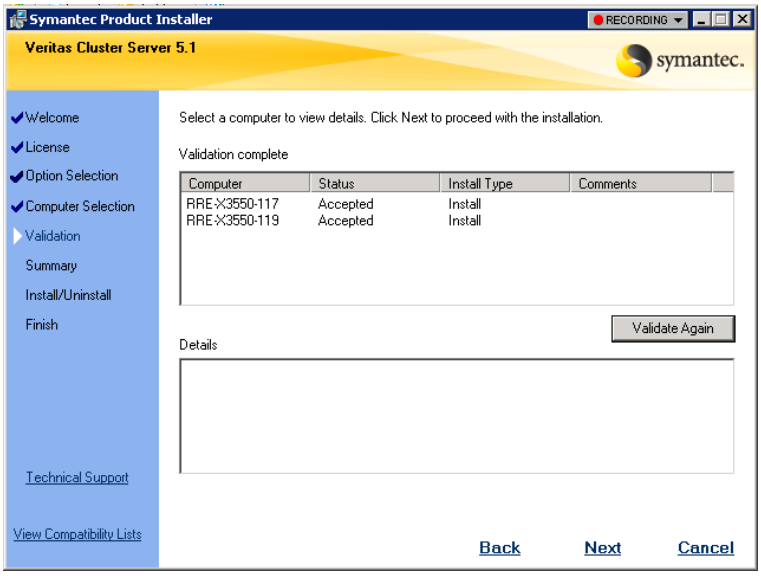

Figure 9) Veritas Cluster Server product installer (page 8).

9. After the installer validates the system for installation, click **Next**.

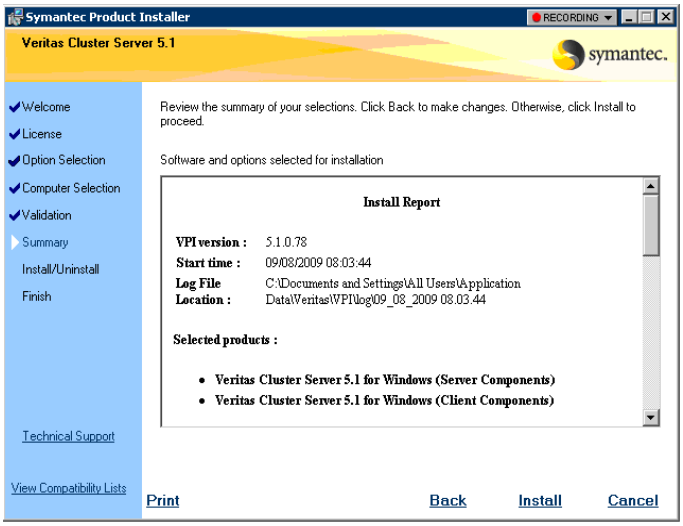

Figure 10) Veritas Cluster Server product installer (page 9).

10. Review the summary, and click **Install**.

    NOTE: During the installation on the specified systems, click **Yes** if prompted to accept the Veritas driver software.

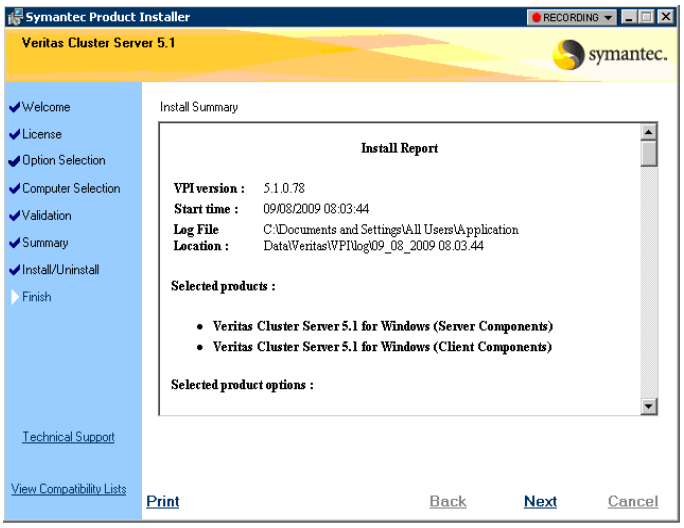

Figure 11) Veritas Cluster Server product installer (page 10).

11. Review the installation report and click **Next**.

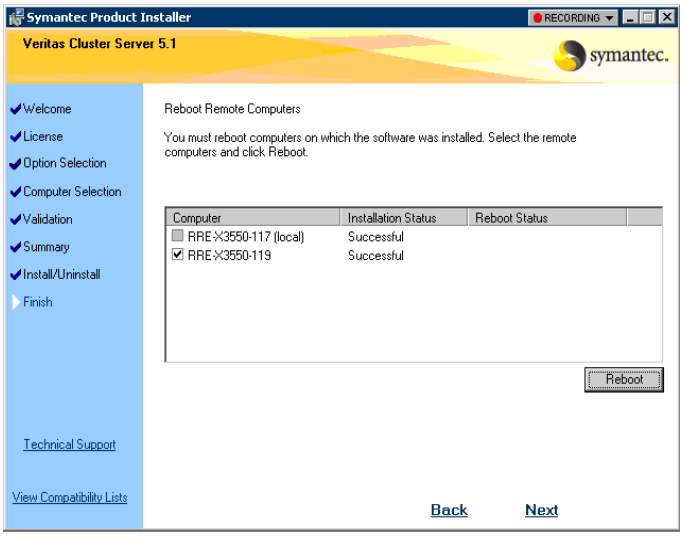

Figure 12) Veritas Cluster Server product installer (page 11).

12. **Reboot** the remote nodes.

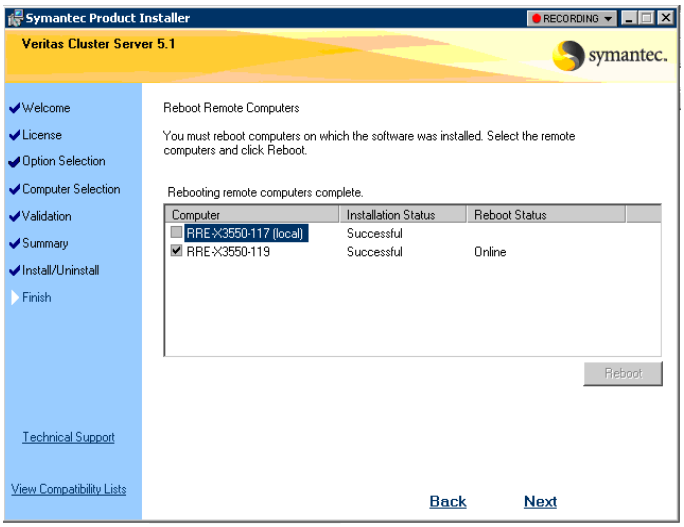

Figure 13) Veritas Cluster Server product installer (page 12).

13. Click **Next**.

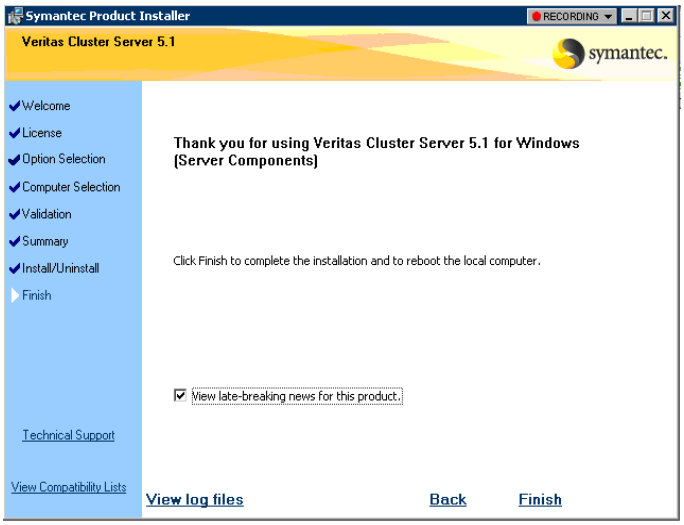

Figure 14) Veritas Cluster Server product installer (page 13).

14. Click **Finish**.

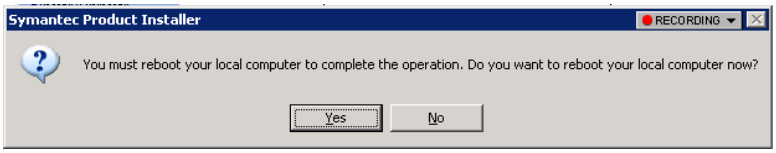

Figure 15) Veritas Cluster Server product installer completion.

15. Click **Yes** to reboot the local node.

CONFIGURING THE VERITAS CLUSTER SERVER CLUSTER

This section outlines the procedures to set up the components required to run Veritas Cluster Server. The "Veritas Cluster Server Configuration Guide" sets up the cluster infrastructure, including LLT and GAB; and the cluster service group, which contains the resources for the cluster management console (single cluster mode), also referred to as Web console, notification, and global clusters.

1. Start the Cluster Configuration Wizard by clicking **Start > All programs> Symantec > Veritas Cluster Server>Configuration Tools> Cluster configuration wizard**.
2. Click **Next** on the Welcome screen.

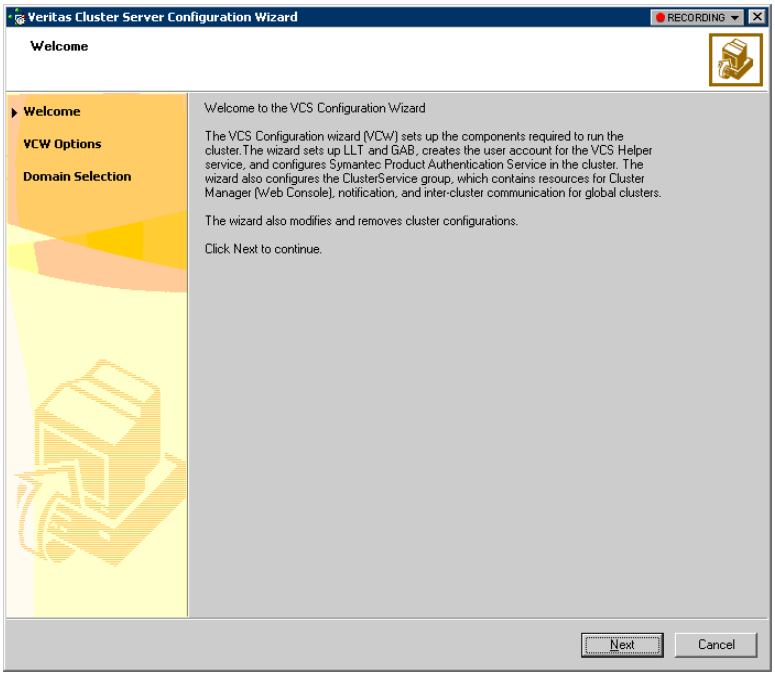

Figure 16) Veritas Cluster Server configuration wizard (page 1).

3. Select **Cluster Operations** and click **Next**.

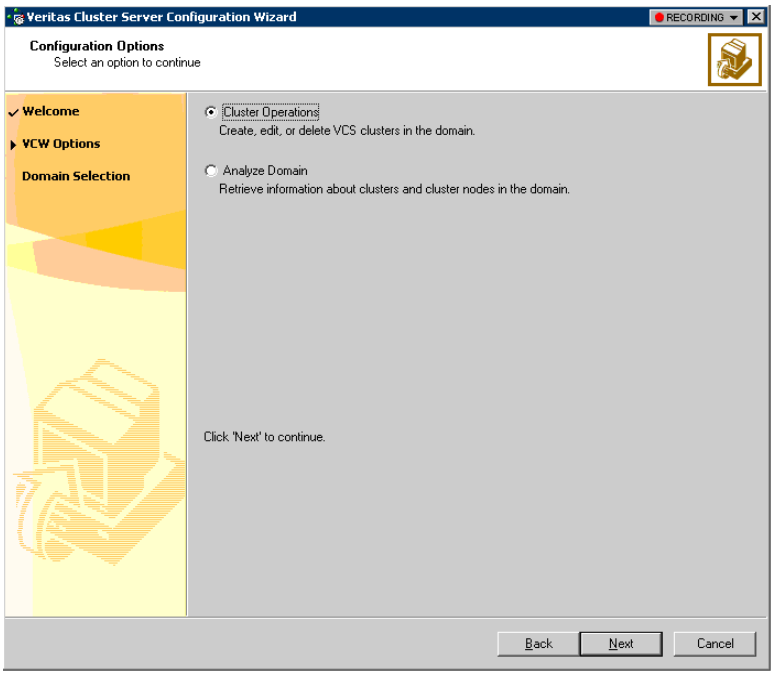

Figure 17) Veritas Cluster Server configuration wizard (page 2).

4. Select or type the domain name in which the cluster resides and select the discovery options, then click **Next**.

   Note: Selecting **Specify Systems and Users Manually** disables the domain discovery.

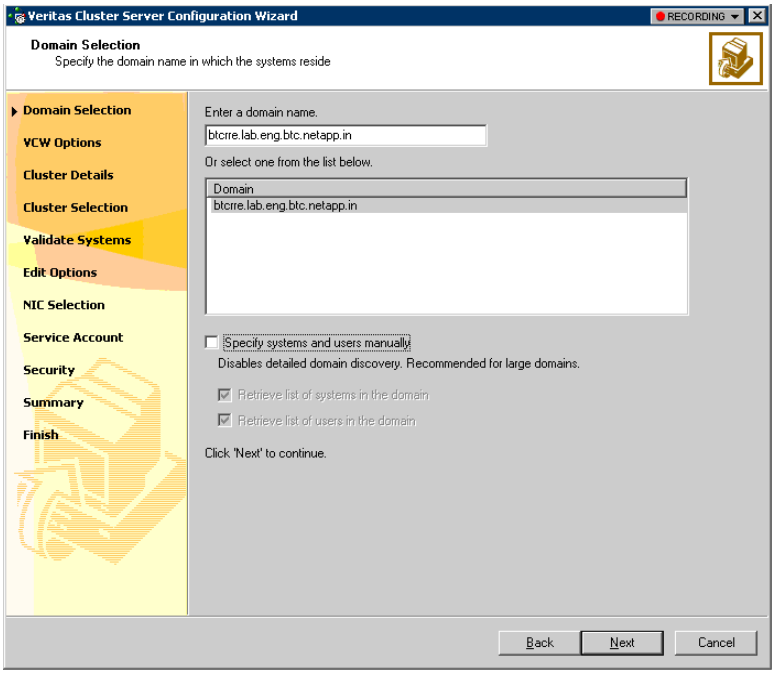

Figure 18) Veritas Cluster Server configuration wizard (page 3).

5. Make sure systems are in Accepted status and click **Next**.

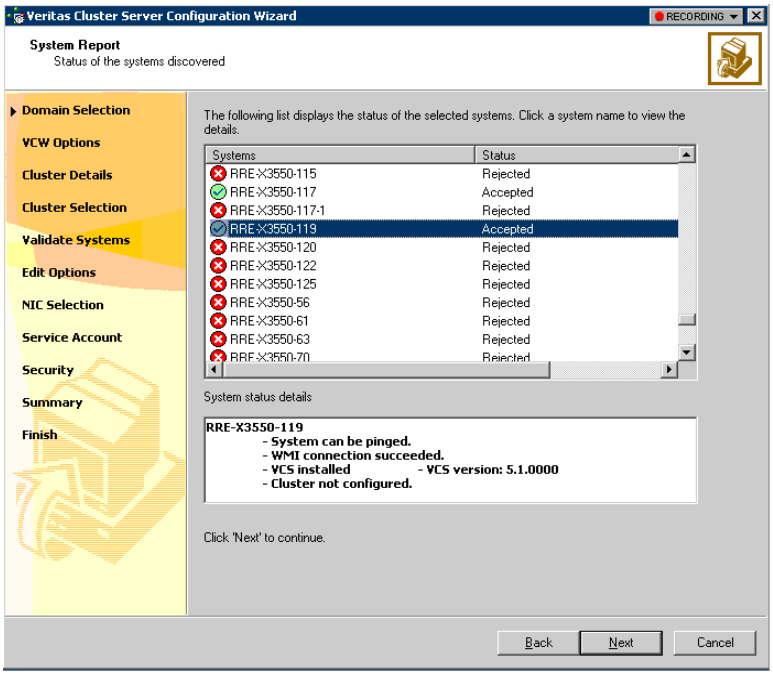

Figure 19) Veritas Cluster Server configuration wizard (page 4).

6. On the Cluster Configuration Options pane, select **Create New Cluster** and click **Next**.

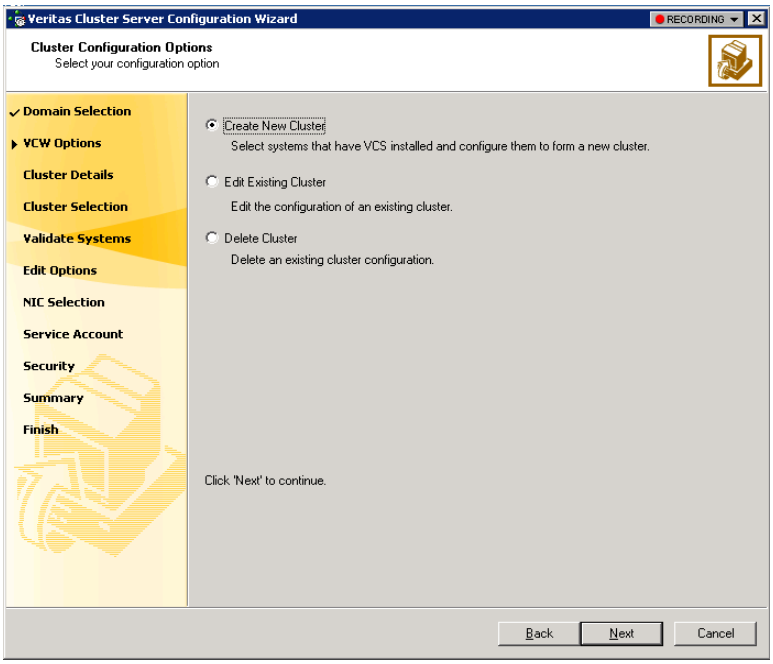

Figure 20) Veritas Cluster Server configuration wizard (page 5).

7. On the Cluster Details pane, specify the details for the cluster (cluster came, cluster ID, and cluster members) and click **Next**.

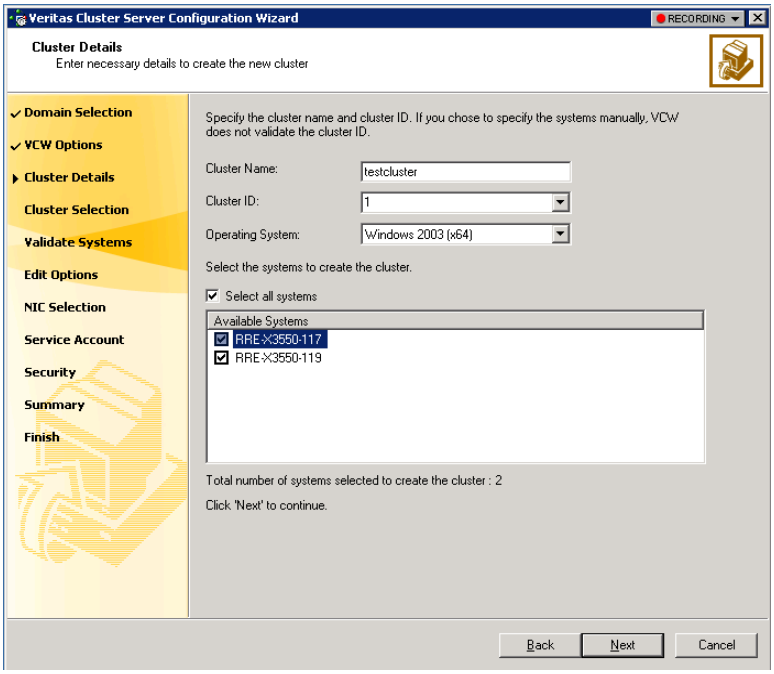

Figure 21) Veritas Cluster Server configuration wizard (page 6).

8. After the wizard completes validation on the systems for cluster membership, click **Next**.

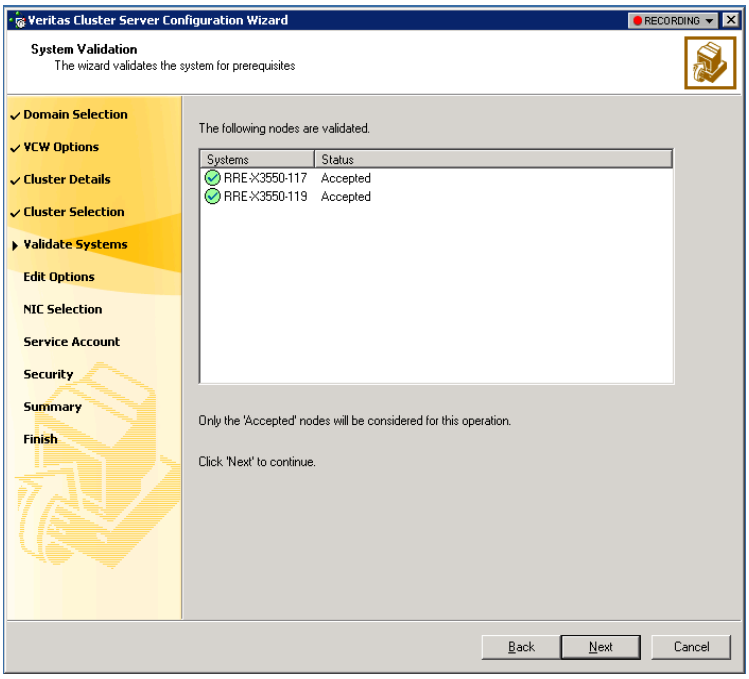

Figure 22) Veritas Cluster Server configuration wizard (page 7).

9. On the Private Network Configuration pane, configure the Veritas Cluster Server private network and click **Next**.

   NOTE: Symantec recommends reserving two NICs exclusively for the private network. However, you could lower the priority of one of the NICs by right-clicking it and selecting low priority and using the low-priority network for public and private communication. If you have only two NICs on the hosts, please lower the priority of at least one NIC of that system.

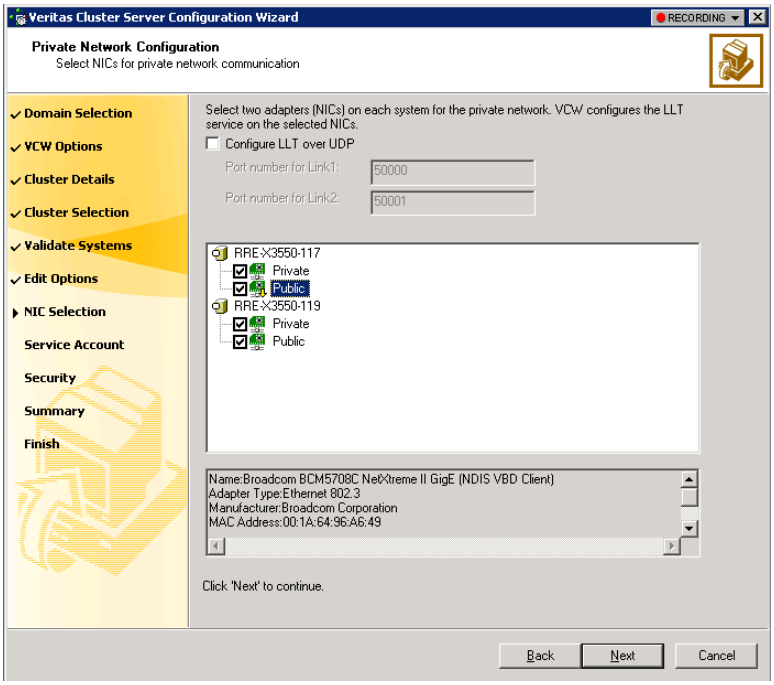

Figure 23) Veritas Cluster Server configuration wizard (page 8).

10. Enter the VCS Helper service user account and click **Next**.

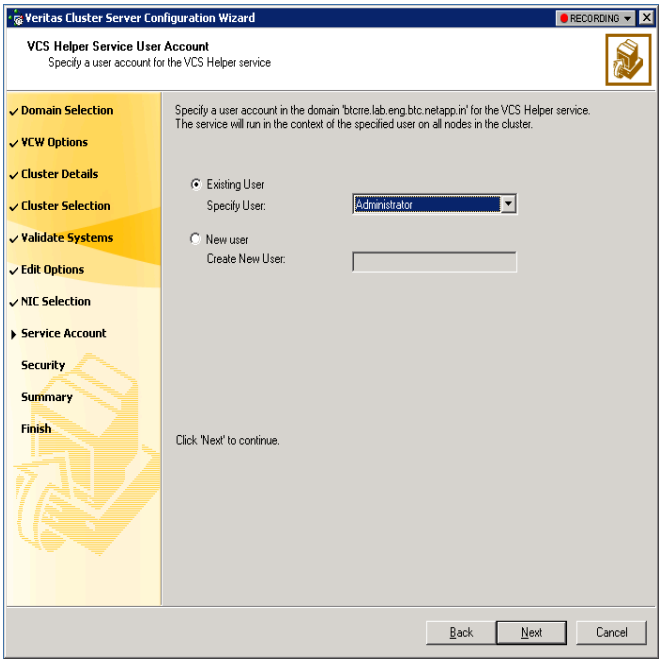

Figure 24) Veritas Cluster Server configuration wizard (page 9).

11. Enter the password and click **OK**.

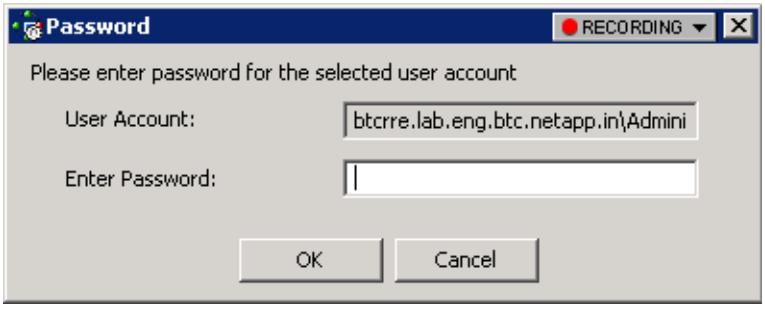

Figure 25) Veritas Cluster Server configuration wizard (page 10).

12. On the Configure Security Service option pane, specify security options for the cluster and then click **Next**.

    Note: The default user name for the Veritas Cluster Server administrator is “admin,” and the default password is “password.” Use this account to log on to Veritas Cluster Server using the cluster management console (single cluster mode) or Web console when Veritas Cluster Server is not running in secure mode.

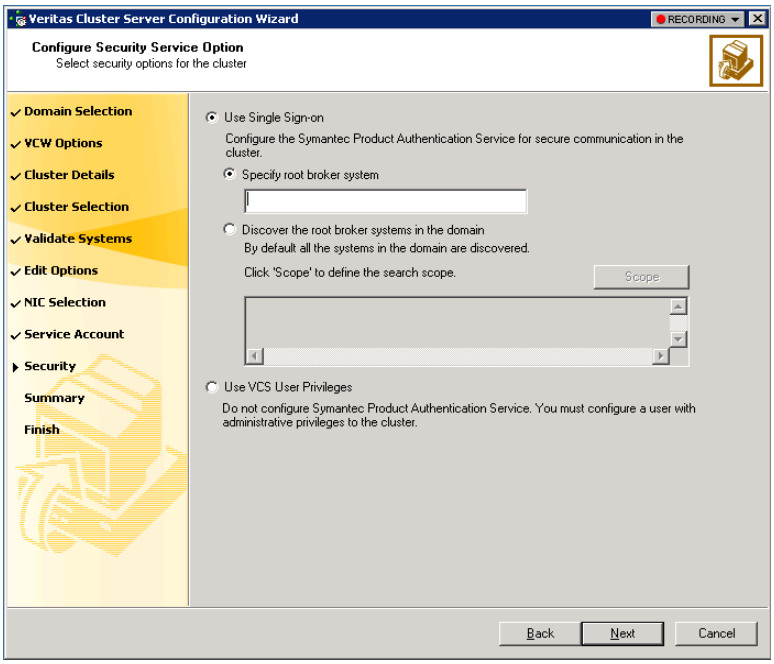

Figure 26) Veritas Cluster Server configuration wizard (page 11).

13. Review the summary and click **Configure**.

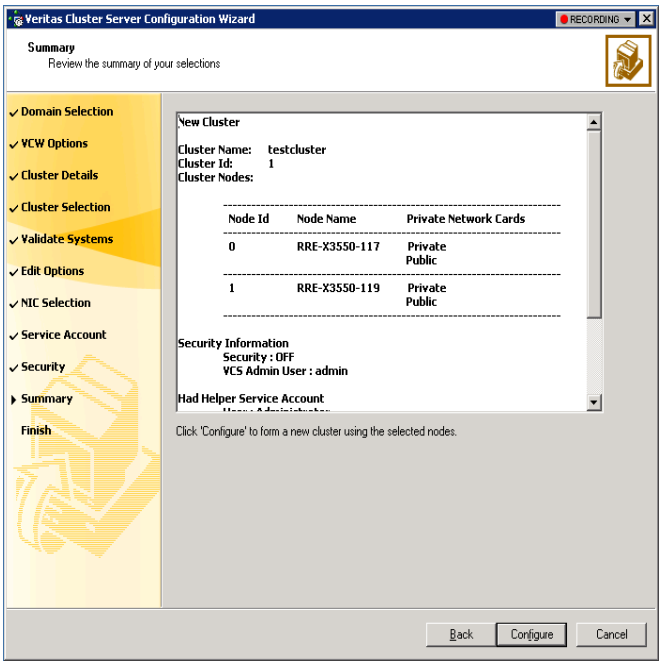

Figure 27) Veritas Cluster Server configuration wizard (page 12).

14. Click **Next** to configure the cluster services group. This group is required to set up the components for the cluster management console (single cluster mode) or Web console, notification, and for global clusters.

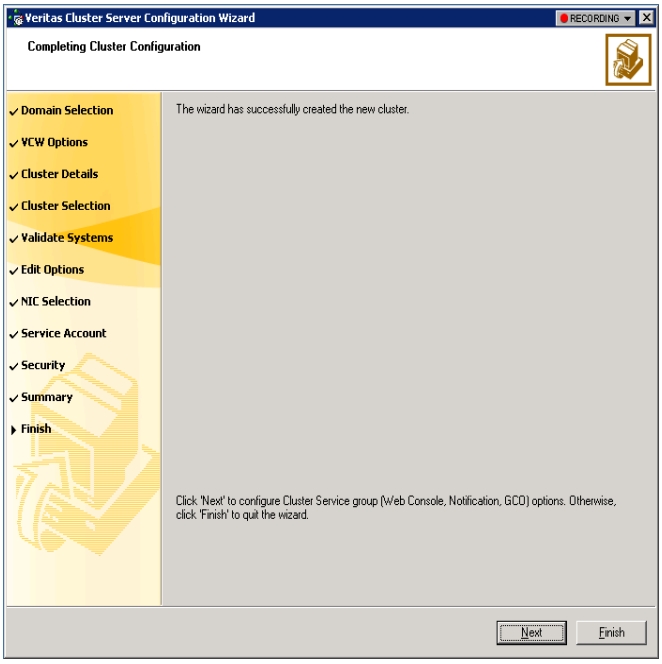

Figure 28) Veritas Cluster Server configuration wizard (page 13).

15. Select the **Web Console** checkbox to configure the cluster management console (single cluster mode), also referred to as the Web console.

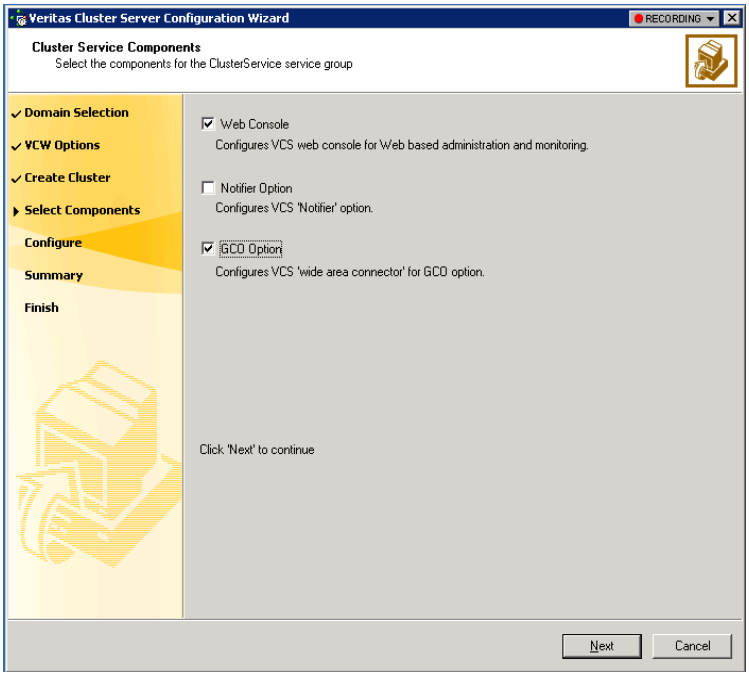

Figure 29) Veritas Cluster Server configuration wizard (page 14).

16. Enter the IP address for GCO and click **Next**.

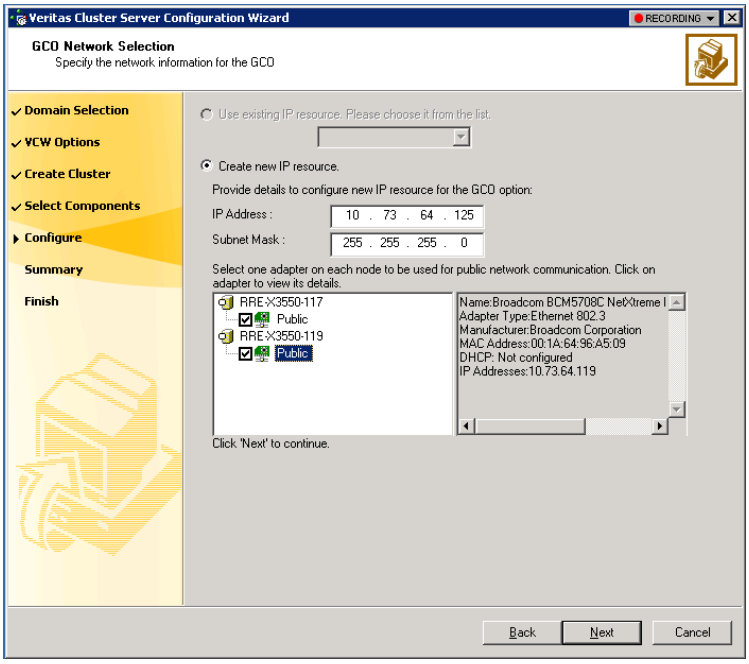

Figure 30) Veritas Cluster Server configuration wizard (page 15).

17. Review the summary and click **Configure**.

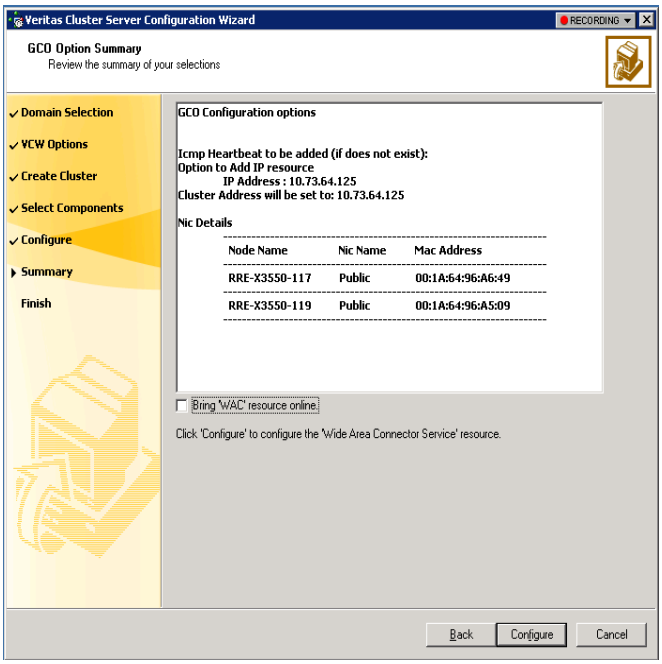

Figure 31) Veritas Cluster Server configuration wizard (page 16).

18. Click **Finish** to complete the cluster configuration.

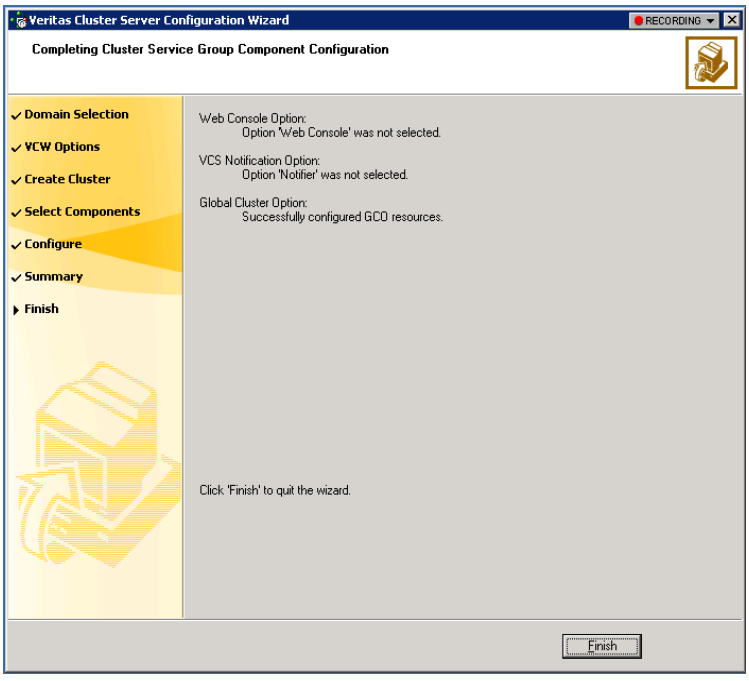

Figure 32) Veritas Cluster Server configuration wizard (page 17).

CONFIGURING WEB CONSOLE (OPTIONAL)

This section describes the steps to configure the Veritas Cluster Server cluster management console (single cluster mode).

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

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

2. Review the summary information and choose whether or not you want to bring the Web console resources online when Veritas Cluster Server is started. Then click **Configure**.

3. If you choose to configure the notifier resource, click **Next** to proceed with the configuration. Otherwise, click **Finish** to exit the wizard.

UPGRADE VERITAS TO 5.1AP1

1. Stop the cluster using the command **`hastop -all`**

2. In the Symantec Product Installer, select **Application Pack 1 for SFW 5.1, SFWHA 5.1, and VCS 5.1 for Windows.**

Figure 33) Configuration checker (page 1).

3. Click **Next**.

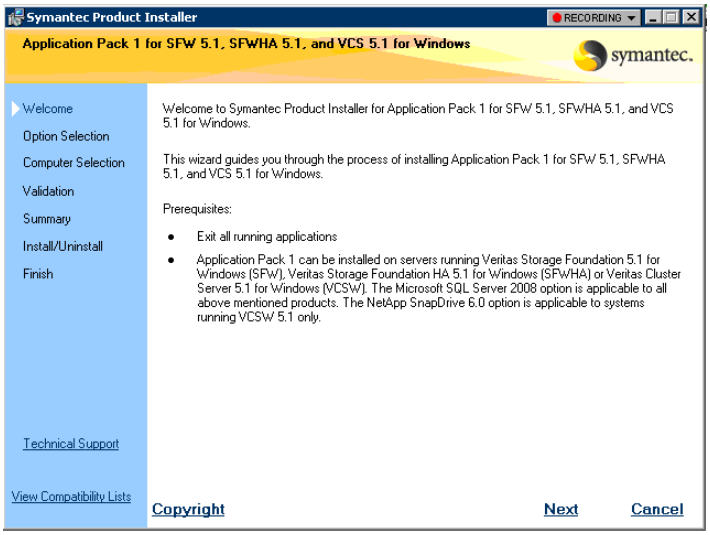

Figure 34) Configuration checker (page 2).

4. Select **SnapDrive 6.0**. Click **Next.**

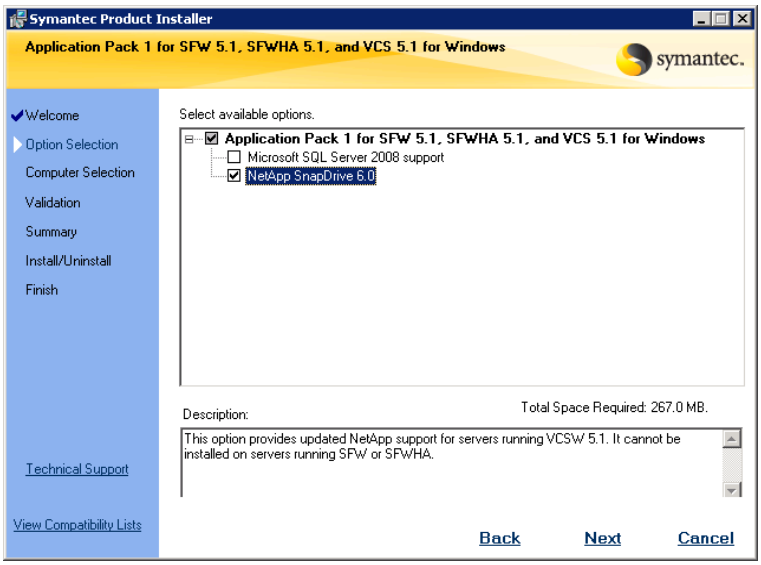

Figure 35) Configuration checker (page 3).

5. Add servers to be upgraded and click **Next**.

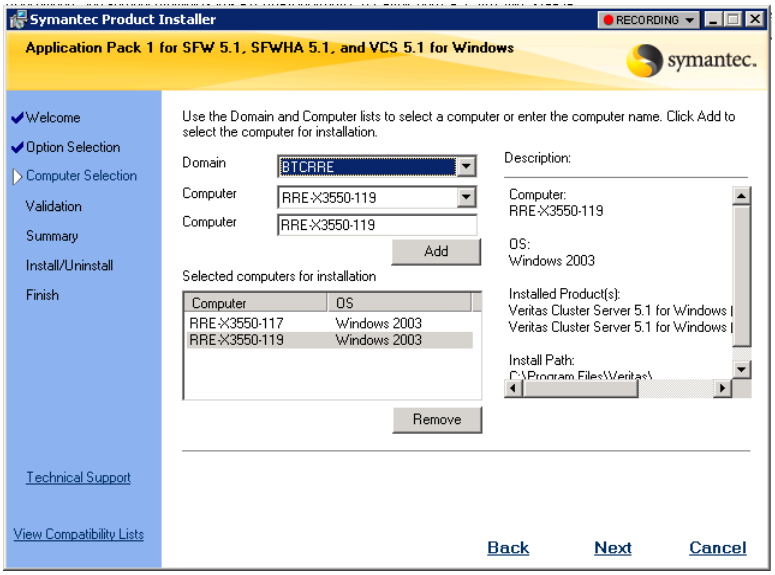

Figure 36) Configuration checker (page 4).

6. Select **Next** after validation completes.

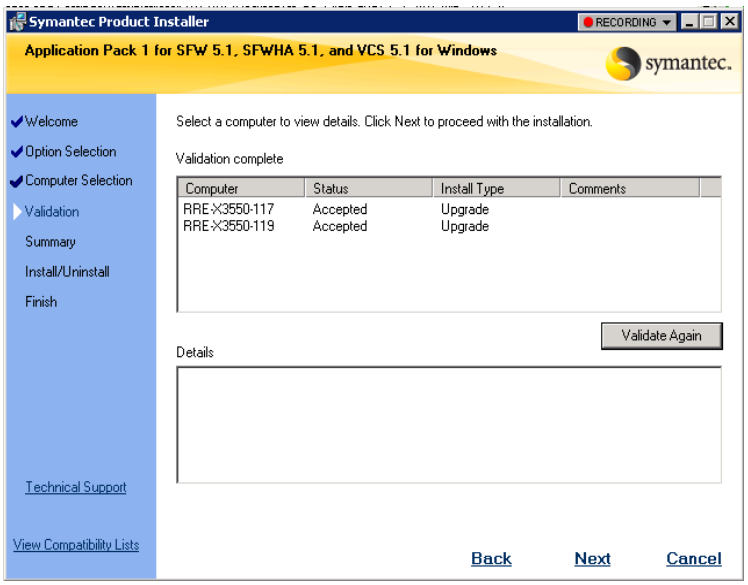

Figure 37) Configuration checker (page 5).

7. Review summary and click **Install**.

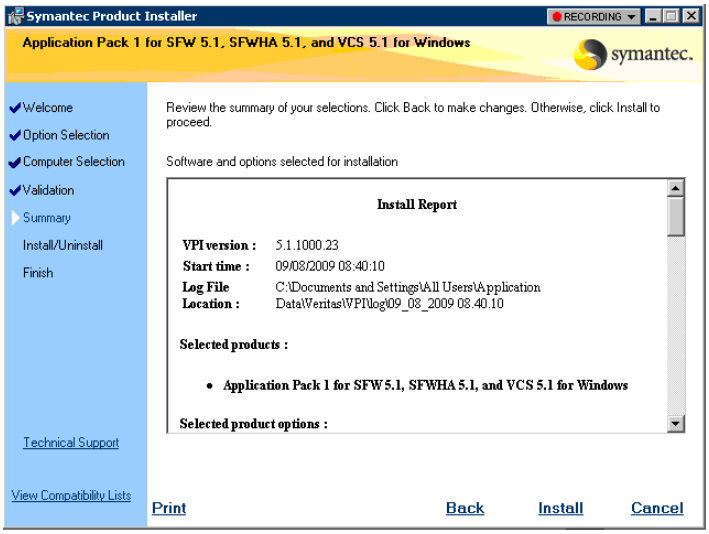

Figure 38) Configuration checker (page 6).

8. Click **Next**.

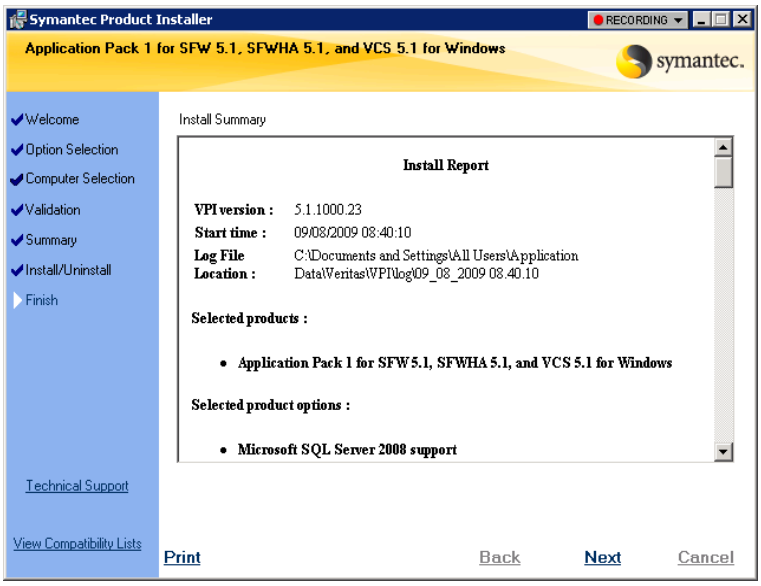

Figure 39) Configuration checker (page 7).

9. Select **Finish** to complete installation.

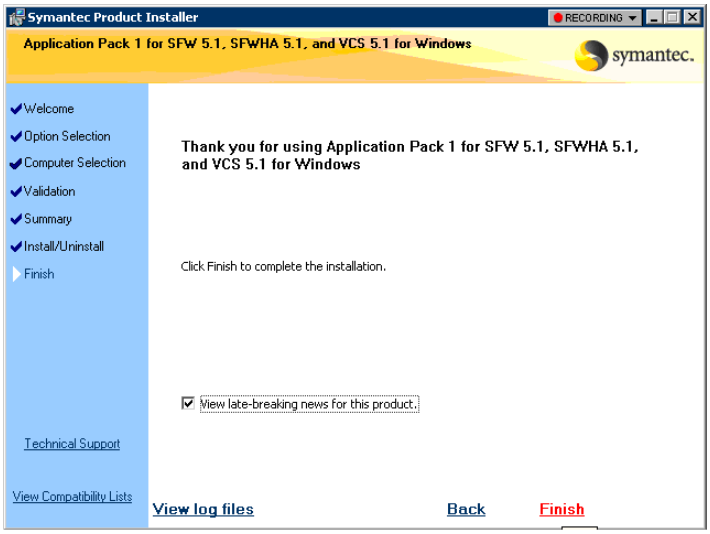

Figure 40) Configuration checker (page 9).

10. To start the cluster, run the command `hastart` on all the nodes.

8.4 INSTALLING MICROSOFT EXCHANGE SERVER

This section describes how to install and configure Microsoft Exchange Server and its components in a Veritas Cluster Server cluster environment.

8.4.1 Overview

Installing Microsoft Exchange in a Veritas Cluster Server cluster environment involves three major tasks:

1. Preinstallation
2. Microsoft Exchange installation
3. Postinstallation

The Exchange Setup Wizard for the Veritas Cluster Server performs the preinstallation and postinstallation tasks. Refer to Appendix A for prerequisites for installing Microsoft Exchange Server on a Veritas Cluster Server cluster.

SHARED LUN REQUIREMENT FOR MICROSOFT EXCHANGE INSTALLATION

Typical configurations will have two LUNs: one for database and one for log.

- The Database LUN and log LUN should be placed on different NetApp volumes.
- Qtree is not supported.
- The transaction log and registry replication can be on the same drive.

Perform the following steps on the first node in the primary site. To create two LUNs with drive letters `E` and `F`:

1. Open Computer Management.(click **Start > Run.** Type `compmgmt.msc` and then click **OK**.)
2. Select SnapDrive in the left pane and expand it. For more information, see SnapDrive Installation and Administration Guide.
3. Right-click **Disks** and select **Create Disk**, then click **Next** on the Welcome screen.
4. Provide the path for the volume designated for this LUN, provide a name for the new LUN, and click **Next**.
5. Select the virtual disk type as **Dedicated** and click **Next**. Provide an appropriate size for the new LUN, assign a drive letter of your choice, and click **Next** .
6. Select an initiator for this virtual disk and click **Next**. Choose SnapDrive to manage the igroup automatically, and click **Next.** Then click **Finish** to begin to create the LUN.
7. Perform the same steps again to create another LUN.

8.4.2 Preinstallation: Exchange Setup Wizard

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

Note: After the wizard completes, you must reboot the server. Make sure to close all applications and save your data before running the wizard.

1. Verify that the LUN created to store the registry replication information is connected to this node and is not connected to other nodes in the cluster.

2. Start the Exchange Server setup wizard for Veritas Cluster Server by clicking **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange Server 2007 Setup Wizard**. Review the information in the Welcome pane and click **Next**.

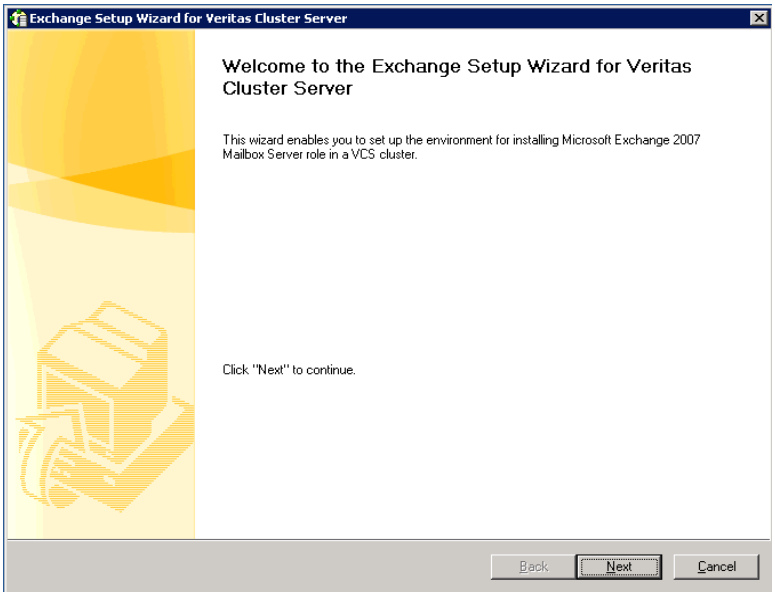

Figure 41) Exchange setup wizard (page 1).

3. On the Available Option pane, select **Install Exchange 2007 Mailbox Server role for High Availability** and click **Next**.

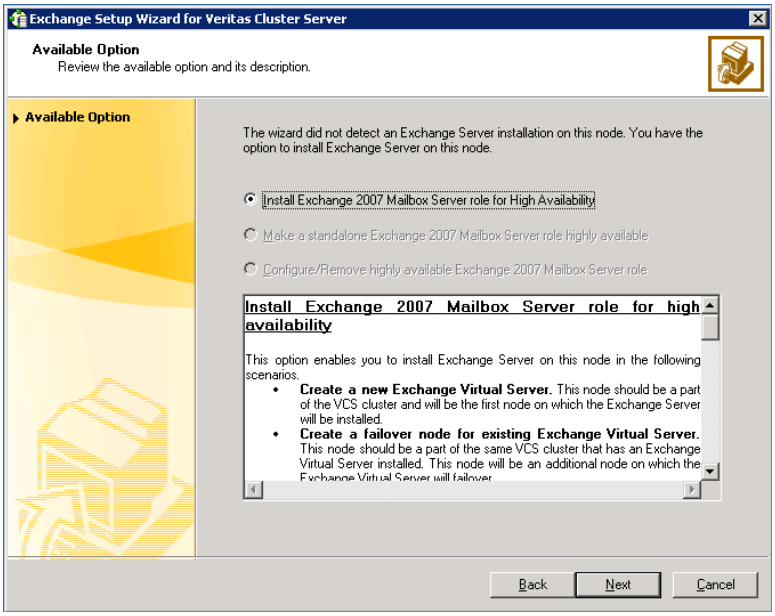

Figure 42) Exchange setup wizard (page 3).

4. On the Select Option pane, select **Create a new Exchange Virtual Server** and click **Next**.

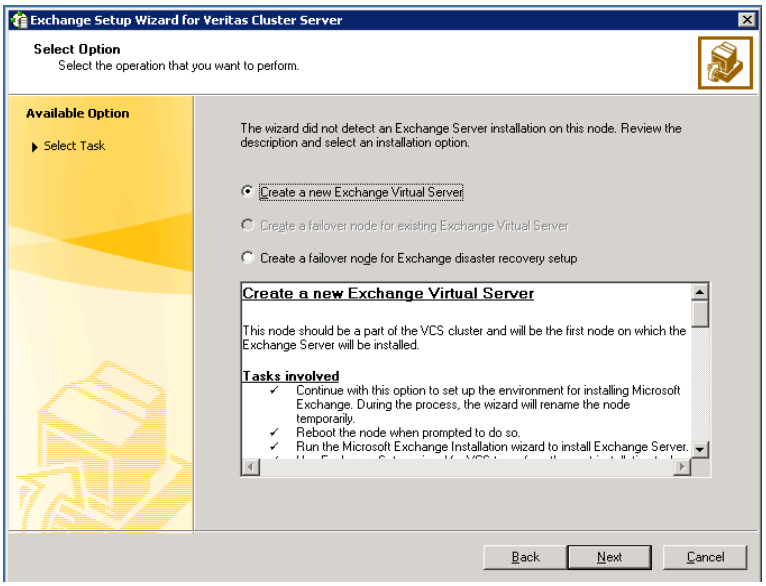

Figure 43) Exchange setup wizard (page 4).

5. Specify the following network information for the Exchange Virtual Server and click **Next.**
   a. Enter a unique virtual name for the Exchange Server.
      Note: Once you assign 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 Veritas Cluster Server environment and reinstall it using the Exchange Server Setup Wizard for Veritas Cluster Server.
   b. Enter the name of a domain suffix for the Exchange Server.
   c. 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.
   d. Enter a unique virtual IP address for the Exchange Server and enter the subnet mask for the virtual IP address.

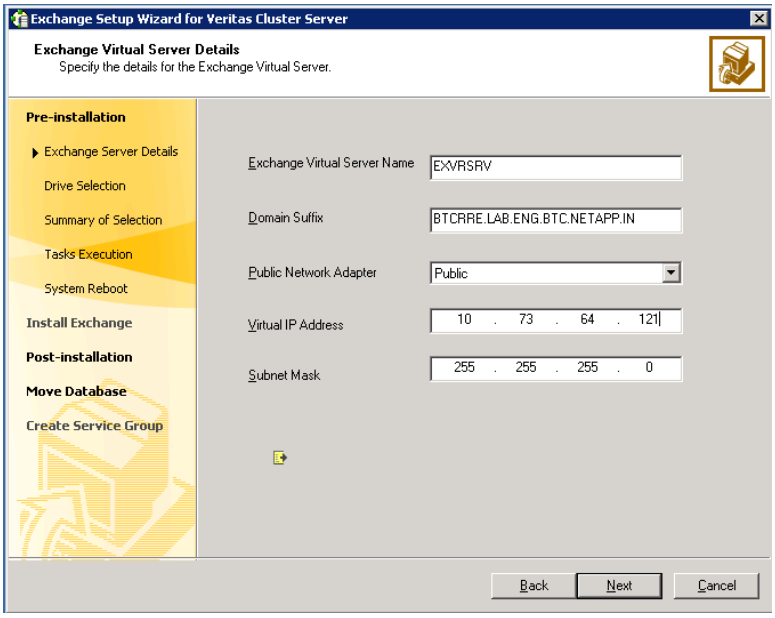

Figure 44) Exchange setup wizard (page 5).

6. Select a drive where the registry replication data will be stored and click **Next** (Drive F in this case).

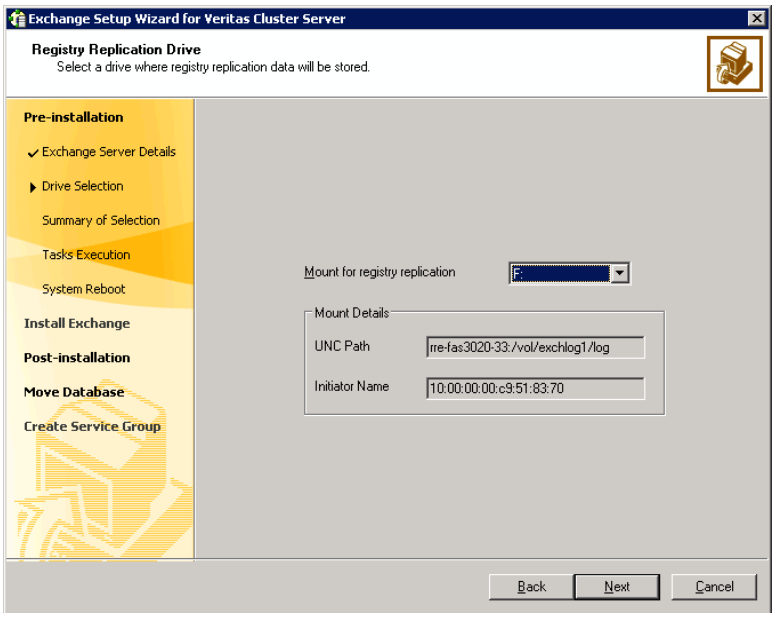

Figure 45) Exchange setup wizard (page 6).

7. Review the summary and click **Next**.

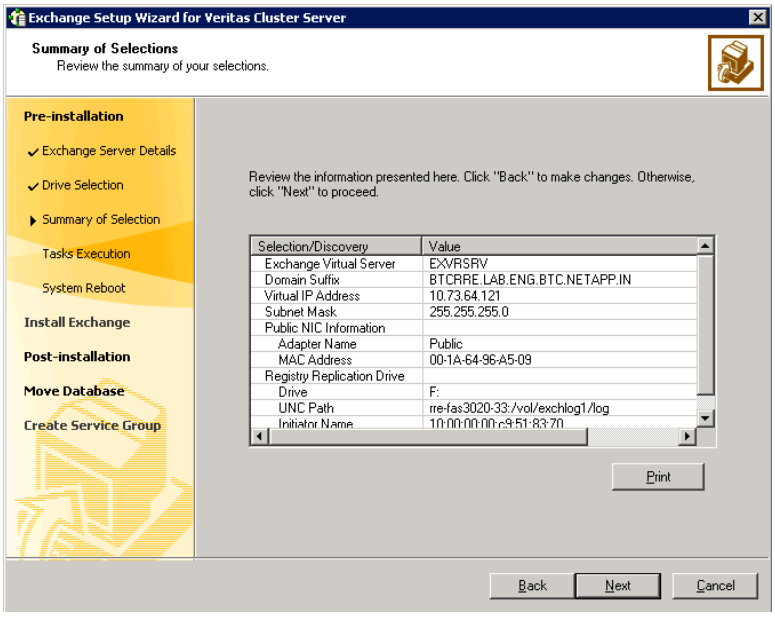

Figure 46) Exchange setup wizard (page 7).

8. Click **Yes** to continue at the prompt that the system will be renamed and restarted after you quit the wizard.

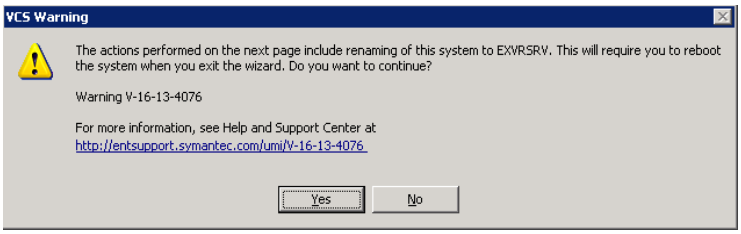

Figure 47) Exchange setup wizard (page 8).

9. Click **Next**.

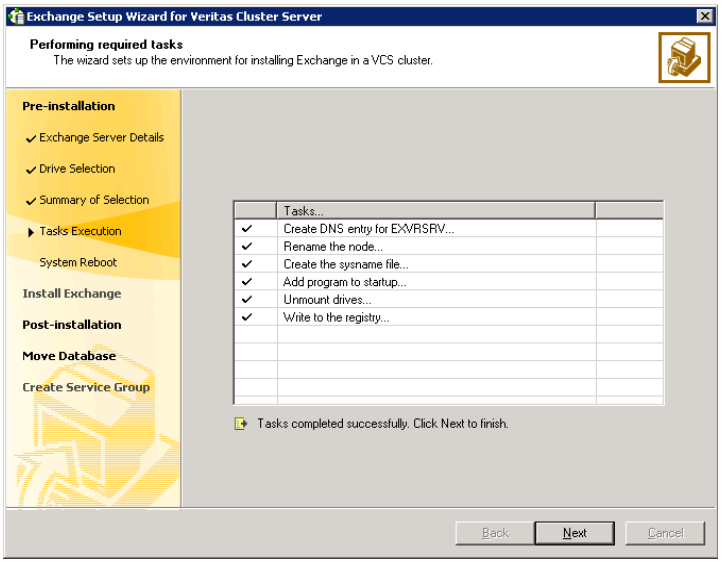

Figure 48) Exchange setup wizard (page 9).

10. Click **Reboot**.

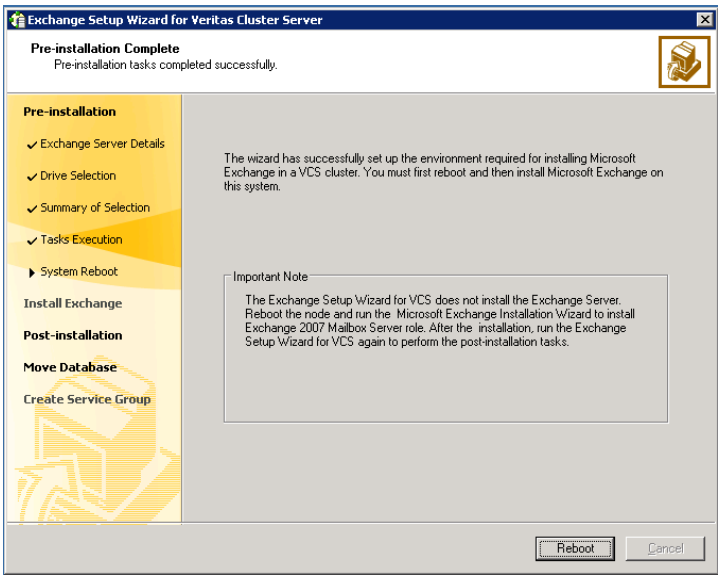

Figure 49) Exchange setup wizard (page 10).

Note: After you reboot the node, the value specified for the Exchange virtual server is temporarily assigned to the node. Therefore, all network connections to the node must be made using the temporary name. After installing Microsoft Exchange, you must run this wizard again to assign the original name to the node. On rebooting the node, the Exchange Setup Wizard for Veritas Cluster Server is launched automatically. Review the information in the wizard dialog box and proceed to installing Microsoft Exchange Server.

8.4.3 Installation of Microsoft Exchange Server on the First Node

Perform the following steps to install Microsoft Exchange Server on the first node after completing the preinstallation wizard.

Note: HA support for Microsoft Exchange Server is available only for the mailbox server role. While Installing Microsoft Exchange Server, be sure to install only the mailbox server role.

1. Prepare the Active Directory forest and domain. (Run the command `setup /prepareAD` from the installation media followed by the setup `/prepareDomain` command.)

```
C:\Documents and Settings\Administrator.BTCRRE\Desktop\exch2007_SP1_64bit>setup
/preparead

Welcome to Microsoft Exchange Server 2007 Unattended Setup

Preparing Exchange Setup

No server roles will be installed

Performing Microsoft Exchange Server Prerequisite Check

    Organization Checks              ........................... COMPLETED

Configuring Microsoft Exchange Server

    Organization Preparation         ........................... COMPLETED

The Microsoft Exchange Server setup operation completed successfully.

C:\Documents and Settings\Administrator.BTCRRE\Desktop\exch2007_SP1_64bit>+_
```

```
C:\Documents and Settings\Administrator.BTCRRE\Desktop\exch2007_SP1_64bit>setup
/preparedomain

Welcome to Microsoft Exchange Server 2007 Unattended Setup

Preparing Exchange Setup

No server roles will be installed

Performing Microsoft Exchange Server Prerequisite Check

    Organization Checks              ........................... COMPLETED

Configuring Microsoft Exchange Server

    Prepare Domain Progress          ........................... COMPLETED

The Microsoft Exchange Server setup operation completed successfully.

C:\Documents and Settings\Administrator.BTCRRE\Desktop\exch2007_SP1_64bit>_
```

2. Run Exchange 2007 Setup, click **Install Microsoft Exchange**, then click **Next**.
3. Select installation type **Custom Installation** and click **Next**. Select **Mailbox Server Role and Exchange Management Tools** and complete the Exchange Server installation.

8.4.4 Postinstallation: Exchange Server Setup Wizard

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

1. Make sure that the LUN containing the registry replication information is connected to the node on which you will perform the postinstallation procedure.
2. If the Exchange installation did not prompt you to reboot the node, click **Continue** from the Exchange Server Setup Wizard and proceed to step 4. If you rebooted the node after Microsoft Exchange installation, the Exchange Server Setup Wizard launches automatically.
3. Review the information and click **Continue**.

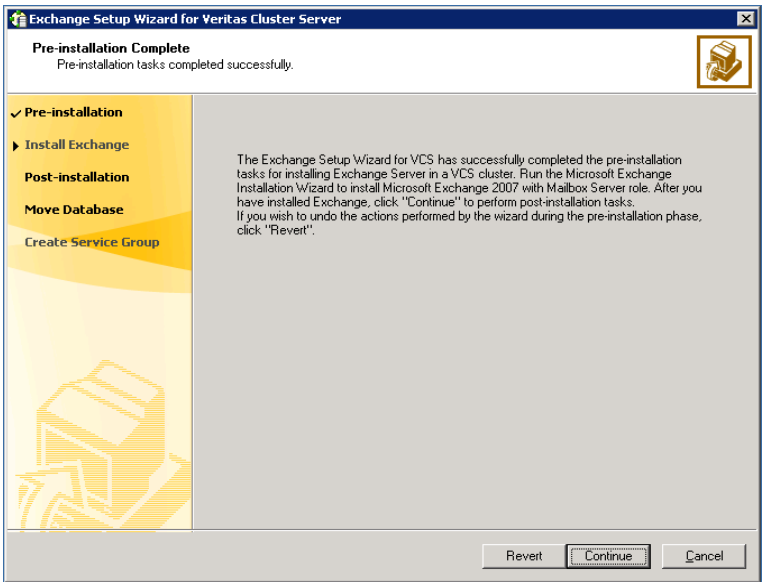

Figure 50) Exchange setup wizard (page 1).

4. Click **Yes** to continue. This sets the node name back to its physical host name.

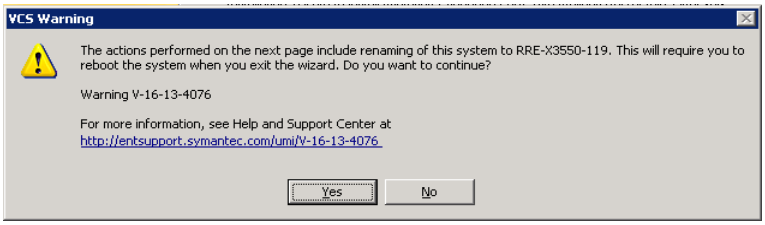

Figure 51) VCS warning.

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

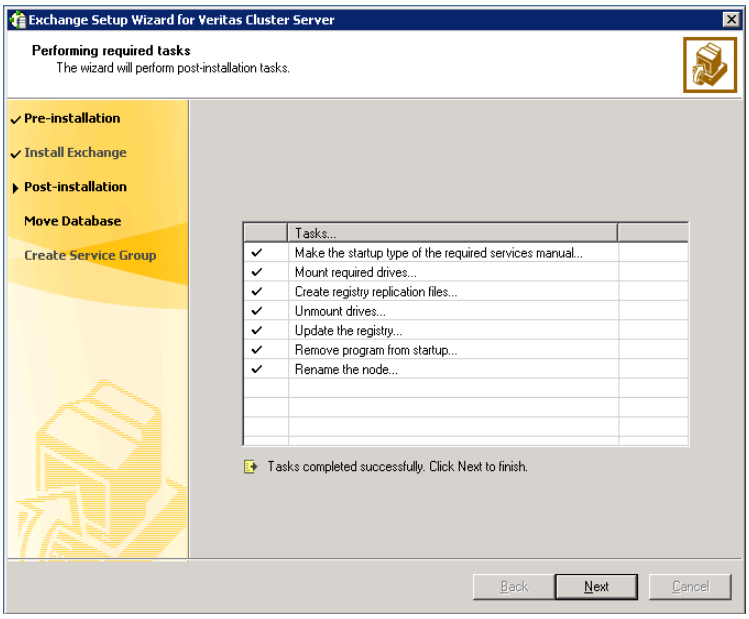

Figure 52) Exchange setup wizard (page 3).

6. Click **Finish**.

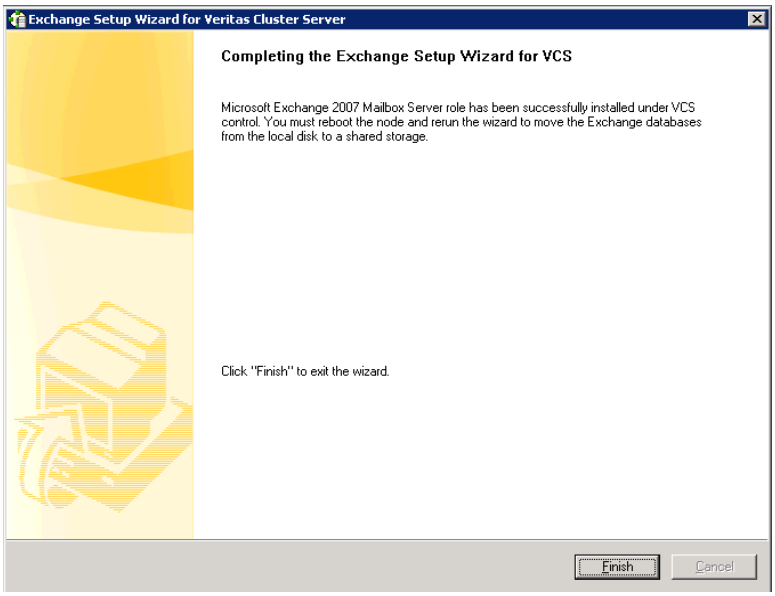

Figure 53) Exchange setup wizard (page 4).

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

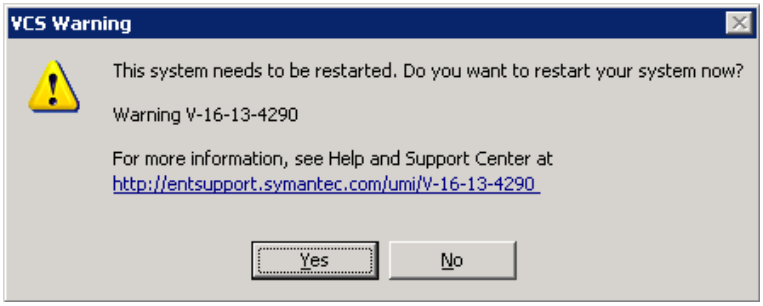

Figure 54) Exchange setup wizard (page 5).

NOTE: Changes made during the postinstallation phase do not take effect until the server is rebooted. After the server is rebooted, move the databases created during the Exchange installation on the local drive to the shared storage.

8.4.5 Moving the Exchange Server Databases to Shared Storage

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

Complete the following tasks before moving the databases:

- Make sure that the LUNs created to store the Exchange database, transaction logs, and registry replication information are connected.
- The Exchange Setup Wizard for Veritas Cluster Server cannot move the Exchange storage groups until local continuous replication (LCR) is suspended for those storage groups. Suspend LCR using the Exchange management console or the Exchange management shell before moving the Exchange databases. Refer to the Microsoft Exchange documentation for information on how to suspend LCR.

Perform the following steps to move the Exchange Server databases to the shared storage:

1. Start the Exchange Setup Wizard for Veritas Cluster Server by clicking **Start > All Programs Symantec > Veritas Cluster Server > Configuration Tools > Exchange Server 2007 Setup Wizard**. Review the information in the Welcome pane and click **Next**.

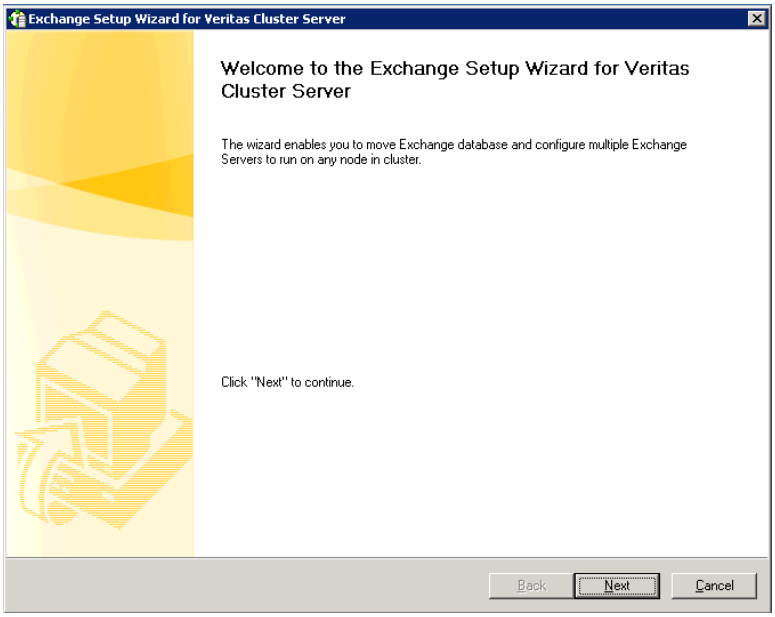

Figure 55) Moving Exchange Server Databases to shared storage (1).

2. In the Available Option pane, select **Configure/Remove highly available Exchange Server** and click **Next**.

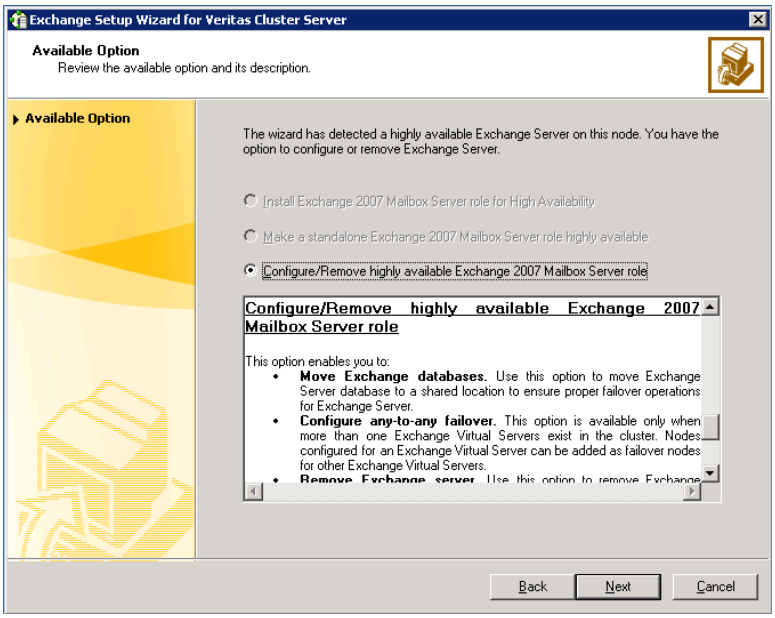

Figure 56) Moving Exchange Server Databases to shared storage (2).

3. In the Select Option pane, select **Move Exchange Databases** and click **Next**.

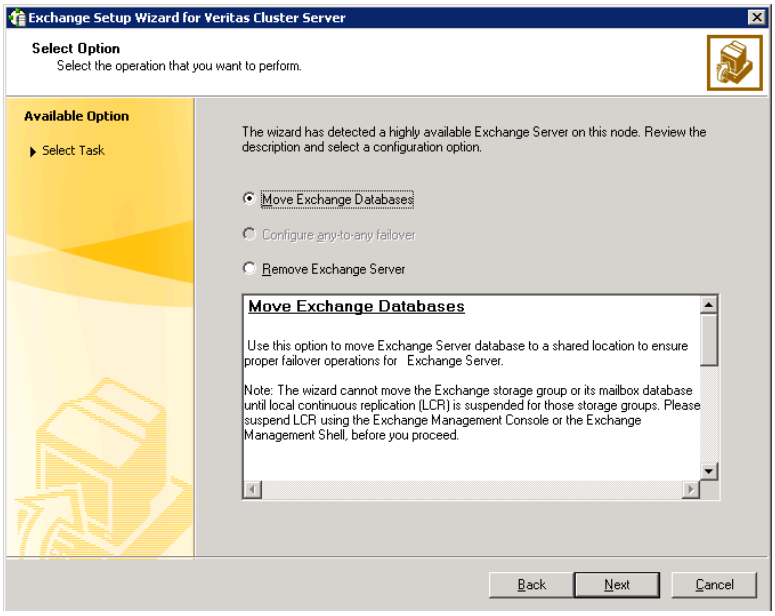

Figure 57) Moving Exchange Server Databases to shared storage (3).

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

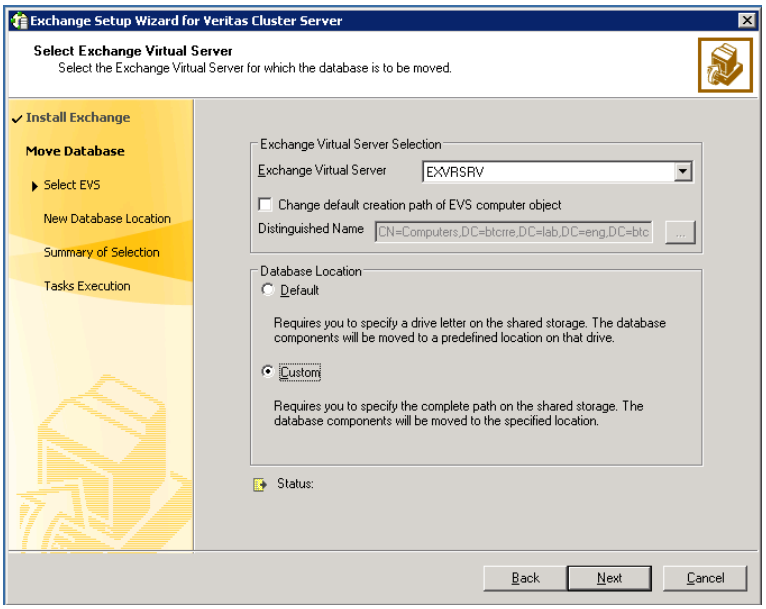

Figure 58) Moving Exchange Server Databases to shared storage (4).

5. In the Exchange Database Components pane, enter data and log LUN information and then click **Next**. **Note**: For the Exchange database and logs enter separate drives.

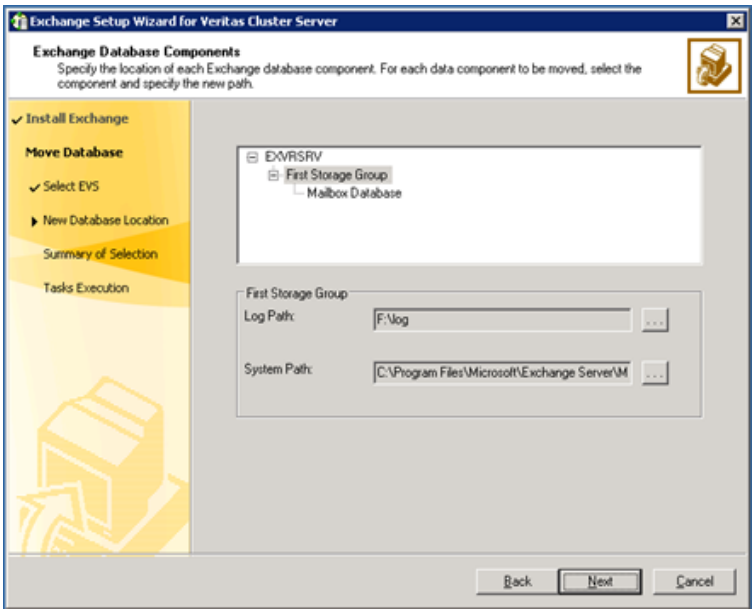

Figure 59) Moving Exchange Server Databases to shared storage (5).

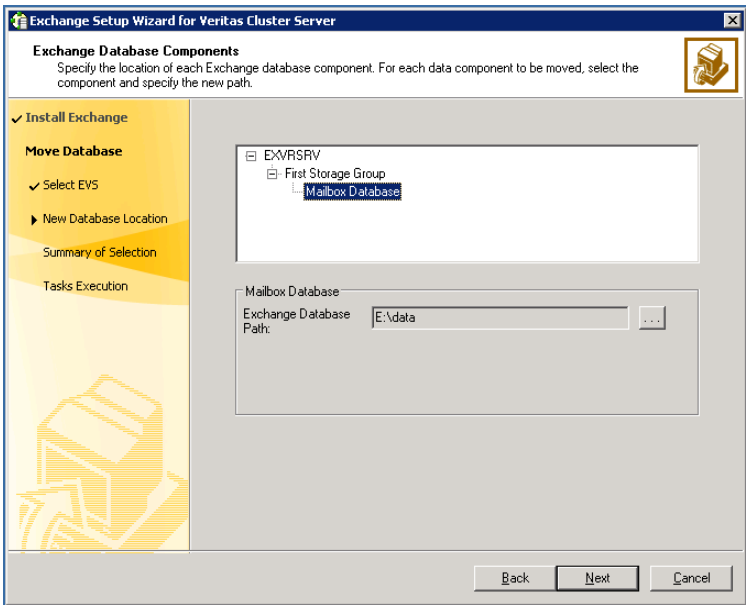

Figure 60) Moving Exchange Server Databases to shared storage (6).

6. Review the summary and click **Next**.

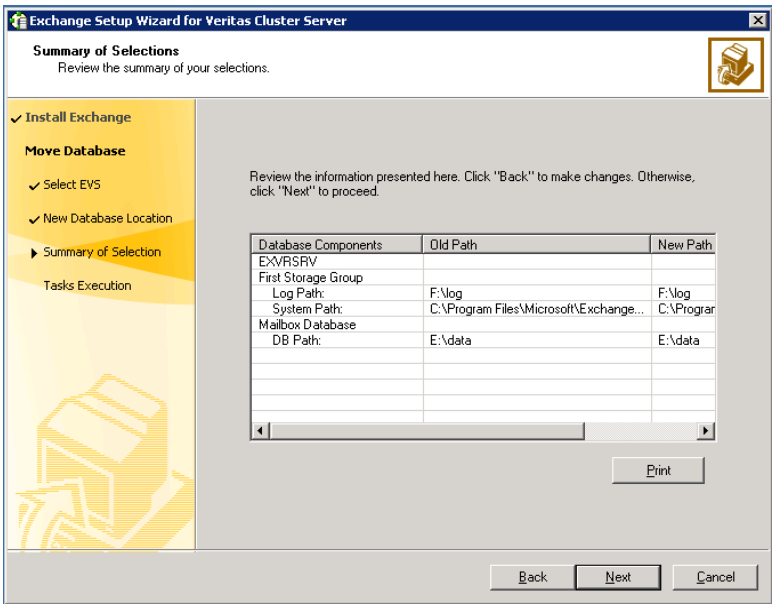

Figure 61) Moving Exchange Server Databases to shared storage (7).

7. 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.**

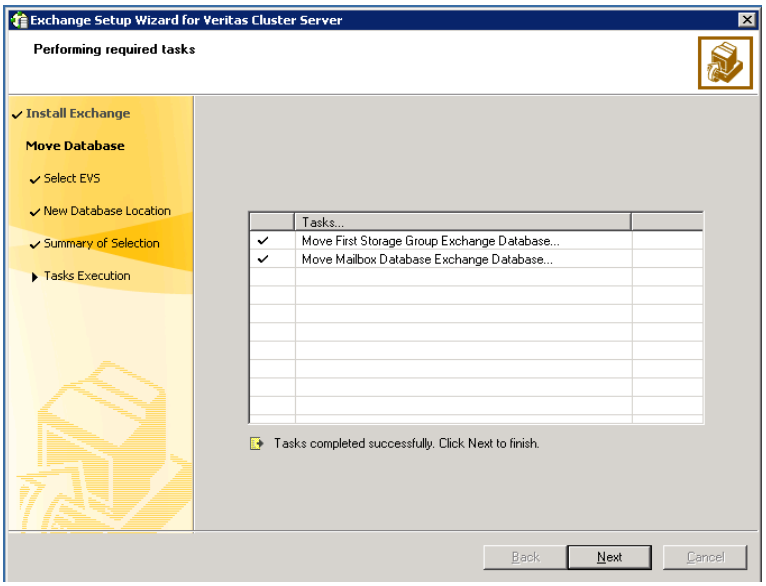

Figure 62) Moving Exchange Server Databases to shared storage (8).

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

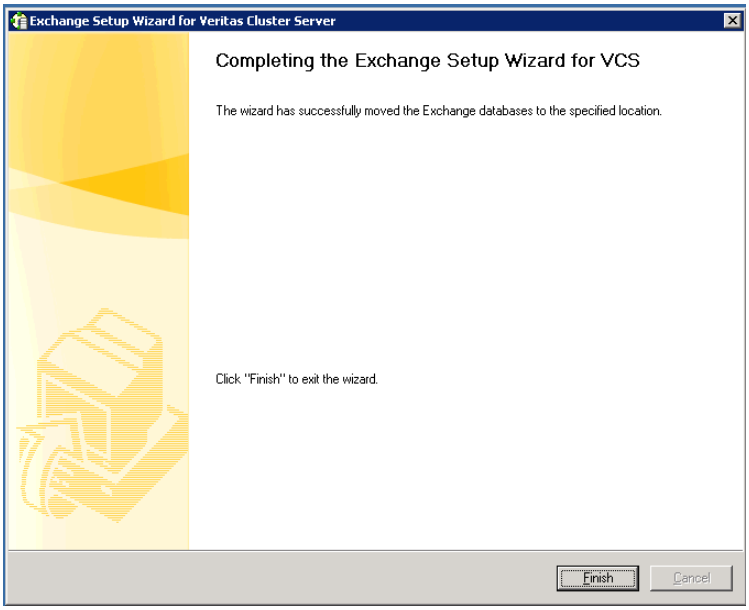

Figure 63) Moving Exchange Server Databases to shared storage (9).

8.4.6 Installing Microsoft Exchange Server 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 preinstallation, installation, and postinstallation procedures on each additional node.

PREINSTALLATION

Use the Exchange Server Setup Wizard for Veritas Cluster Server to complete the preinstallation phase. Before adding a node to the Exchange cluster, make sure that the server meets the prerequisites for the Exchange Server installation.

1. Disconnect the LUNs created to store the registry replication information on the first node.
2. From this additional/second node, connect to the already created LUN for registry replication. Make sure that LUNs are not connected to any other nodes.
3. Start the Exchange Server Setup Wizard for Veritas Cluster Server from the node to be added to an Exchange cluster by clicking **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange Server 2007 Setup Wizard**.
4. Review the information in the Welcome pane and click **Next.**

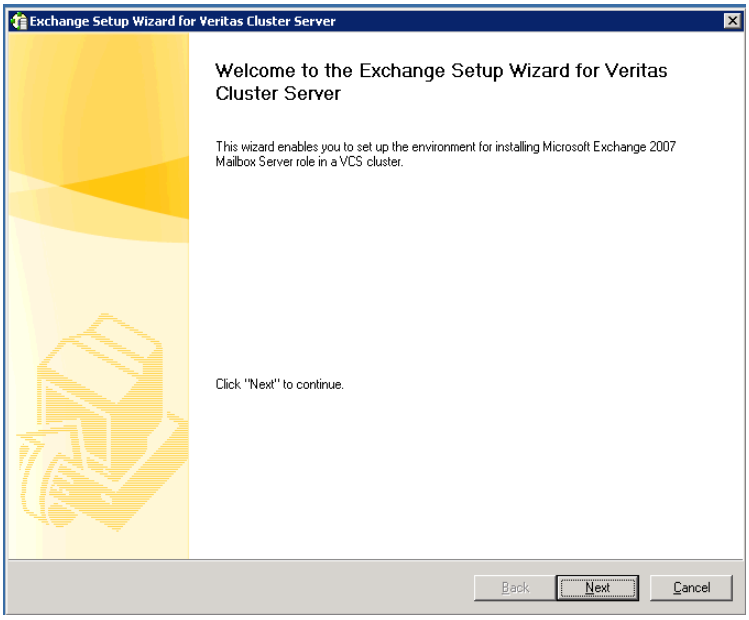

Figure 64) Preinstallation (1).

5. In the Available Option pane, click **Install Exchange 2007 Mailbox Server role for High Availability** and click **Next.**

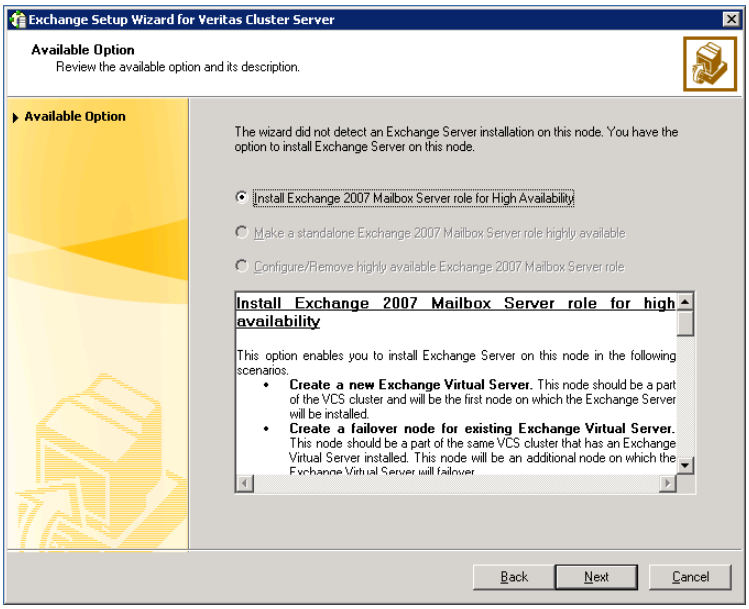

Figure 65) Preinstallation (2).

6. In the Select Option pane, click **Create a failover node for existing Exchange Virtual Server** and click **Next**.

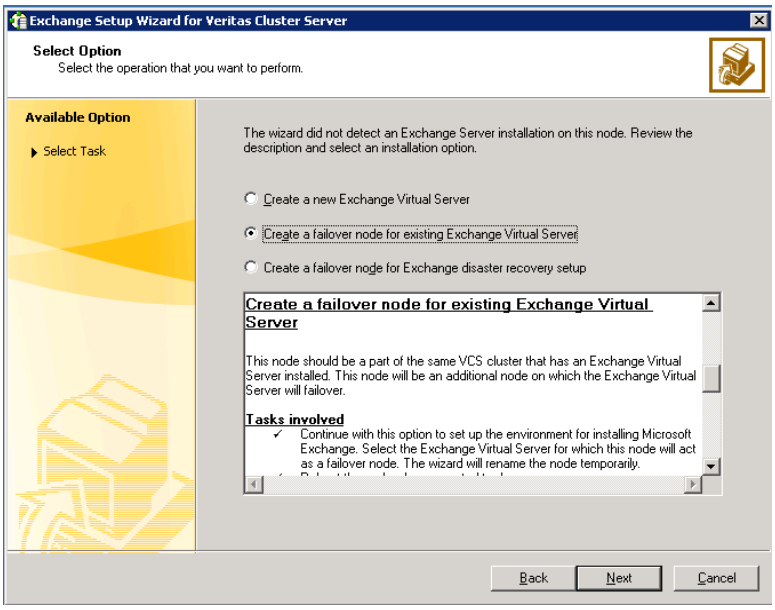

Figure 66) Preinstallation (3).

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

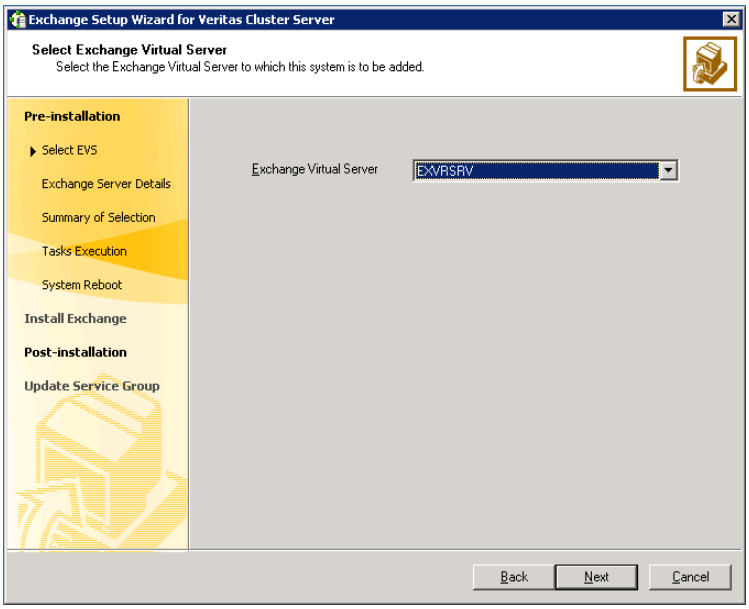

Figure 67) Preinstallation (4).

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.
   a. 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.
   b. Enter the virtual IP address for the Exchange virtual server.
   c. Click **Next**.

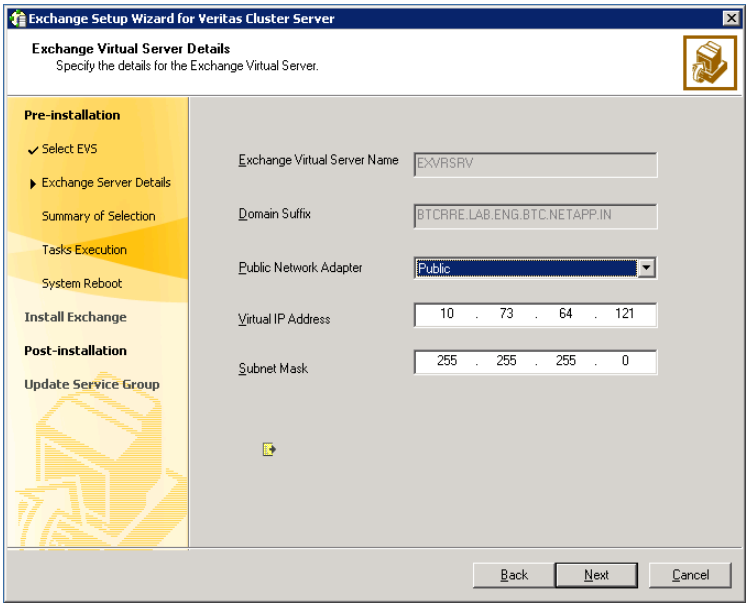

Figure 68) Preinstallation (5).

9. Read the warning and select **Yes.**

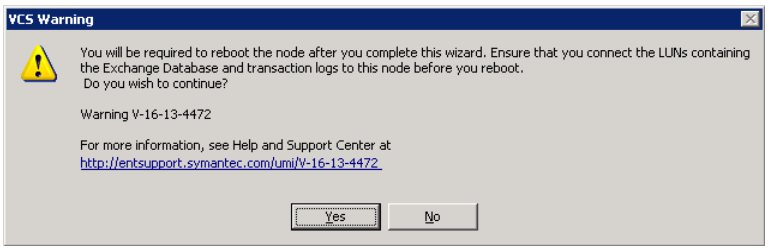

Figure 69) Preinstallation (6).

10. Review the summary and select **Next**.

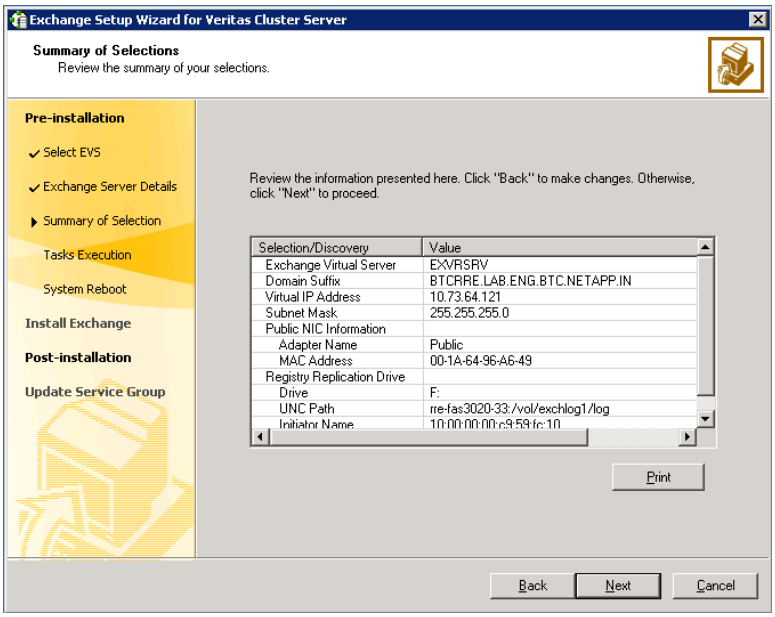

Figure 70) Preinstallation (7).

11. A message appears informing you that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue and the wizard starts running commands to set up the Veritas Cluster Server environment.

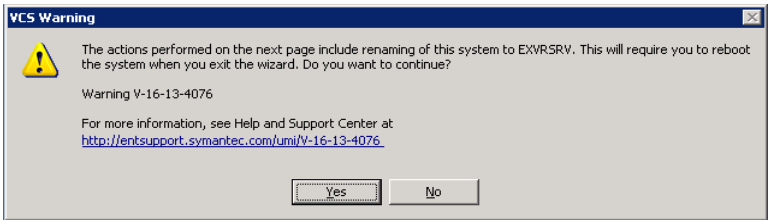

Figure 71) Preinstallation (8).

12. Various messages indicate the status of each task. After all the commands are executed, click **Next**.

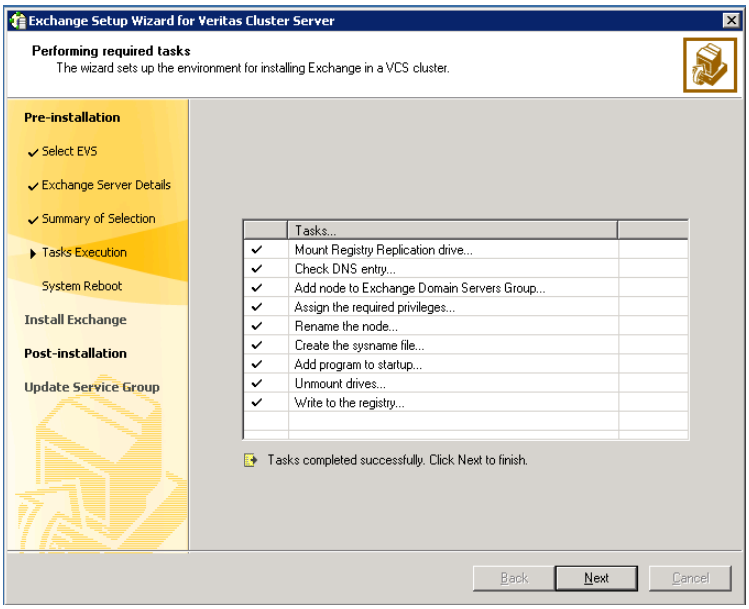

Figure 72) Preinstallation (9).

13. Click **Reboot**.

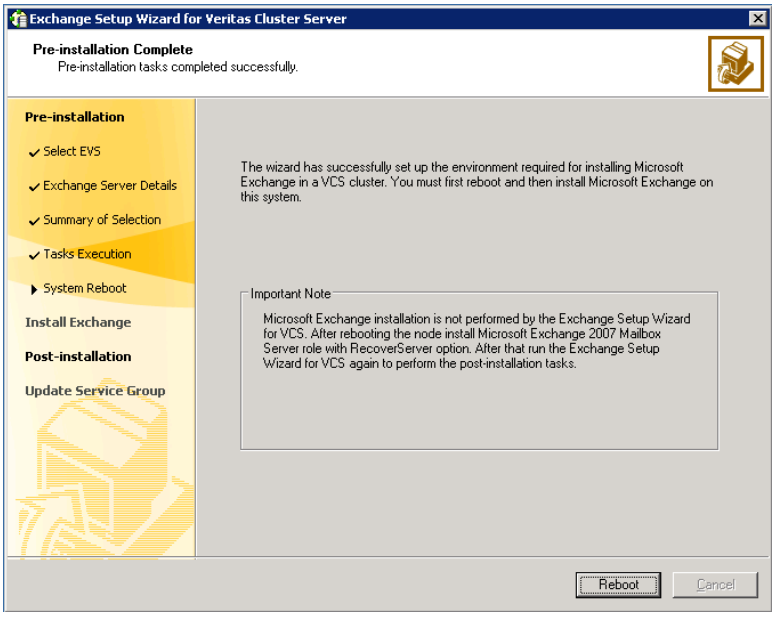

Figure 73) Preinstallation (10).

14. Click **Yes.**

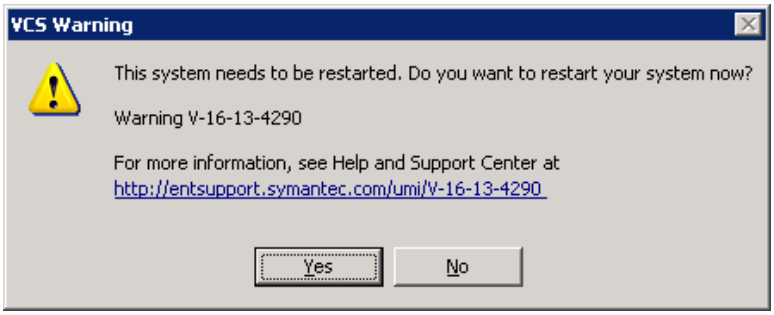

Figure 74) Preinstallation (11).

Note: 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.

8.4.7 Microsoft Exchange Server Installation on Additional Nodes

Install Exchange on the node where the Exchange Server Setup Wizard was run for the preinstallation tasks.

Note: HA support for Microsoft Exchange Server 2007 is available only for the mailbox server role. Be sure to install only the mailbox server role and also be sure to install the same version of Exchange Server and components.

Perform the following steps to complete the Exchange Server installation on the additional nodes:

1. Begin the Exchange installation for disaster recovery at the command prompt using RecoverServer as the install mode (**`<drive letter> setup.com /mode:recoverserver`**, where the drive letter is the installation media location).

```
C:\Documents and Settings\Administrator.BTCRRE\Desktop\exch2007_SP1_64bit>setup
/mode:recoverserver

Welcome to Microsoft Exchange Server 2007 Unattended Setup

Preparing Exchange Setup

The following server roles will be recovered
    Mailbox Role
    Management Tools

Performing Microsoft Exchange Server Prerequisite Check

    Mailbox Role Checks               ..... COMPLETED

Configuring Microsoft Exchange Server

    Copying Exchange files            ..... COMPLETED
    Mailbox Role                      ..... COMPLETED
    Exchange Management Tools         ..... COMPLETED

The Microsoft Exchange Server setup operation completed successfully.
Setup has made changes to operating system settings that require a reboot to tak
e effect. Please reboot this server prior to placing it into production.

C:\Documents and Settings\Administrator.BTCRRE\Desktop\exch2007_SP1_64bit>_
```

2. Setup copies the setup files locally to the computer on which you are installing Exchange 2007 and then checks the prerequisites, including all prerequisites specific to the server roles that you are installing. If you have not met all of the prerequisites, setup fails and returns an error message that explains the reason for the failure. If you have met all of the prerequisites, setup installs Exchange 2007.
3. Verify that the installation completed successfully.

8.4.8 Postinstallation: Installing Microsoft Exchange Server 2007 on Additional Nodes

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

To run the Exchange postinstallation:

1. Make sure that the LUNs containing the registry replication information and the Exchange database are connected to the node on which you will perform the postinstallation.
2. If the Exchange installation did not prompt you to reboot the node, click **Continue** from the Exchange Server Setup Wizard and proceed to step 4.

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

3. Review the information in the Welcome pane and click **Continue**.

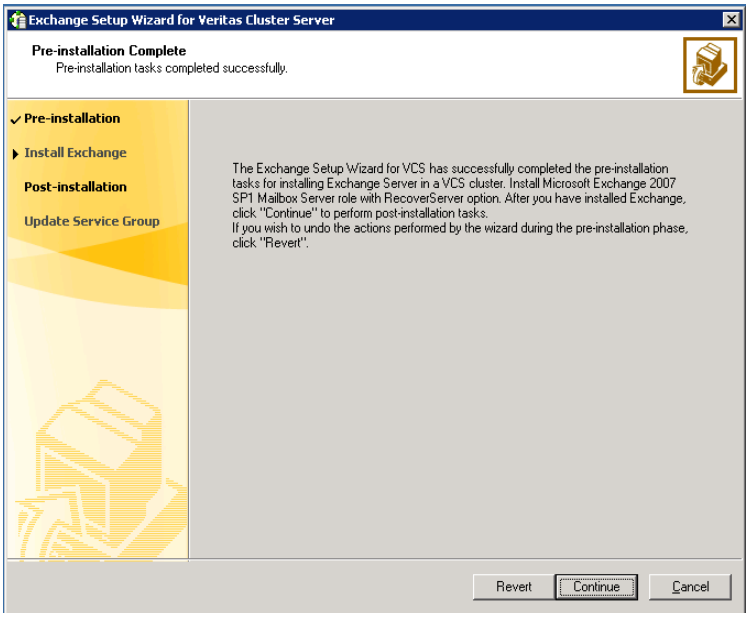

Figure 75) Post installation (1).

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

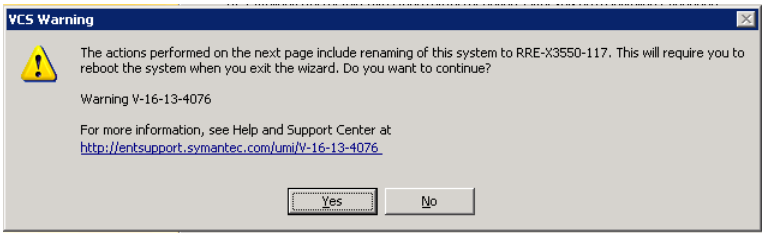

Figure 76) Post installation (2).

4. The wizard starts performing the postinstallation tasks. After all commands are executed, click **Next**.

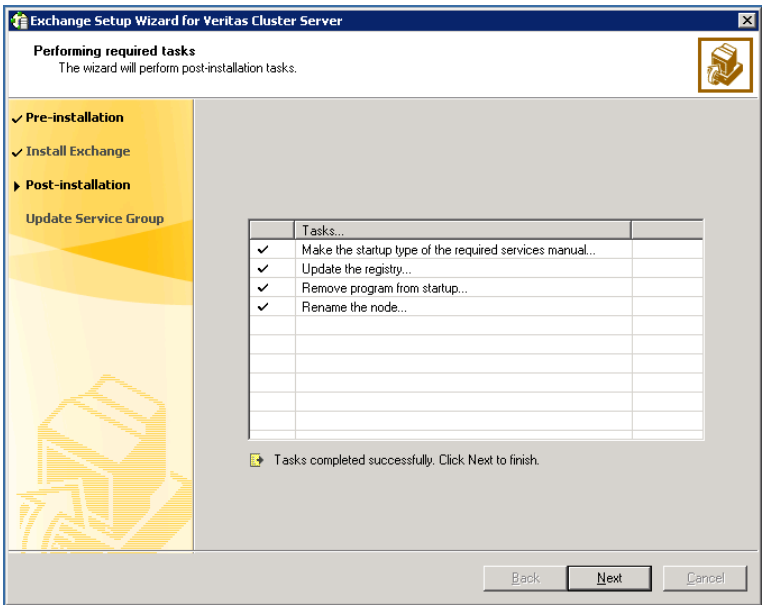

Figure 77) Post installation (3).

5. Specify whether you want to add the node to the SystemList of the service group for the EVS selected in the Exchange preinstallation step.

   Note: 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**.

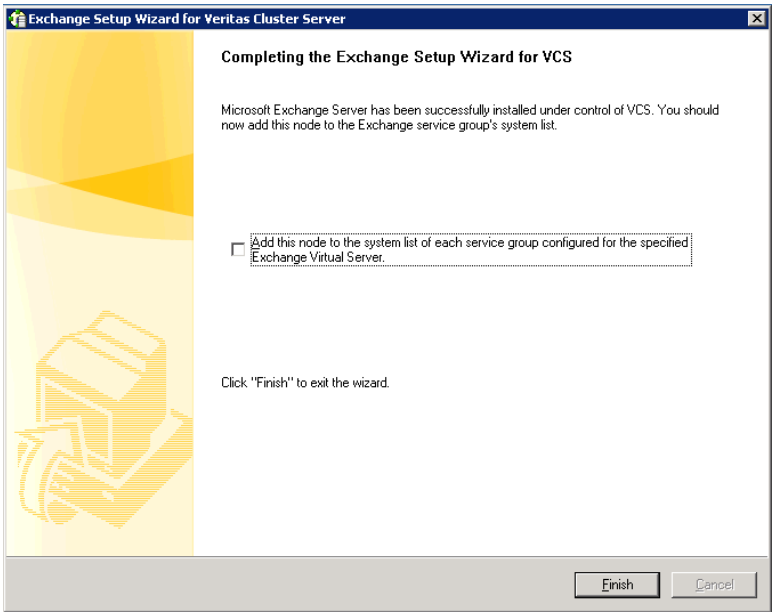

Figure 78) Post installation (4).

7. When the wizard prompts you to reboot the node, click **Yes**.

   Note: Changes made during the postinstallation steps do not take effect until you reboot the node.

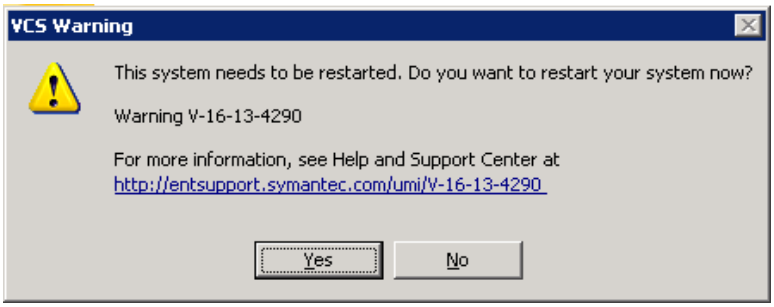

Figure 79) Post installation (5).

8.4.9 Configuring the Exchange Service Group

Before configuring the service group, be sure the following prerequisites are met.

Prerequisites

- Verify that Veritas Cluster Server for NetApp SnapMirror is installed on all cluster nodes.
- Verify that Exchange is installed and configured identically on all the cluster nodes.
- Verify that the cluster is configured using the Veritas Cluster Server configuration wizard.
- 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 storage system containing the LUNs created to store Exchange data components.
- Verify that the command server is running on all systems in the cluster.
- Verify that the Veritas high-availability daemon (HAD) is running on the system from where you run the wizard.
- Verify that the virtual disks (LUNs) created to store the following data components are connected to the node where you run the wizard and are disconnected from other nodes in the cluster.

Configuration Instructions

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

1. Start the Exchange Server Configuration Wizard by clicking **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools> Exchange Server 2007 Configuration Wizard**.
2. Review the information in the Welcome pane and click **Next.**

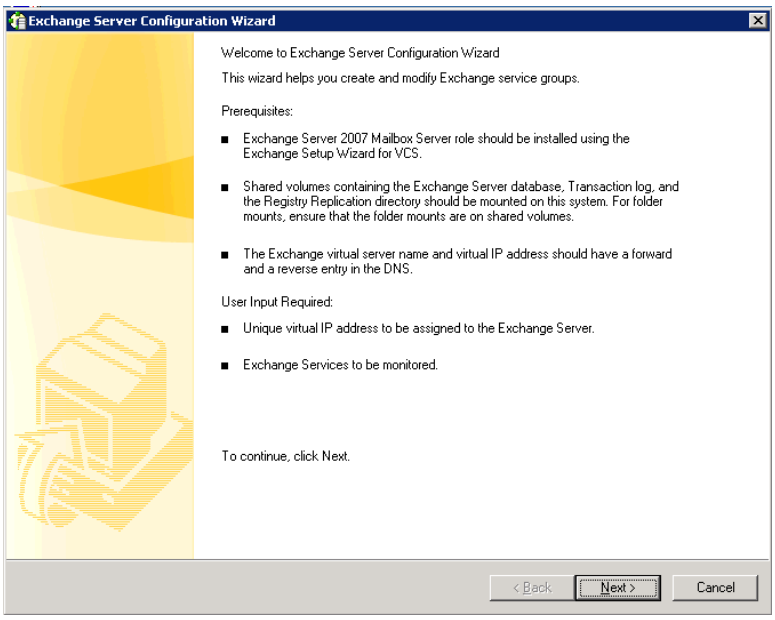

Figure 80) Configuration (1).

3. In the Wizard Options pane, select **Create service group** and click **Next.**

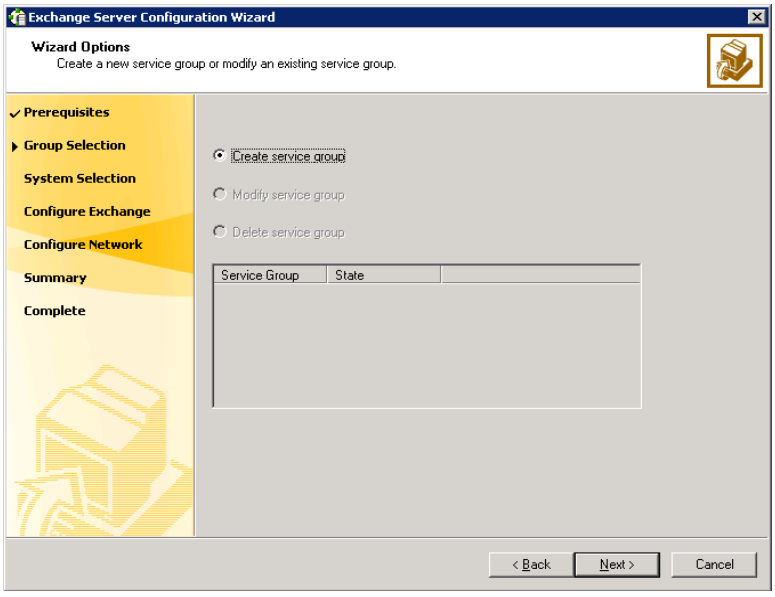

Figure 81) Configuration (2).

4. On the Service Group Configuration pane, specify the service group name and the systems that will be part of the service group as follows. Then click **Next**.

- Service Group Name: Type a name for the Exchange service group.

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

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

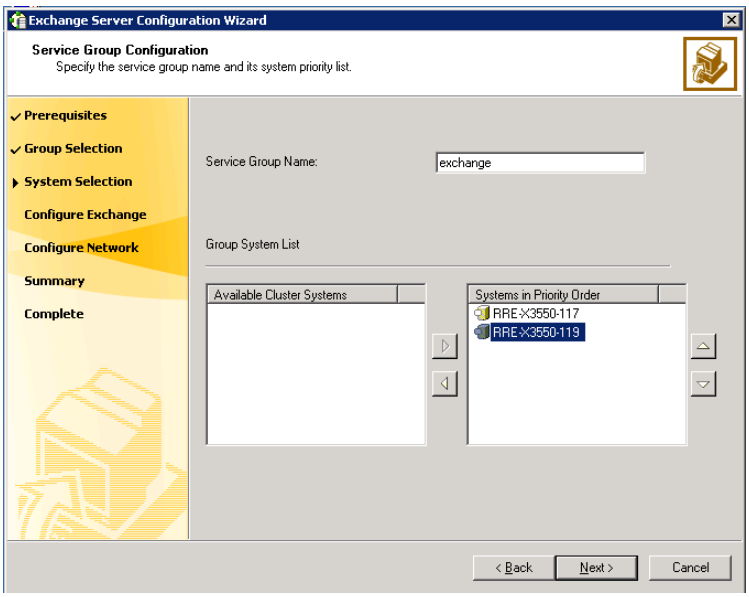

Figure 82) Configuration (3).

5. On the Exchange Server Configuration pane, verify that the Exchange virtual server name and paths to the LUNs were created to store Exchange data.
   Note: An informational message appears asking if you choose to configure a SnapMirror resource without configuring replication between NetApp storage systems at the primary and secondary DR 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.
   a. Specify the Exchange virtual server.
   b. Check the **Configure NetApp SnapMirror Resource(s)** checkbox if you want to configure a NetApp SnapMirror resource. A SnapMirror resource is required only in case of a disaster recovery configuration. If running the wizard to modify a service group, unchecking this checkbox removes the NetApp SnapMirror resource from the service group configuration. Keep this unchecked the first time you create a service group on the source side.
   c. Verify the Exchange database and transaction log path, then click **Next**.

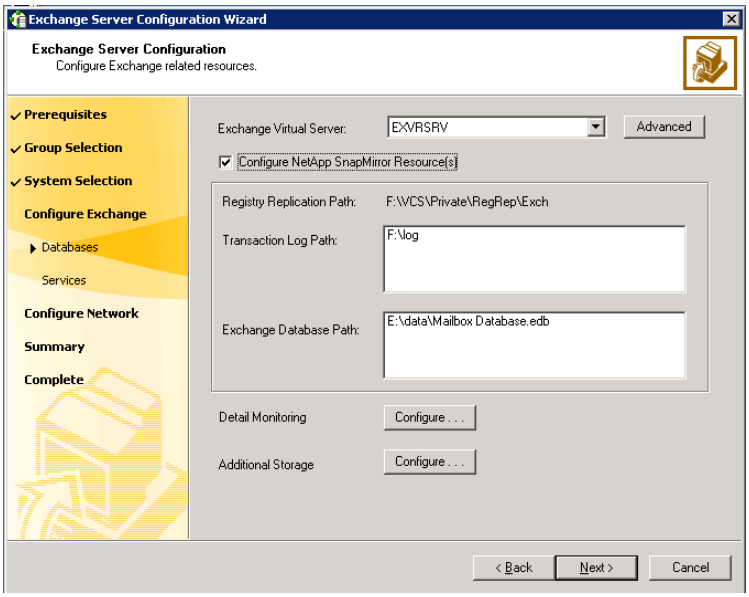

Figure 83) Configuration (4).

6. Select the optional Exchange services to be monitored and click **Next**. Each optional service that is selected will be configured as a Veritas Cluster Server resource of type ExchService2007.

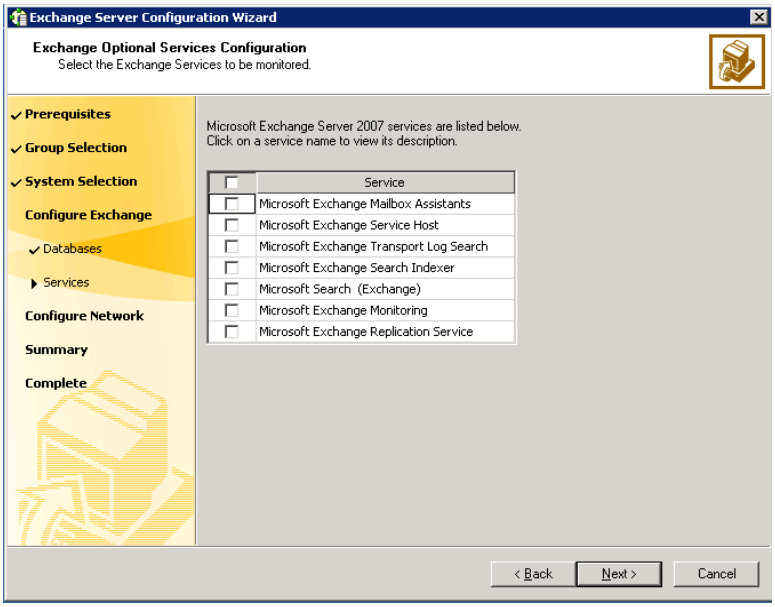

Figure 84) Configuration (5).

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

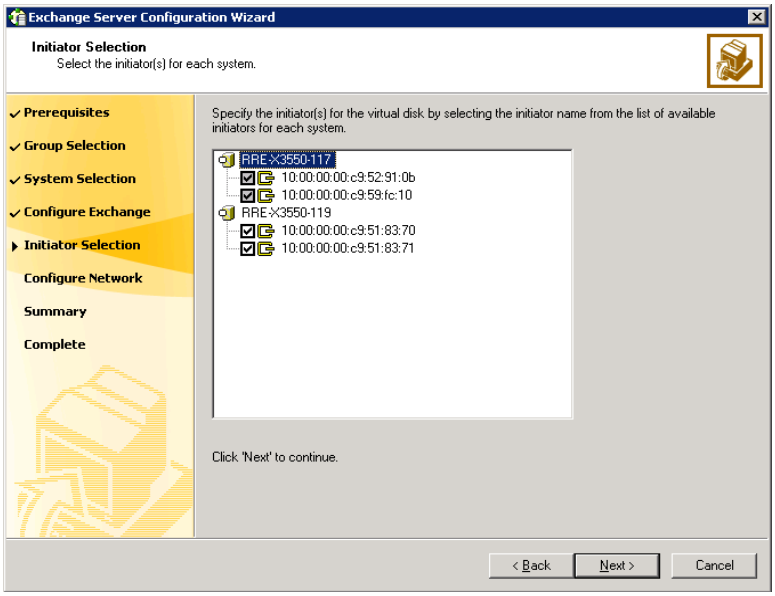

Figure 85) Configuration (6).

8. On the Network Configuration pane, specify network-related information and then click **Next**.
   Note: 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.

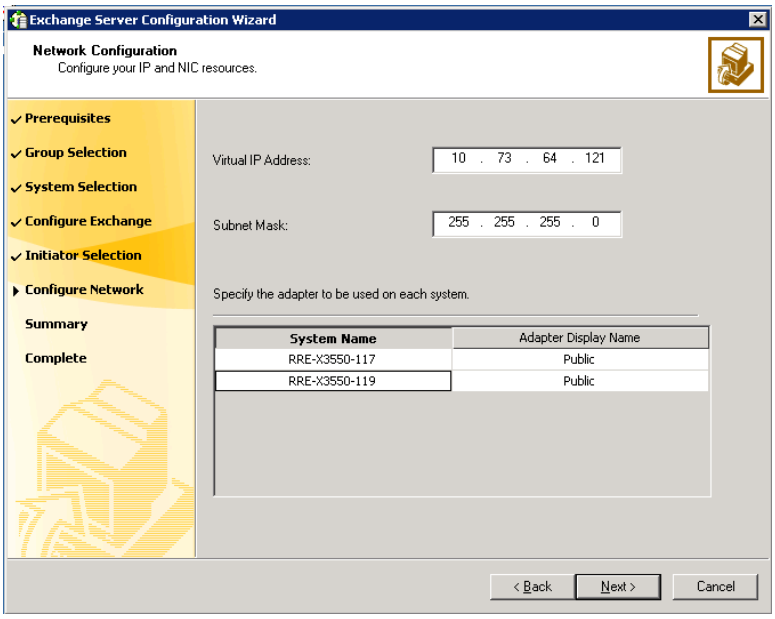

Figure 86) Configuration (7).

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

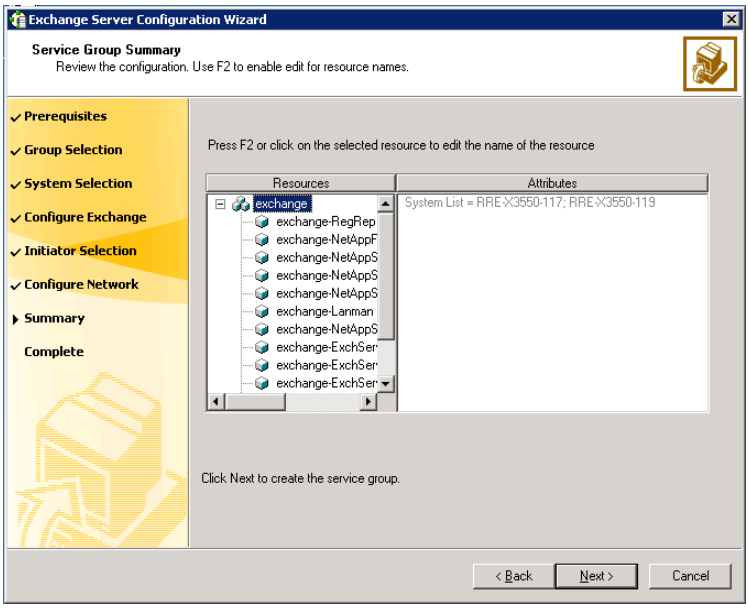

Figure 87) Configuration (8).

10. Click **Yes** at the prompt so that the wizard will run commands to modify the service group configuration. Various messages indicate the status of these commands.

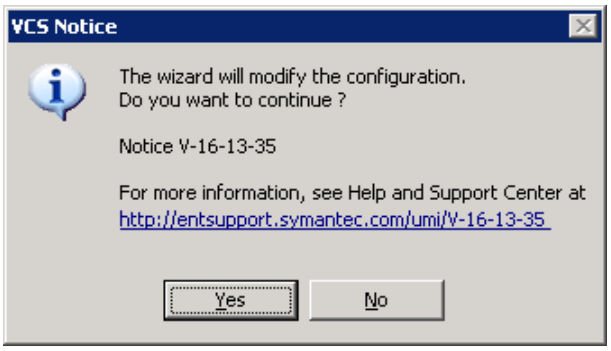

Figure 88) Configuration (9).

11. In the Completing the Exchange Configuration pane, select the **Bring the service group online** checkbox to bring the service group online on the local node. Then click **Finish**.
    Note: After bringing the service group online, run the Exchange management console to modify the database settings such that all the stores are automatically mounted on startup.

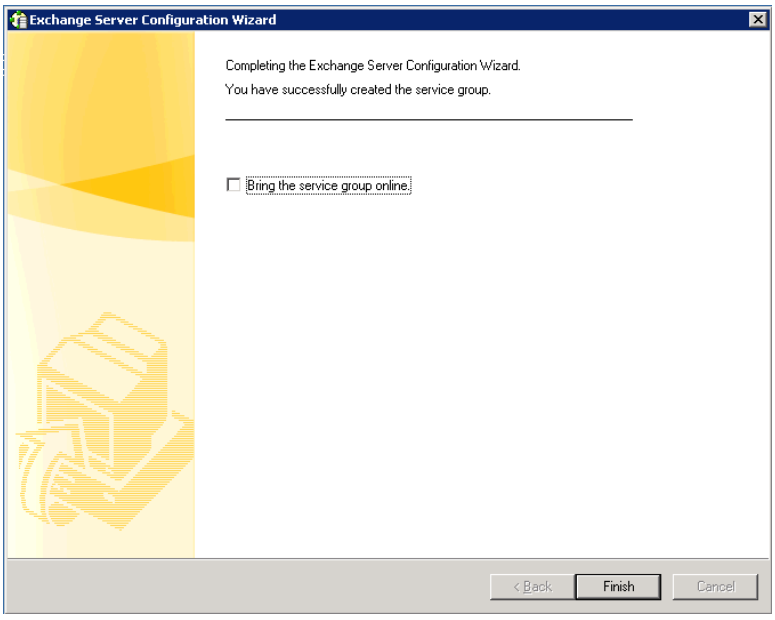

Figure 89) Configuration (10).

8.4.10 Configuring the Stores to Mount at Startup

Run the Exchange Management console so that all the stores that were previously mounted are automatically mounted on startup.

Perform the following steps to reconfigure mounting of stores at startup:

1. Start Exchange 2007 Management Console.
2. Select Mailbox in the left pane under Server Configuration and select the Exchange Server from the right pane.

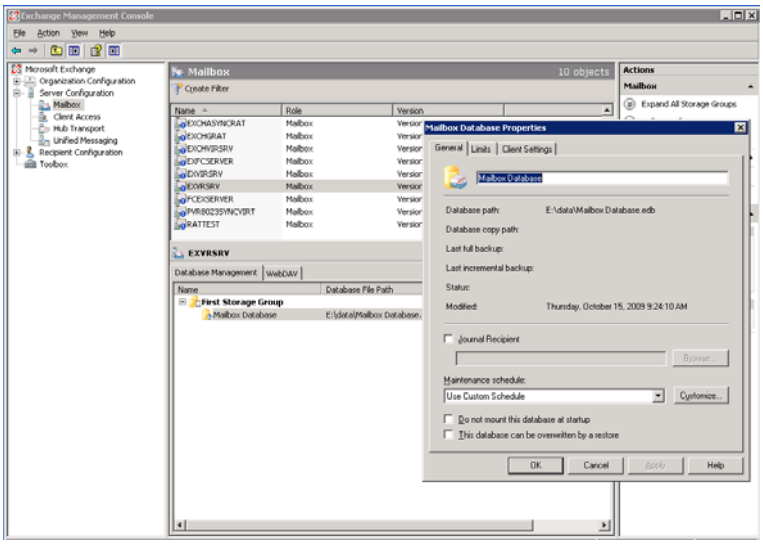

Figure 90) Configuration for stores to mount at startup.

3. Right-click and choose properties of the database. Clear the **Do not mount this database at startup** checkbox from the General tab. Click **OK.**

8.5 INSTALLING AND CONFIGURING SNAPMANAGER FOR EXCHANGE

Install SnapManager for Exchange on all members of the cluster. For more information about installing, configuring, and administering SnapManager for Exchange, see the "SnapManager for Exchange Installation and Administration Guide."

SnapManager 5.0 for Microsoft Exchange Installation and Administration Guide

SnapManager 4.0 for Microsoft Exchange Installation and Administration Guide

8.6 DEPLOYING AGENTS FOR DISASTER RECOVERY IN THE SECONDARY DR SITE

This section describes the steps to be performed in the secondary DR site to set up a disaster recovery solution for Microsoft Exchange Server using the Veritas Cluster Server agent for NetApp 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.

8.6.1 Setting Up the Secondary DR Site

Do the following before proceeding:

- Configure the Exchange databases for backup and restore using the SnapManager for Exchange Configuration Wizard.
- Make sure the volumes at both sites are of the same size.
- Make sure the LUN names used on the destination volume are the same name as in the source vol.

The following sections provide a brief overview of the steps to configure the secondary site.

1. Install Veritas Cluster Server for NetApp SnapMirror with the GCO option and then configure the Veritas Cluster Server cluster. While configuring the cluster, ensure that you select the GCO option to configure the wide area connector (WAC) resource in the cluster at the secondary site.
2. Install Microsoft Exchange at the secondary site using the Exchange Server Setup Wizard for Veritas Cluster Server.
3. Configure an Exchange service group with SnapMirror resources at the secondary site.

4. Replicate the volumes containing data for all Exchange components using NetApp SnapMirror.
5. Configure SnapMirror resources in the Exchange service group at the primary site.
6. Link the clusters at the primary and secondary sites.
7. Configure the Exchange service group to be a global group.

INSTALLING AND CONFIGURING VCS SOFTWARE AT THE SECONDARY (DR) SITE

To install Veritas Cluster Server software, see the section Installing Veritas Cluster Server Software.

To configure clusters, see the section Configuring Veritas Cluster Server Cluster.

INSTALLING MICROSOFT EXCHANGE SERVER AT THE SECONDARY (DR) SITE

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

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

Installing on First Failover Node at Secondary Site

The procedure for installing Microsoft Exchange Server at the secondary (DR) site is similar to the installation procedure at the primary site, except for the preinstallation process for the first failover node, detailed below.

Preinstallation Instructions

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

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

1. Verify that 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 Veritas Cluster Server.
3. In the Available Option pane, click **Install Exchange Server for High Availability** and click **Next**.

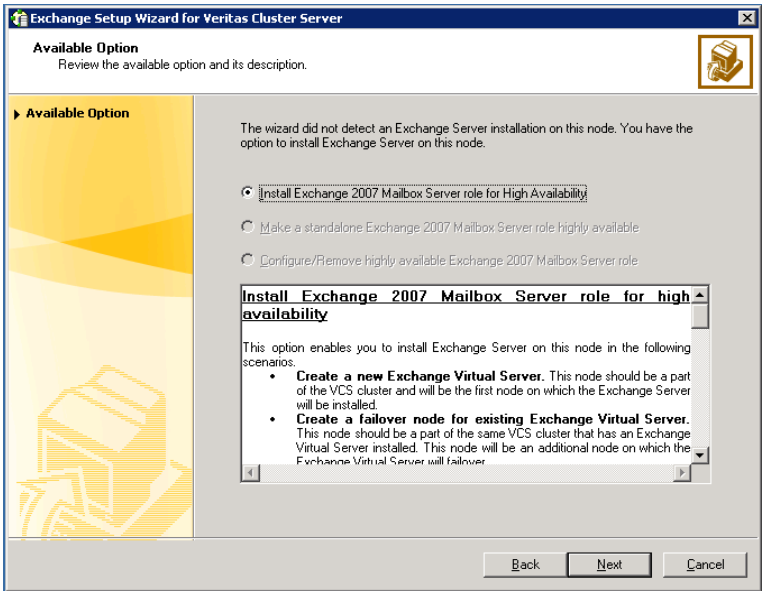

Figure 91) Preinstallation (1).

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

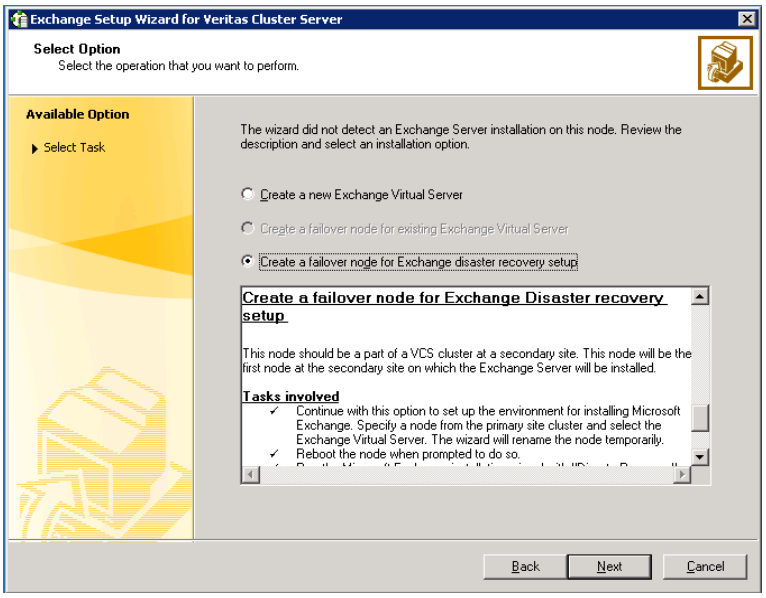

Figure 92) Preinstallation (2).

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

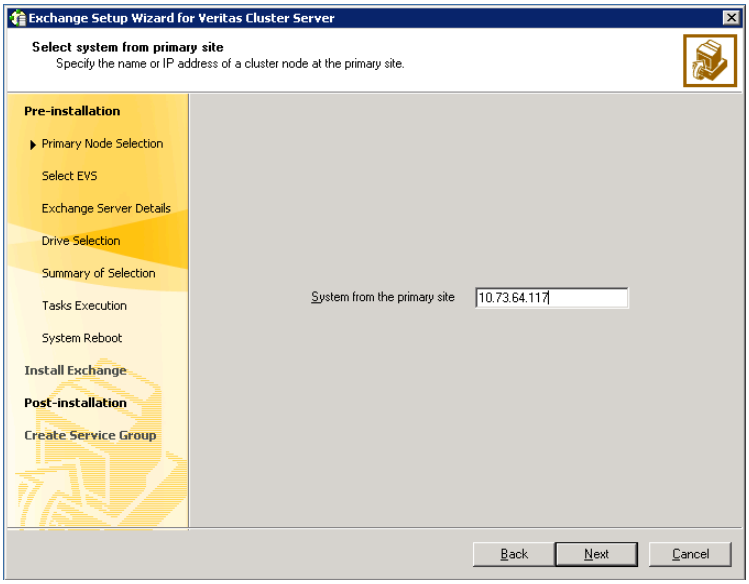

Figure 93) Preinstallation (3).

6. In the Select Exchange Virtual Server pane, select the Exchange virtual server for disaster recovery and click **Next**.
   Note: The installer verifies that the selected node meets the Exchange requirements. If the service group on the primary node has not been taken offline, the installer prompts you to do so without exiting the installer, or you can cancel the installation wizard and take the service group offline manually. When all requirements are validated, click **Next**, enter the name of a failover node, and click **Next.**

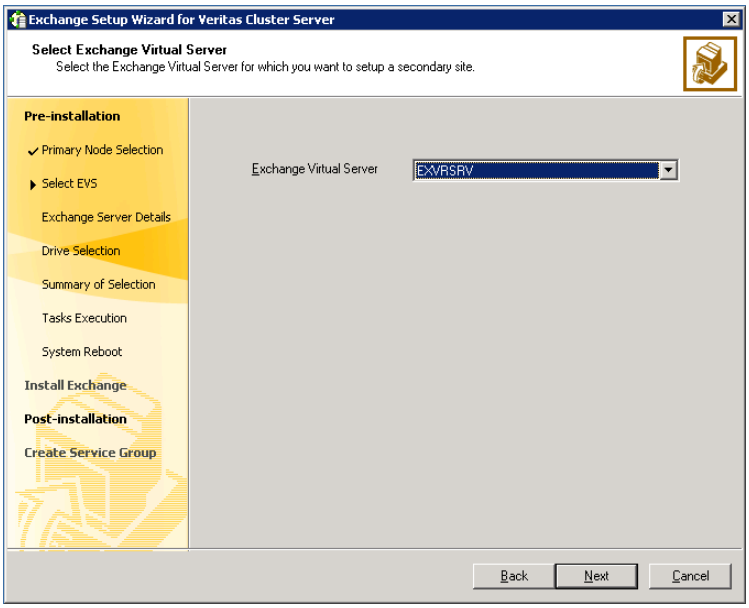

Figure 94) Preinstallation (4).

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

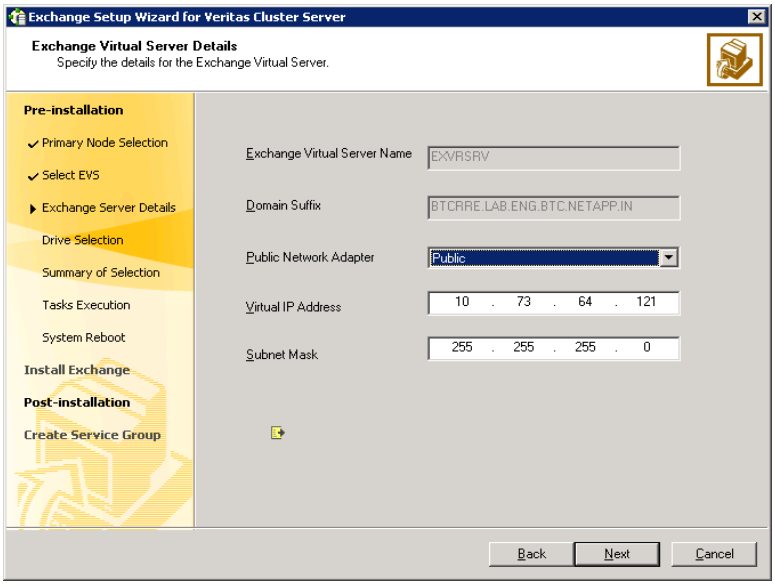

Figure 95) Preinstallation (5).

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

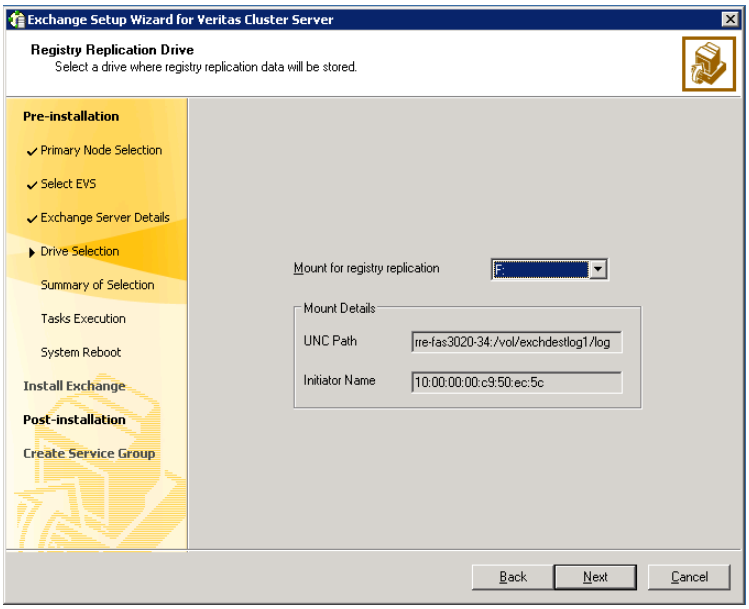

Figure 96) Preinstallation (6).

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

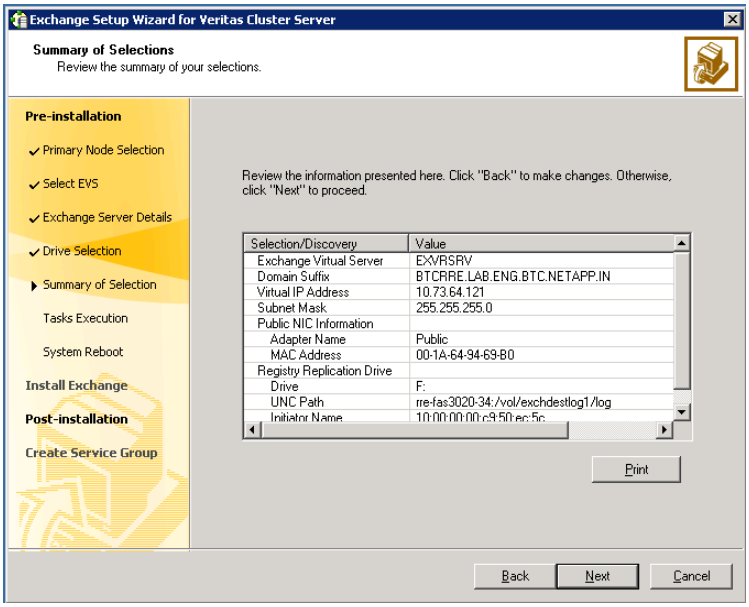

Figure 97) Preinstallation (7).

10. A message appears informing you that the system will be renamed and restarted after you quit the wizard. Click **Yes** to continue.
    If a DNS entry for the specified Exchange Server and IP address does not exist, the wizard will display a message. Click **OK** to let the wizard create the DNS entry. If the wizard is unable to create the entry, click **OK** to continue.

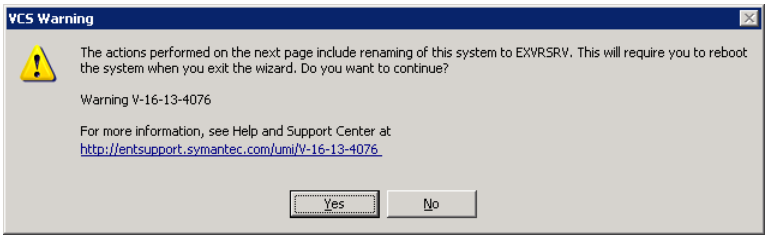

Figure 98) Preinstallation (8).

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

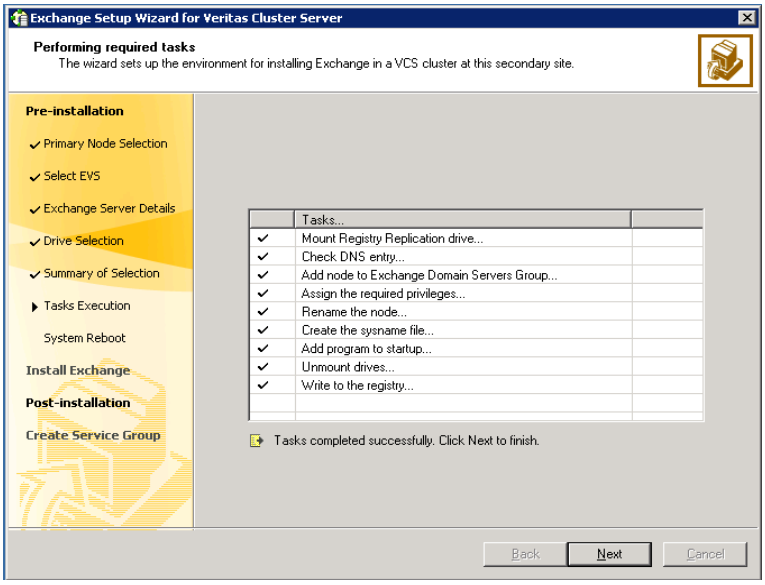

Figure 99) Preinstallation (9).

12. The wizard prompts you to reboot the node. Click **Reboot**.

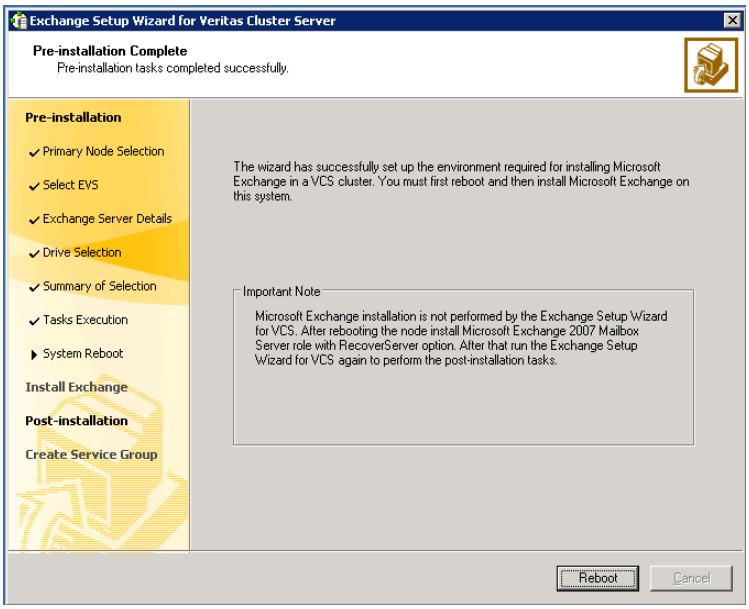

Figure 100) Preinstallation (10).

13. Click **Yes**.

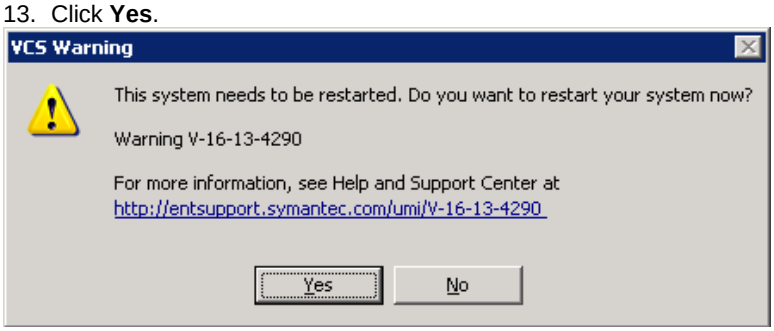

Figure 101) Preinstallation (11).

Note: 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.

Installation Instructions

To install Microsoft Exchange Server 2007 on the first failover node at the secondary (DR) site, perform the procedure described in the section Microsoft Exchange Server Installation on Additional Nodes.

Postinstallation Instructions

To complete the postinstallation of the Microsoft Exchange Server installation, perform the procedures listed in:

- Postinstallation: Exchange Server
- Moving the Exchange Server Databases to Shared

Installing Microsoft Exchange Server on Additional Nodes at Secondary (DR) Site

Install Microsoft Exchange Server on additional nodes in the secondary (DR) site cluster to configure the nodes as failover nodes for the same Exchange virtual server. The reinstallation, Exchange installation, and postinstallation must be completed on each additional node.

For the installation procedure, see the section Microsoft Exchange Server Installation on Additional Nodes.

CONFIGURING THE EXCHANGE SERVICE GROUP AT THE SECONDARY (DR) SITE

For the configuration procedure, see the section Configuration **Instructions**.

CONFIGURING REPLICATION USING NETAPP SNAPMIRROR

You can replicate Exchange data by establishing a SnapMirror relationship between the storage controllers at the primary and secondary sites. Before configuring replication, make sure the service group is offline at the secondary site. SnapMirror replicates point-in-time Snapshot copies created on a storage controller from the primary site and replicates them to the storage controller at the destination site over a wide area network. These Snapshot copies can be used by the target host to provide rapid recovery in case of a disaster.

To configure the asynchronous SnapMirror relationship between source and destination site storage systems:

1. On the destination storage controller console use the options `snapmirror.access` command to specify the hostnames of the storage systems that are allowed to copy data directly from the source storage system. For example: `options snapmirror.access host=<destination_storage>.`
2. Restrict the volumes to allow SnapMirror to access them using the command `vol restrict:`
   `Vol restrict <volume_name>`
3. Turn on SnapMirror using the `snapmirror on` command line on both the source and the destination controllers.
4. To set up SnapMirror update schedules, edit the `/etc/snapmirror.conf` file at the destination storage controller console.

- Edit the `snapmirror.conf` file on the destination storage using `wrfile /etc/snapmirror.conf` and click **Enter**.
- Type `<src_storage>:<vol_name> <dest_storage>:<vol_name> - <Minute> <Hour> <week of the month> <day of the week>.`

  Example: `<NB-6070-1>:<SRC_VOL> <NB-6070-3>:<DEST_VOL> - - - - -`

  Note: The example above has the schedules disabled. SnapMirror updates will be done by SnapManager for Exchange.

5. From the destination storage controller initialize SnapMirror to make a first copy of the source data. For example:
   `Snapmirror initialize -S <src_storage_name>:<src_vol> <dest_storage_name>:<dest_vol>`

   Note: You can use the **`snapmirror status`** command to check the SnapMirror status as shown below:
   `NB-6070-1> snapmirror status`

```
Snapmirror is on

Source                  Destination          State         Lag          Status
NB-6070-1:SRC1   NB-6070-2:DEST1     source        transferring  (276 MB done)
NB-6070-1:SRC2   NB-6070-2:DEST2     source        transferring  (56 MB done)
```

CONFIGURING NETAPP SNAPMIRROR RESOURCES AT THE PRIMARY SITE

Configure NetApp SnapMirror resources at the primary site to monitor data replication from the primary site to the secondary site. You may want to repeat this procedure and create a NetApp SnapMirror resource at the secondary site. This is required in cases in which:

- The service group is online at the secondary site (either it is failed over or switched to the secondary site) and the storage system 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 the SnapMirror resource using the Exchange Server Configuration Wizard:

1. Verify that 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 by clicking **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Exchange Server 2007 Configuration Wizard**.
3. Review the information in the Welcome pane and click **Next**.
4. In the Wizard Options pane, click **Modify service group**, click the service group to be modified, and click **Next**.
5. In the Service Group Configuration pane, verify the list of systems in the service group and click **Next**.
6. In the Exchange Server Configuration pane, 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 pane.
8. In the Completing the Exchange Configuration pane, uncheck the Bring the service group online checkbox and click **Finish**.

LINKING THE CLUSTERS AT THE PRIMARY AND THE SECONDARY (DR) SITES

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

Linking Clusters

Before linking clusters, verify that the virtual IP address for the ClusterAddress attribute for each cluster is set. Use the same IP address as the one assigned to the IP resource in the Remote Cluster Configuration Wizard.

1. Open the Cluster Manager Java console on the source site cluster node on which the service group is active.
2. From Cluster Explorer, click **Edit>Add/delete Remote Cluster** to run the Remote Cluster Configuration Wizard. Review the required information for the Remote Cluster Configuration Wizard and click **Next**.

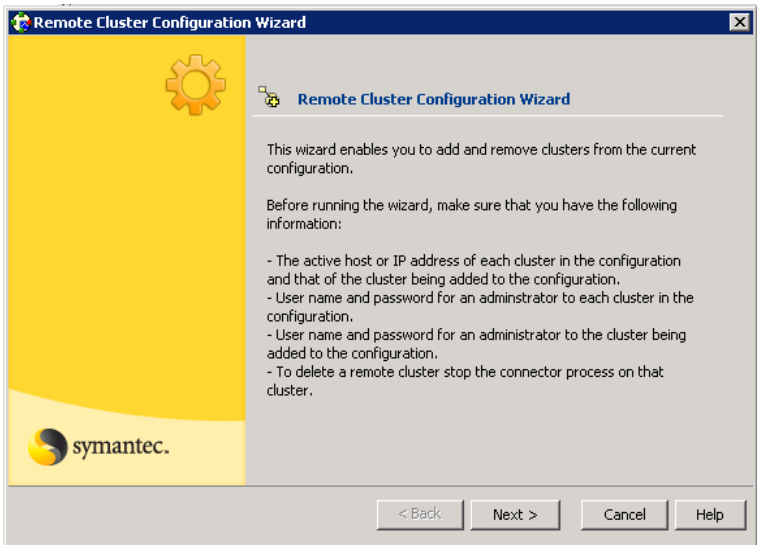

Figure 102) Linking clusters (1).

3. In the Wizard Options dialog box, select **Add Cluster** and click **Next**.

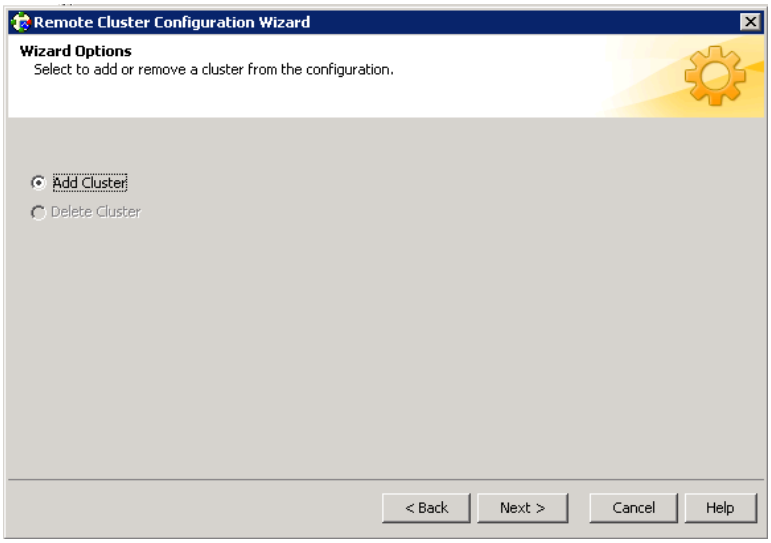

Figure 103) Linking clusters (2).

4. Enter the details of the new cluster and click **Next**.

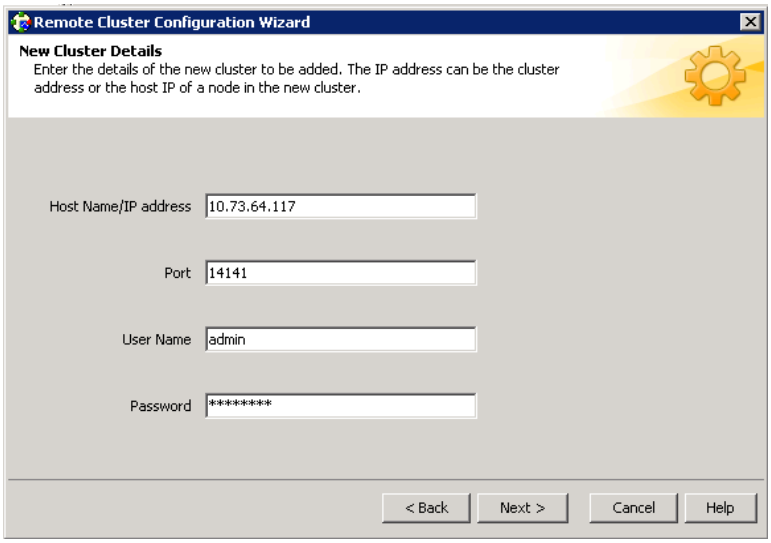

Figure 104) Linking clusters (3).

5. Follow the wizard and finish the process.

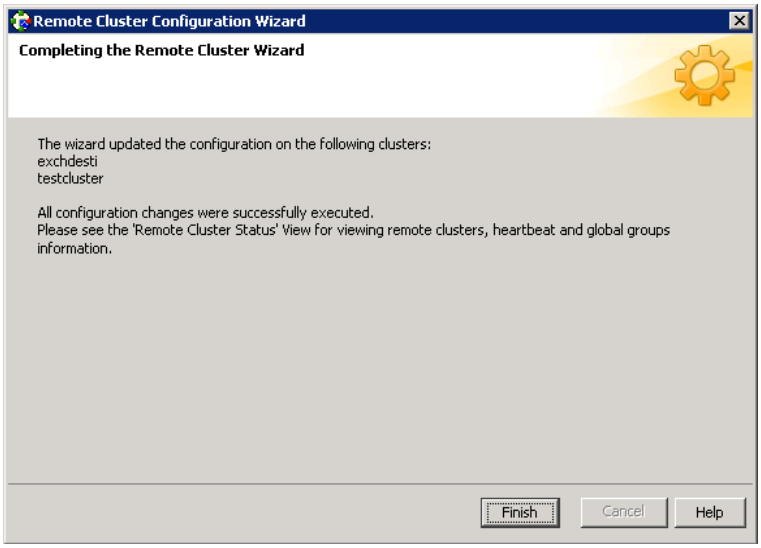

Figure 105) Linking clusters (4).

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.

1. From the Cluster Explorer configuration tree, right-click the service group and click **Configure As Global**.
2. In the Cluster List Details pane:
   a. In the Available Clusters box, select the clusters on which the group can come online. Click the right arrow to move the cluster name to the Clusters for Service Group box; for global to local cluster conversion, click the left arrow to move the cluster name back to the Available Clusters box. A priority number (starting with 0) indicates the cluster on which the group will attempt to come online. If necessary, double-click the entry in the Priority column to enter a new value.
   b. Select the policy for cluster failover:
   - **Manual** prevents a group from automatically failing over to another cluster.
   - **Auto** enables a group to automatically fail over to another cluster if it is unable to fail over within the cluster, or if the entire cluster faults.
   - **Connected** enables a group to automatically fail over to another cluster if it is unable to fail over within the cluster.
3. Click **Next** to continue.

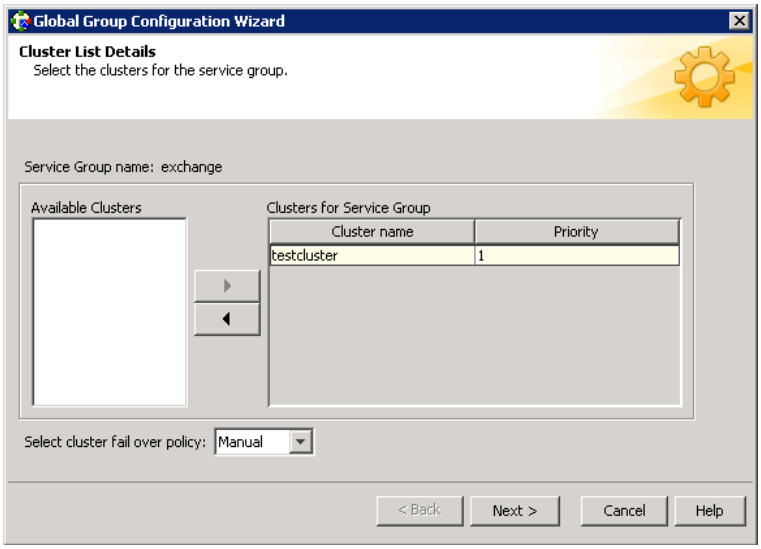

Figure 106) Cluster list details.

4. Enter or review the connection details for each cluster:
   Click the **Configure** icon to review the remote cluster information for each cluster.
   a. Enter the IP address of the remote cluster, the IP address of a cluster system, or the host name of a cluster system.
   b. Verify the port number.
   c. Enter the user name and password and click **OK.**
   Click **Next** to continue.

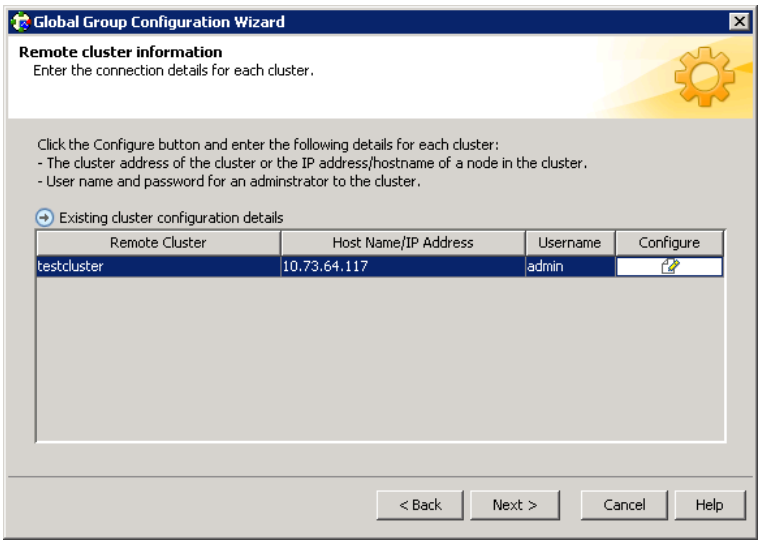

Figure 107) Remote cluster information.

5. Click **Finish**.

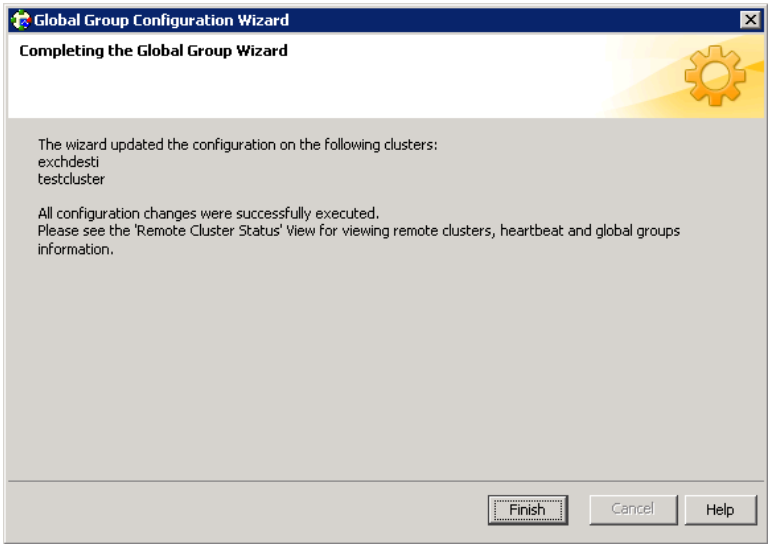

Figure 108) Global wizard completion.

SET VCS SERVICE TIMEOUT

Follow the procedure given in Appendix C to set VCS service timeouts.

8.7 MANAGING FAILOVER IN A DISASTER RECOVERY ENVIRONMENT

In a disaster recovery configuration, the Veritas Cluster Server 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, Veritas Cluster Server 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.

8.7.1 Managing Successful Remote Failover

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

1. Right-click and select **Freeze** to freeze the Exchange service group at the remote site.
2. Reconfigure NetApp SnapManager for Exchange to detect the changes in the snapinfo directory.
3. Restore Exchange data from the latest valid database Snapshot copy using the NetApp SnapManager Restore Wizard as follows.
    i. Open the SnapManager application.
    ii. Make sure that all Explorer windows are closed on the Exchange Server running SnapManager.
    iii. Disable any SnapManager operations that are scheduled to run against the Exchange data you are restoring, including any jobs scheduled on remote management or remote verification servers.
    iv. Click **Exchange Server** node in the Scope pane.
    v. From the SnapManager Actions pane, select the SnapManager Restore Wizard.
    vi. Follow the instructions in the Restore Wizard and go to the “Restore Status” window.
    vii. Click **Start Now** to start the restore process.
    viii. After the restore process is complete, click **OK**.
    ix. You can optionally perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.

4. Right-click and select **Unfreeze** to unfreeze the Exchange service group.

8.7.2 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.

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 copy using the NetApp SnapManager Restore utility.
7. Unfreeze the Exchange service group.

8.7.3 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, Veritas Cluster Server 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 NetApp SnapManager.
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. Check the SnapMirror status of storages at the primary and DR site using snapmirror status.
2. Verify `/etc/snapmirror.conf` entries on both primary and DR storages.
3. Check the cluster status on the primary site servers. If SnapDrive and SnapMirror resources are online, bring them offline in the same order.
4. Typically `/etc/snapmirror.conf` becomes empty as a result of a primary site disaster.
5. DR site storage should have appropriate `/etc/snapmirror.conf` entries for the `fbsync` command to work as expected.
6. If the `/etc/snapmirror.conf` entry does not exist on the DR site storage, create or add it as it was present before the disaster occurred (original primary to DR replication entries).
7. Synchronize the Exchange data at both sites by running the `fbsync` action at the site and host 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.

   This command will resync the SnapMirror relation from the DR site to the primary site and modify the entries in `/etc/snapmirror.conf`.

8. Run the action for each SnapMirror resource.
   Now the replication will be from the DR site to the primary site. Verify this with the `snapmirror status` command.
9. Back up the Exchange data using NetApp SnapManager and update the snapmirror. See the NetApp documentation for instructions.
10. 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.**

9 GENERAL TROUBLESHOOTING

Use Windows Event Viewer to check events related to Veritas and HBA/Software iSCSI initiators. Below are useful commands to check the status/logs of different components of the cluster.

9.1 NETAPP STORAGE

Use the following commands on the storage console to check LUN/Volume availability and mapping information:

- `lun show`
- `lun show –m`
- `vol status`

Initiator group details and initiator log-in information may be viewed using the following command:

- `igroup show`

Make sure zoning is done properly. If the LUN is not available at the host or the initiator is not logged in in case of FC SAN, use the `ping` command to check connectivity.

9.2 SOFTWARE ISCSI INITIATORS

The MS iSCSI Initiator Service and the MS iSCSI Initiator kernel mode driver both log errors, warnings, and informational messages to the system eventlog. If a problem occurs, consult the eventlog first.

Use `C:\Program Files\NetApp\iSCSI Host Utilities>msiscsi_info.exe` to view details about Microsoft software iscsi initiators.

9.3 NETAPP SNAPDRIVE

The SnapDrive debug log is available at `C:\Program Files\NetApp\SnapDrive\Snpdrvdbg.log`.

9.4 NETAPP SNAPMANAGER FOR EXCHANGE

Reports are available at `C:\Program Files\NetApp\SnapManager for Exchange\Report directory`.

9.5 NETAPP SNAPMIRROR

The following commands may be used to collect information and to troubleshoot SnapMirror issues:

- `snapmirror status`
- `snapmirror status –l`
- `snapmirror release`
- `snapmirror break`
- `snap delete`
- `snapmirror resync`

9.6 VCS FOR NETAPP

All VCS for NetApp agents create log files in `C:\Program Files\Veritas\cluster server\log\`. Carefully go through the log file of the failed agent to find out the reason for the failure.

9.7 NETAPP SNAPMIRROR RELATIONSHIP CLEANUP

Use the following procedure to fail back an Exchange resource group if the command `fbsync` specified in **"Failover in Response to a Disaster"** does not work. This procedure can also be used if there are stale SnapMirror relationships between the primary and DR site.

1. Verify status on primary site storage.

```
PRIMARY-STORAGE> snapmirror status

Snapmirror is on.

Source                   Destination              State          Lag        Status

PRIMARY-STORAGE:exchgdb   DR-STORAGE:exchgdb   Source         00:35:58   Idle

PRIMARY-STORAGE:exchglog  DR-STORAGE:exchglog  Source         00:36:07   Idle

PRIMARY-STORAGE> rdfile /etc/snapmirror.conf

#Regenerated by registry Mon Mar 16 15:22:42 GMT 2009

PRIMARY-STORAGE> lun show -m

LUN path                            Mapped to          LUN ID  Protocol

-------------------------------------------------------------------------

/vol/exchgdb/exchgdb                viaRPC.iqn.1991-05.com.microsoft:rre-x3550-
61.btcrre.lab.eng.btc.netapp.in        1     iSCSI

/vol/exchglog/exchglog              viaRPC.iqn.1991-05.com.microsoft:rre-x3550-
61.btcrre.lab.eng.btc.netapp.in        0     iSCSI
```

2. Verify status on DR site storage.

```
DR-STORAGE> snapmirror status

Snapmirror is on.

Source                   Destination              State          Lag        Status

PRIMARY-STORAGE:exchgdb   DR-STORAGE:exchgdb   Broken-off     00:36:11   Idle

PRIMARY-STORAGE:exchglog  DR-STORAGE:exchglog  Broken-off     00:36:20   Idle

DR-STORAGE> rdfile /etc/snapmirror.conf

#Regenerated by registry Mon Mar 16 15:40:15 GMT 2009

DR-STORAGE> lun show -m

LUN path                            Mapped to          LUN ID  Protocol

-------------------------------------------------------------------------

/vol/exchgdb/exchgdb                viaRPC.iqn.1991-05.com.microsoft:rre-x3550-
71.btcrre.lab.eng.btc.netapp.in        1     iSCSI

/vol/exchglog/exchglog              viaRPC.iqn.1991-05.com.microsoft:rre-x3550-
71.btcrre.lab.eng.btc.netapp.in        0     iSCSI
```

3. Verify Exchange service group on primary and DR site servers.

   A. Now All services will be online on DR site server.
   B. Snapmirror and snapdrive services may be online on Primary site server.

4. Manual steps to fail back Exchange service group to primary site:

   a) Offline SnapDrive and SnapMirror services on primary site server if they are online.

   b) Manually release stale SnapMirror relationships from primary site storage.

```
PRIMARY-STORAGE> snapmirror status

Snapmirror is on.
```

```
Source                    Destination               State          Lag        Status
PRIMARY-STORAGE:exchgdb   DR-STORAGE:exchgdb   Source         00:41:25   Idle
PRIMARY-STORAGE:exchglog  DR-STORAGE:exchglog  Source         00:41:34   Idle
PRIMARY-STORAGE> snapmirror release exchgdb   DR-STORAGE:exchgdb
PRIMARY-STORAGE> snapmirror release exchglog   DR-STORAGE:exchglog
```

c) Check SnapMirror status on primary site storage.

```
PRIMARY-STORAGE> snapmirror status
Snapmirror is on.
PRIMARY-STORAGE>
```

d) Check SnapMirror status on DR site storage.

```
DR-STORAGE> snapmirror status
Snapmirror is on.
Source                    Destination               State          Lag        Status
PRIMARY-STORAGE:exchgdb   DR-STORAGE:exchgdb   Broken-off     00:42:07   Idle
PRIMARY-STORAGE:exchglog  DR-STORAGE:exchglog  Broken-off     00:42:16   Idle
```

e) Delete the stale Snapshot copies for the broken-off SnapMirror relationship on the DR site storage.

```
 DR-STORAGE> snapmirror status -l
Snapmirror is on.

Source:                 PRIMARY-STORAGE:exchgdb
Destination:            DR-STORAGE:exchgdb
Status:                 Idle
Progress:               -
State:                  Broken-off
Lag:                    00:42:14
Mirror Timestamp:       Mon Mar 16 20:52:44 IST 2009
Base Snapshot:          DR-STORAGE(0118059145)_exchgdb.1
Current Transfer Type:  -
Current Transfer Error: -
Contents:               Replica
Last Transfer Type:     Resync
Last Transfer Size:     624 KB
Last Transfer Duration: 00:00:03
Last Transfer From:     PRIMARY-STORAGE:exchgdb

Source:                 PRIMARY-STORAGE:exchglog
Destination:            DR-STORAGE:exchglog
Status:                 Idle
Progress:               -
State:                  Broken-off
Lag:                    00:42:23
Mirror Timestamp:       Mon Mar 16 20:52:35 IST 2009
```

```
Base Snapshot:          DR-STORAGE(0118059145)_exchglog.1

Current Transfer Type:  -

Current Transfer Error: -

Contents:               Replica

Last Transfer Type:     Resync

Last Transfer Size:     1820 KB

Last Transfer Duration: 00:00:01

Last Transfer From:     PRIMARY-STORAGE:exchglog

DR-STORAGE> snap delete -V exchgdb DR-STORAGE(0118059145)_exchgdb.1

Mon Mar 16 21:35:13 IST [DR-STORAGE: wafl.snap.delete:info]: Snapshot copy DR-
STORAGE(0118059145)_exchgdb.1 on volume exchgdb NetApp was deleted by the Data ONTAP
function snapcmd_delete. The unique ID for this Snapshot copy is (88, 10523).

DR-STORAGE> snap delete -V exchglog DR-STORAGE(0118059145)_exchglog.1

Mon Mar 16 21:35:24 IST [DR-STORAGE: wafl.snap.delete:info]: Snapshot copy DR-
STORAGE(0118059145)_exchglog.1 on volume exchglog NetApp was deleted by the Data ONTAP
function snapcmd_delete. The unique ID for this Snapshot copy is (100, 5091).
```

f) Status on DR site storage.

```
DR-STORAGE> snapmirror status

Snapmirror is on.

DR-STORAGE>
```

g) Add `/etc/snapmirror.conf` entries on primary site storage.

```
PRIMARY-STORAGE> wrfile /etc/snapmirror.conf

DR-STORAGE:exchgdb   PRIMARY-STORAGE:exchgdb - - - - -

DR-STORAGE:exchglog  PRIMARY-STORAGE:exchglog - - - - -

read: error reading standard input: Interrupted system call
```

h) Status after adding `/etc/snapmirror.conf` entries.

```
PRIMARY-STORAGE> rdfile /etc/snapmirror.conf

DR-STORAGE:exchgdb   PRIMARY-STORAGE:exchgdb - - - - -

DR-STORAGE:exchglog  PRIMARY-STORAGE:exchglog - - - - -

PRIMARY-STORAGE>
```

i) Resyncing SnapMirror at primary site storage.

```
PRIMARY-STORAGE> snapmirror resync -S DR-STORAGE:exchgdb PRIMARY-STORAGE:exchgdb

The resync base snapshot will be: PRIMARY-STORAGE(0118058343)_exchgdb.2

Are you sure you want to resync the volume? y

Mon Mar 16 21:36:29 IST [PRIMARY-STORAGE: snapmirror.dst.resync.info:notice]:
SnapMirror resync of exchgdb to DR-STORAGE:exchgdb is using PRIMARY-
STORAGE(0118058343)_exchgdb.2 as the base snapshot.

Volume exchgdb will be briefly unavailable before coming back online.

Share exchdb disabled while volume exchgdb is offline.

Mon Mar 16 21:36:30 IST [PRIMARY-STORAGE: wafl.snaprestore.revert:notice]: Reverting
volume exchgdb to a previous snapshot.

Share exchdb activated.

Mon Mar 16 21:36:30 IST [PRIMARY-STORAGE: cifs.shares.activated:info]: Activated 1 CIFS
share on the volume exchgdb.

exportfs [Line 5]: NFS not licensed; local volume /vol/exchgdb not exported
```

```
Revert to resync base snapshot was successful.

Mon Mar 16 21:36:30 IST [PRIMARY-STORAGE: replication.dst.resync.success:notice]:
SnapMirror resync of exchgdb to DR-STORAGE:exchgdb was successful.

Transfer started.

Monitor progress with 'snapmirror status' or the snapmirror log.

PRIMARY-STORAGE> snapmirror resync -S DR-STORAGE:exchglog PRIMARY-STORAGE:exchglog

The resync base snapshot will be: PRIMARY-STORAGE(0118058343)_exchglog.2

Are you sure you want to resync the volume? y

Mon Mar 16 21:36:42 IST [PRIMARY-STORAGE: snapmirror.dst.resync.info:notice]:
SnapMirror resync of exchglog to DR-STORAGE:exchglog is using PRIMARY-
STORAGE(0118058343)_exchglog.2 as the base snapshot.

Volume exchglog will be briefly unavailable before coming back online.

Share exchglog disabled while volume exchglog is offline.

Mon Mar 16 21:36:43 IST [PRIMARY-STORAGE: wafl.snaprestore.revert:notice]: Reverting
volume exchglog to a previous snapshot.

Share exchglog activated.

Mon Mar 16 21:36:43 IST [PRIMARY-STORAGE: cifs.shares.activated:info]: Activated 1 CIFS
share on the volume exchglog.

exportfs [Line 6]: NFS not licensed; local volume /vol/exchglog not exported

Revert to resync base snapshot was successful.

Mon Mar 16 21:36:43 IST [PRIMARY-STORAGE: replication.dst.resync.success:notice]:
SnapMirror resync of exchglog to DR-STORAGE:exchglog was successful.

Transfer started.

Monitor progress with 'snapmirror status' or the snapmirror log.
```

j) Check SnapMirror status on primary and DR storage.

```
PRIMARY-STORAGE> snapmirror status
Snapmirror is on.

Source                  Destination             State          Lag        Status

DR-STORAGE:exchgdb   PRIMARY-STORAGE:exchgdb   Snapmirrored   00:00:36   Idle

DR-STORAGE:exchglog  PRIMARY-STORAGE:exchglog  Snapmirrored   00:00:22   Idle

PRIMARY-STORAGE>

DR-STORAGE> snapmirror status

Snapmirror is on.

Source                  Destination             State          Lag        Status

DR-STORAGE:exchgdb   PRIMARY-STORAGE:exchgdb   Source         00:00:47   Idle

DR-STORAGE:exchglog  PRIMARY-STORAGE:exchglog  Source         00:00:33   Idle

DR-STORAGE>
```

k) Fail back Exchange storage group to primary site.

On the DR site, in the cluster administrator, right-click on the Exchange service group and select **Switch to > Remote switch >Select cluster and System > select OK > YES.**

l) Verify that the SnapMirror relationship has been reversed and is in the ideal state.

10 SUMMARY

Every business and organization can experience a serious incident that can prevent it from continuing normal operations or can cause it to lose important data. This can happen on any day at any time. The potential causes are many and varied: flood, explosion, computer malfunction, accident, and so on—the list is endless.

Microsoft Exchange is one of the most mission-critical applications in today's business environments. Service availability is crucial when business needs are very high in enterprises of any size. NetApp has solutions that work in conjunction with the Symantec global cluster application to meet such business needs.

The integrated solution uses NetApp SnapDrive, SnapManager, and SnapMirror applications and Veritas Cluster Server for NetApp SnapMirror (with GCO) from Symantec. The combined solution provides a robust platform to implement Exchange in a highly available disaster recovery environment. NetApp SnapMirror helps Exchange data replication across sites, and Veritas Cluster Server from Symantec helps local and remote cluster failovers as needed.

This guide is written for experienced users who plan and implement Veritas Cluster Server for NetApp SnapMirror solutions. It is intended for use as a one-stop reference; however, an advanced user may need to refer to additional documents related to each product used in this solution.

11 REFERENCES

- "Microsoft Exchange 2007 Disaster Recovery Model Using NetApp Solutions" www.netapp.com/library/tr/3584.pdf
- "Microsoft Exchange Server 2007 Best Practices Guide" www.netapp.com/library/tr/3578.pdf
- "Protecting Exchange Server 2007 with NetApp SnapManager for Exchange" www.netapp.com/library/tr/3598.pdf
- "SnapDrive 5.0 Installation and Administration Guide" http://now.netapp.com/NOW/knowledge/docs/snapdrive/relsnap50/html/index.shtml
- "SnapManager 4.0 for Microsoft Exchange Documentation" http://now.netapp.com/NOW/knowledge/docs/SnapManager/relsme40/html/index.shtml
- "Veritas Cluster Server for NetApp SnapMirror" www.symantec.com/business/support/documentation.jsp?pid=51064

APPENDIX A: PREREQUISITES FOR INSTALLING MICROSOFT EXCHANGE SERVER

- Verify that Veritas Cluster Server for NetApp SnapMirror is installed on the nodes.
- Verify that you have configured a Veritas Cluster Server cluster using the Veritas Cluster Server Configuration Wizard.
- Verify that 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.
- Veritas Cluster Server 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.
- Veritas Cluster Server 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.
- If using iSCSI, verify that the Microsoft iSCSI Initiator is configured to establish a persistent connection between the NetApp storage system and the cluster nodes. See the Microsoft documentation for instructions.
- If using FC, verify that you install the NetApp FCP Attach Kit or Windows Host Utilities on all the cluster nodes. Refer to the NetApp documentation for more information.
- Symantec recommends that you have a minimum of two LUNs (or virtual disks), one each for the following:
    1. Exchange database
    2. Transaction logs for the first storage group and registry replication information

APPENDIX B: SUPPORTED SOFTWARE VERSIONS

- Data ONTAP 7.3.1
- Microsoft Software iSCSI Initiator 2.05 and 2.07
- NetApp SnapManager for Exchange 4.0 and 5.0
- NetApp SnapDrive for Windows 6.0.1
- Windows 2003 Enterprise Edition SP2
- Windows 2003 R2 Enterprise Edition SP2
- Microsoft Exchange 2007 SP1
- NetApp Host Utilities for Windows version 4.1 for iSCSI and 4.0.1 for FC
- NetApp Data ONTAP DSM 3.2R1 (in case of multipath)
- FC HBA driver as supported in IMT
- FC switch OS as supported in IMT

APPENDIX C: VCS SERVICE TIMEOUT SETTINGS

The following settings must be in place for NetApp storage and NetApp SnapDrive resources to avoid site failover during storage controller takeover/giveback.

`Monitor interval 60`

`TolerenceLimit  1`

Follow the procedure given below to set these values.

Open Cluster Manager (Java console): Select NetAppFiler resource on the left pane. Select properties from the right pane. Click on the **Edit** icon on the right side of the parameters (Monitor Interval and TolerenceLimit) to set the values.

Follow the same procedure to set these values for NetApp SnapDrive.

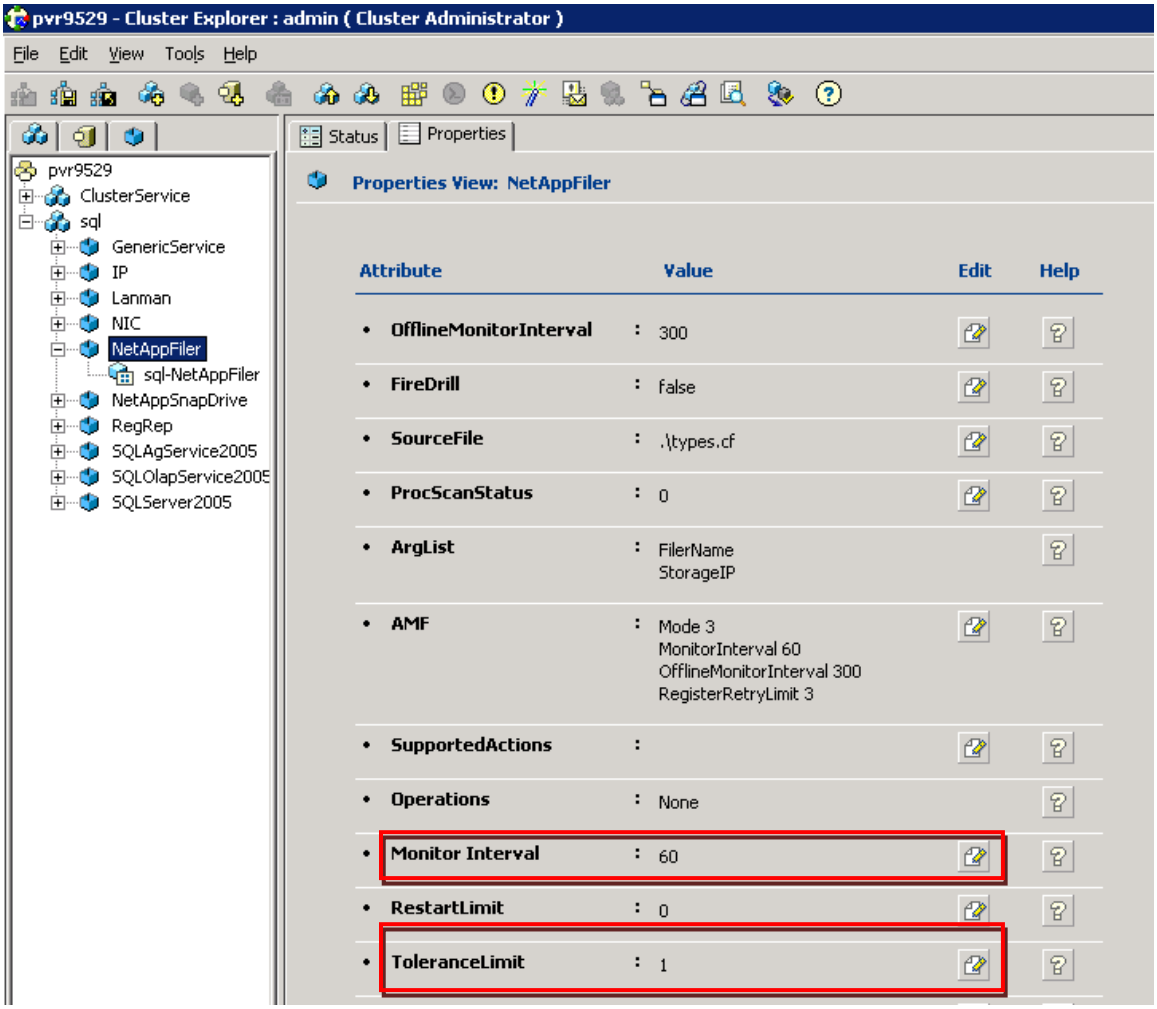

Figure 109) VCS timeout settings.

APPENDIX D: RESOURCE DEPENDENCY GRAPH

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

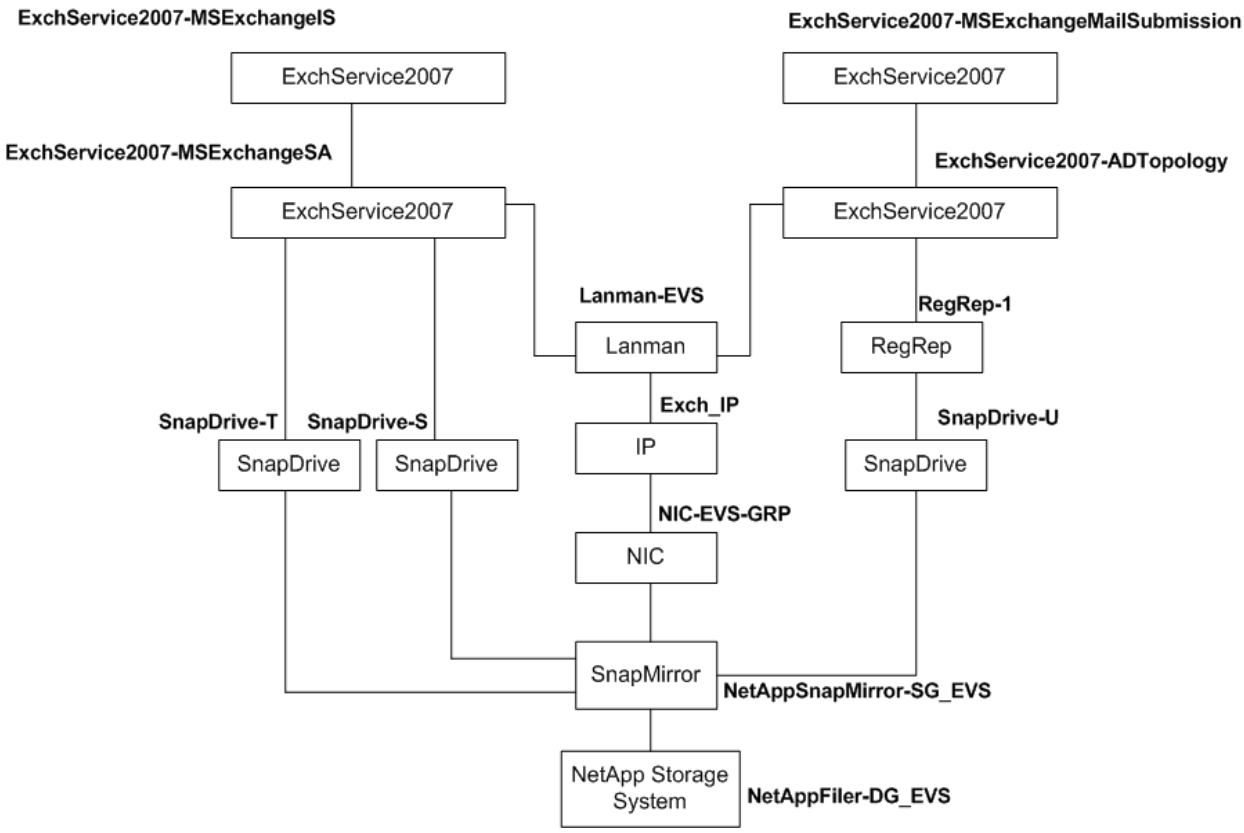

Figure 110) Resource dependency graph.

NetApp provides no representations or warranties regarding the accuracy, reliability or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

www.netapp.com