Veritas™ Cluster Server Implementation Guide for Oracle with NetApp SnapMirror

Windows 2000, Windows Server 2003

5.0 Release Update 1

symantec.

Veritas Cluster Server Implementation Guide for Oracle with NetApp SnapMirror

Third-party legal notices

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

Windows is a registered trademark of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation.

Licensing and registration

Veritas Cluster Server is a licensed product. See the *Storage Foundation and High Availability Solutions for Windows, Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit http://entsupport.symantec.com and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Index

Introduction

The Veritas Cluster Server (VCS) agent for Oracle provides high availability to Oracle in a VCS environment. The VCS agent for Network Appliance (NetApp) SnapMirror enables configuring NetApp filers in a VCS environment. Both the agents work together to provide high availability for Oracle, in environments that use Network Appliance filers for shared storage.

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

Figure 1-1   Typical VCS configuration in a NetApp storage environment
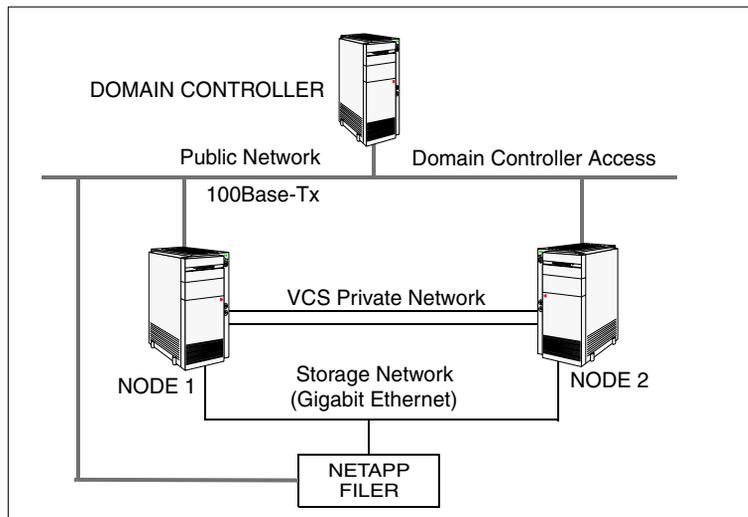
This chapter provides an overview of the agents. For more information about the agents, including their resource type definitions and attribute definitions, see Appendix A, "Resource type definitions" on page 93.

About the VCS agent for Oracle

The VCS for NetApp SnapMirror Database agent for Oracle monitors the Oracle database and listener services, brings them online, and takes them offline.

The package contains two VCS agents:

- The Oracle agent, which monitors the Oracle database services.

- The Netlsnr agent, which monitors the listener services.

Both agents work together to provide high availability for Oracle.

Oracle agent

The Oracle agent monitors the database processes. The agent brings the Oracle database services online, monitors their status, and takes them offline. Specific agent operations include:

- Online—Starts the Oracle service.

- Offline—Stops the Oracle service. The operation also stops all the services that are dependent on the Oracle service.

- Monitor—Verifies the status of Oracle services. The agent provides two levels of application monitoring: basic and detail.

    - Basic monitoring: The agent queries the Service Control Manager (SCM) to verify that Oracle services are continuously active.

    - Detail monitoring: The agent runs a SQL script to verify the status of the database. Detail monitoring is optional. It updates a temporary table in the Oracle database to verify the availability of the database instance. See "Configuring detail monitoring" on page 79 for instructions on configuring detail monitoring for an Oracle database.

- Clean—Forcibly stops the Oracle database.

- Info—Provides static and dynamic information about the state of the database. See "Info entry point" on page 11 for more information.

- Action—Performs predefined actions on a resource. See "Action entry point" on page 12 for more information.

NetIsnr agent

The Netlsnr agent monitors the listener process. The agent controls the listener for the database. The listener is a server process that listens to incoming client connection requests and manages traffic to the database.

The Netlsnr agent brings the listener services online, monitors their status, and takes them offline. Specific agent operations include:

■ Online—Starts the listener service.

■ Offline—Stops the listener service.

■ Monitor—Queries the SCM for the status of the listener service.

■ Clean—Forcibly stops the listener service.

Info entry point

The Info entry point provides static and dynamic information about the state of the database.

The entry point retrieves the following static information:

Version	InstanceNo	InstanceName
HostName	StartupTime	Parallel
Thread	InstanceRole	

The entry point retrieves the following dynamic information:

InstanceStatus	Logins	DatabaseStatus
ShutdownPending		

You can add additional attributes by adding `sql` statements to the file `%VCS_HOME%\bin\Oracle\scripts\info\db_info.sql`. For example:

```
select 'static:HostName:'||host_name from v$instance;
select 'dynamic:ShutdownPending:'||shutdown_pending from
v$instance;
```

The format of the selected record must be as follows:

`attribute_type:userkey_name:userkey_value`

The variable `attribute_type` can take the value `static` and/or `dynamic`.

Action entry point

The Action entry point enables you to perform predefined actions on a resource.

To perform an action on a resource, type the following command:

```
C:\> hares -action <res> <token> [-actionargs <arg1> ...] [-sys
<system>] [-clus <cluster>]
```

Table 1-1 includes the actions that the agent supports.

Table 1-1   Actions supported by Oracle agent

Token for Action	Description
VRTS_GetInstanceName	Retrieves the name of the configured instance.
VRTS_GetRunningServices	Retrieves the list of processes monitored by the agent.
DBRestrict	Changes the database session to enable the RESTRICTED mode.
DBUndoRestrict	Changes the database session to disable the RESTRICTED mode.
DBSuspend	Suspends a database.
DBResume	Resumes a suspended database.
DBTbspBackup	Backs up a tablespace; actionargs contains name of the tablespace to be backed up.

You can also add custom actions for the agent. For further information, refer to the *Veritas Cluster Server Agent Developer's Guide*.

About VCS hardware replication agents for Network Appliance

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

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

■   NetAppFiler agent—Monitors the state of the filer.

■   NetAppSnapDrive agent—Connects and disconnects virtual disks (LUNs) using the iSCSI or the FC protocol.

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

NetApp Filer agent

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

Agent operation

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

NetApp SnapDrive agent

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

Agent operations

- Online—Connects a virtual disk (LUN) using an iSCSI or FC Initiator. The agent presents the LUN as a locally-attached drive to the host. The agent also removes LUN-host mappings made before the online operation.

- Offline—Disconnects the virtual disk (LUN) from the host.

- Monitor—Verifies that the specified virtual disk (LUN) is connected to the host.

- Open—Verifies that there is connectivitiy to the filer. It also checks that the VCS Helper service is running with the same privileges as the SnapDrive service.

- Clean—Attempts to forcibly disconnect a virtual disk (LUN).

NetApp SnapMirror agent

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

Agent operations

- Online—If the state of the local filer device is SOURCE, the agent creates a lock file to indicate that the resource can come online. This effectively makes the devices writable for the application.

  If the state of the local filer is SNAPMIRRORED, the agent attempts to reverse the direction of replication by changing the state of the local filer to SOURCE and that of the original source to SNAPMIRRORED.

  If the original source filer is down, the agent performs a mirror breakoff to enable local write access, if the filer is not already broken off.

  If the original source returns to life, you must re-synchronize the data manually. The Online entry point touches a lock file if Read Write access is enabled successfully.

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

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

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

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

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

How the agent makes Oracle highly available

In the basic monitoring mode, the database agent for Oracle detects a failure if the database or a listener service is not running. In the detail monitoring mode, the agent detects failure if a preconfigured SQL script cannot execute or access the database or if the listener service is not running.

When the agent detects a failure, the Oracle service group switches to the next available system listed in the service group's SystemList attribute. VCS starts

the configured Oracle and listener services on the new system, thus ensuring high availability for the Oracle services and data.

Typical Oracle configuration in a VCS cluster

In a typical configuration, VCS is configured in a two-node cluster (System 1 and System 2). Oracle is installed on both systems, and the data to be used by Oracle is installed on shared storage. The VCS for NetApp SnapMirror Database agent for Oracle is installed on both systems.

Figure 1-2   Typical Oracle configuration in a VCS cluster
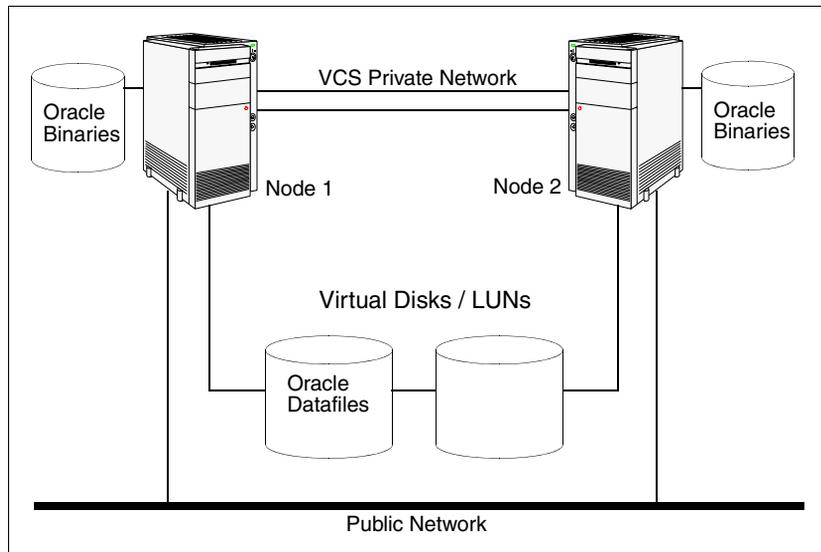
Installing VCS for Network Appliance SnapMirror

This chapter presents key considerations for software installation and describes how to install Veritas Cluster Server for Network Appliance SnapMirror.

Licensing

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

Evaluation license key

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

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

Virtual Server license policy

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

License management

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

Symantec License Inventory Manager

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

Prerequisites

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

Supported software

- Veritas Cluster Server 5.0 Release Update for NetApp SnapMirror with the VCS database agent for Oracle
- Oracle 10g, Release 1 (10.1.0.2) Standard Edition or Enterprise Edition
  or
  Oracle 10g, Release 2 (10.2.0.1.0) Standard Edition or Enterprise Edition
  with
  Windows 2000 Server, Advanced Server, or Datacenter Server (all required Service Pack 4 with Update Rollup 1)
  or
  Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) (SP1 required, SP2 supported but not required for all editions)

Note: Support for Oracle is limited to 32-bit versions of the operating system.

- Network Appliance Data ONTAP 7.2
- Network Appliance SnapDrive 4.1, 4.2, and 5.0
- NetApp FCP Attach Kit 3.0, Windows Host Utilities 3.0
- Microsoft iSCSI software Initiator 2.02 and 2.05

Software requirements

- The following software must be installed on each node:
  - Microsoft iSCSI Initiator

- Network Appliance SnapDrive
  When installing SnapDrive, you must specify a user account in the SnapDrive Service Credentials dialog box. The user account must be a domain user and part of the Administrators group of the local system and the filer.
- If you plan to use Fibre Channel (FC) for connecting the LUNs, ensure that you install the NetApp FCP Attach Kit or Windows Host Utilities on all the cluster nodes. Refer to NetApp documentation for more details.

- You must have licenses for Network Appliance SnapMirror and SnapRestore (for Disaster Recovery configurations).

Configuration requirements

- Make sure the filers reside in the same domain as the systems.

- Make sure the filers can replicate in both directions.

- Make sure that the filers are accessible on the network; ensure that you can ping the filers using the DNS name.

- If you plan to set up a disaster recovery configuration, make sure the volumes at both sites are of the same size.

- Set up a private network for the shared storage. Assign an IP address to each adapter in the private network.

- Configure the Common Internet File System (CIFS) shares for each volume. See the Network Appliance documentation for instructions.

- If you plan to use Fibre Channel (FC) for connecting the LUNs, type hba_info on the command prompt, and verify that the FC initiators are displayed.
  If FC initiators are not displayed, install the mini port driver provided by your vendor and run the command again to verify that the FC initiators are displayed.

- Ensure that the LUNs are mounted. In case of MPIO, ensure that the LUNs are mounted using the required initiators.

Note: MPIO support is available only with FC.

System requirements

- Shared virtual disks to support applications that migrate between nodes in the cluster. Disaster Recovery configuration requires one array for each site.

■ SCSI, Fibre Channel Host Bus Adapters (HBA), or iSCSI Initiator supported
NICs to access shared storage.

■ Two NICs: one shared public and private, and one exclusively for the private
network; Symantec recommends three NICs, see "Best practices" on page 21
for more information

■ 1 GB of RAM for each system

■ All servers running the same operating system, service pack level, and
system architecture.

Network requirements

■ Install VCS for NetApp on servers in a Windows 2000 Server or Windows
Server 2003 domain.

■ Disable the Windows Firewall on systems running Windows Server 2003
SP1 or SP2.

■ Static IP addresses for the following purposes:

   ■ One IP address for each physical node in the cluster

   ■ One IP address for each cluster

   ■ One IP address for each virtual server

■ Configure name resolution for each node

■ Verify the availability of DNS Services. AD-integrated DNS or BIND 8.2 or
higher are supported.
Make sure a reverse lookup zone exists in the DNS. Refer to the application
documentation for instructions on creating a reverse lookup zone.

■ DNS scavenging affects virtual servers configured in VCS because the
Lanman agent uses Dynamic DNS (DDNS) to map virtual names with IP
addresses. If you use scavenging, then you must set the DNSRefreshInterval
attribute for the Lanman agent. This will enable the Lanman agent to
refresh the resource records on the DNS servers. See the Lanman agent
description in the *Veritas Cluster Server Bundled Agents Reference Guide* for
more information.

■ If the domain controller and the computer running the installation program
are on different subnets, the installer may be unable to locate the
computers selected for installation. In this situation, after the installation
program displays an error message, type the host names and the IP
addresses of the missing computers manually.

Permission requirements

- You must have administrative access to all systems selected for cluster operations. For this, add the domain user to the local Administrators group of each system.

- You must be a domain user.

- You must be a member of the Local Administrators group for all nodes where you are installing.

- Domain Administrator or Account Operator privileges: if you plan to create a new user account for the VCS Helper service, you must have Domain Administrator privileges or belong to the Account Operators group. If you plan to use an existing user account context for the VCS Helper service, you must know the password for the user account.

- The user account for the VCS Helper service must be a member of the administrators group on the filers.

Additional requirements

- Installation media for all products and third-party applications

- Licenses for all products and third-party applications

- You must install the operating system in the same path on all systems. For example, if you install Windows 2003 on C:\WINDOWS of one node, installations on all other nodes must be on C:\WINDOWS. Make sure that the same drive letter is available on all nodes and that the system drive has adequate space for the installation.

- When installing, install only in a single domain.

Best practices

- Symantec recommends three network adapters (two NICs exclusively for the private network and one for the public network).
  When using only two NICs, implement the second private link as a low-priority link over a public interface.

- Route each private NIC through a separate hub or switch to avoid single points of failure.

- Verify that you have set the Dynamic Update option for the DNS server to Secure Only.

Setting Windows driver signing options

Depending on the installation options you select, some Symantec drivers may not be signed. When installing on systems running Windows Server 2003, you must set the Windows driver signing options to allow installation.

Table 2-1 describes the product installer behavior on local and remote systems when installing options with unsigned drivers.

Table 2-1   Installation behavior with unsigned drivers

Driver Signing Setting	Installation behavior on the local system	Installation behavior on remote systems
Ignore	Always allowed	Always allowed
Warn	Warning message, user interaction required	Installation proceeds. The user must log on locally to the remote system to respond to the dialog box to complete the installation.
Block	Never allowed	Never allowed

On local systems set the driver signing option to either Ignore or Warn. On remote systems set the option to Ignore in order to allow the installation to proceed without user interaction.

To change the driver signing options on each system

1   Log on locally to the system.

2   Open the Control Panel and click **System**.

3   Click the **Hardware** tab and click **Driver Signing**.

4   In the Driver Signing Options dialog box, note the current setting, and select **Ignore** or another option from the table that will allow installation to proceed.

5   Click **OK**.

6   Repeat for each computer.
    If you do not change the driver signing option, the installation may fail on that computer during validation. After you complete the installation, reset the driver signing option to its previous state.

Installing the software using the product installer

The product installer enables you to install VCS for NetApp SnapMirror. Ensure that you also select the option to install the Veritas Cluster Server agent for Oracle.

To install VCS for NetApp SnapMirror

1   From Windows Explorer, navigate to the root directory of the VCS for Network Appliance DVD, and double-click **Setup.exe**.

2   On the product installation panel, click **VCS 5.0 for Network Appliance SnapMirror Release Update**.

3   Click Product Installation in the left pane, and then click **Complete/Custom** to install server components and optional client components.
    Click **Administrative Console** if you want to install the client components.

4   Review the welcome message and click **Next**.

5   Read the License Agreement by using the scroll arrows in the view window. If you agree to the license terms, click **I accept the terms of the license agreement** and then click **Next**.

6   In the Enter a license key and click Add field, type the license key, click **Add**, and then click **Next**.
    The License Key Details section displays more information about the selected key. To delete a license key, select the key from the key list and click **Remove**.

7   On the Option Selection panel, select the following product options and click **Next**:

    ■   **VCS 5.0 for Network Appliance SnapMirror Release Update (Server Components)**

    ■   **Global Clustering Option** - if you plan to configure a disaster recovery environment.

    ■   **High Availability Hardware Replication Agents:** Select **Veritas Cluster Server Hardware Replication Agent for NetApp**

    ■   **High Availability Database Agents:** Select **Veritas Cluster Server Database Agent for Oracle**

    ■   **Product Documentation**

    ■   **VCS 5.0 for Network Appliance SnapMirror Release Update (Client Components)** - This will install the VCS Java Console on the same nodes where the server components are installed.

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

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

9 The installer validates the prerequisites for the selected computers and displays the results. Review the information and click **Next**.
   If a computer fails validation, address the issue, and click **Validate Again**.

10 The Summary panel displays the installation settings summary. Review the information, click **Back** if you wish to make any changes, or click **Install** to begin the installation.

11 The Install/Uninstall panel displays the installation progress for the selected computers. After the installation is complete, click **Next**.
   If the installation fails on any computer, the status screen shows a failed installation.

12 The Finish panel displays the installation report. Review the installation report and click **Next**.
   If an installation fails, address the reason for failure. You may have to either repair the installation, or remove the software and re-install it.

13 Click **Reboot** to restart the remote computers.

14 After the remote computers have restarted, click **Next** and then click **Finish**.

15 Click **Yes** to restart the local computer.

After completing the installation sequence, reset the driver signing options on each computer.

To reset the driver signing options

1 Open the Control Panel, and click **System**.

2 Click the **Hardware** tab and click **Driver Signing**.

3 In the Driver Signing Options dialog box, reset the option to **Warn** or **Block**.

4 Click **OK**.

5 Repeat for each computer.

Installing the software from the command line

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

To start the installation from the command window

1   Insert the software CD into a drive connected to the system.

2   Click **Start** > **Run.**

3   Enter `cmd` in the Open field and click **OK**.

4   From the command window, navigate to the root directory of the product CD.

5   Use the following command to install the software:

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

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

Parameters for setup.exe

Information about the possible parameter values follows:

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

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

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

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

Example for setup.exe: client installation

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

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

Example for setup.exe: server installation

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

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

Configuring the cluster

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

■   If you plan to set up a disaster recovery environment, configure the wide-area connector process for global clusters.

■   When configuring a user account for the VCS Helper service, choose the administrative account set up on the filer.

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

To configure a VCS cluster

1   Start the VCS Configuration wizard. (**Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Cluster Configuration Wizard**)

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

3   On the Configuration Options panel, click **Cluster Operations** and click **Next**.

4 On the Domain Selection panel, select or type the name of the domain in which the cluster resides and select the discovery options.
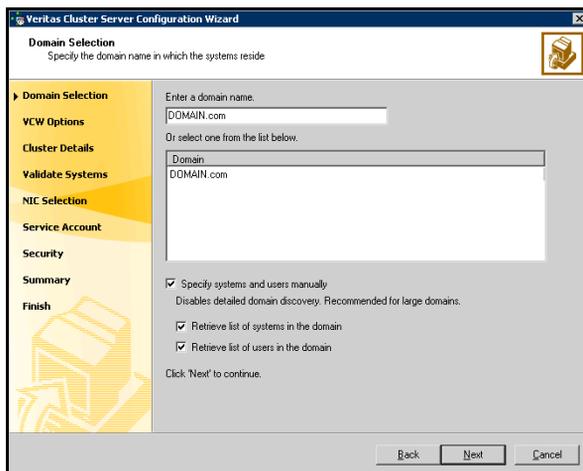
To discover information about all systems and users in the domain:

■ Clear the **Specify systems and users manually** check box.

■ Click **Next**.

Proceed to step 7 on page 31.

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

■ Check the **Specify systems and users manually** check box.

Additionally, you may instruct the wizard to retrieve a list of systems and users in the domain by selecting appropriate check boxes.

■ Click **Next**.

If you chose to retrieve the list of systems, proceed to step 6 on page 31. Otherwise, proceed to the next step.

5   On the System Selection panel, type the name of each system to be added, click **Add**, and then click **Next**. Do not specify systems that are part of another cluster.
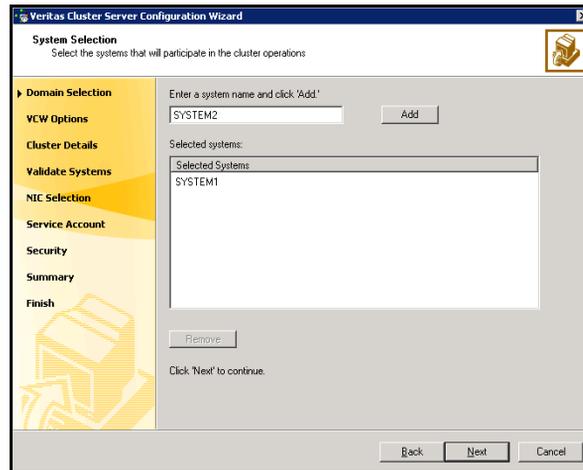
Proceed to step 7 on page 31.

6   On the System Selection panel, specify the systems to form a cluster and then click **Next**. Do not select systems that are part of another cluster.
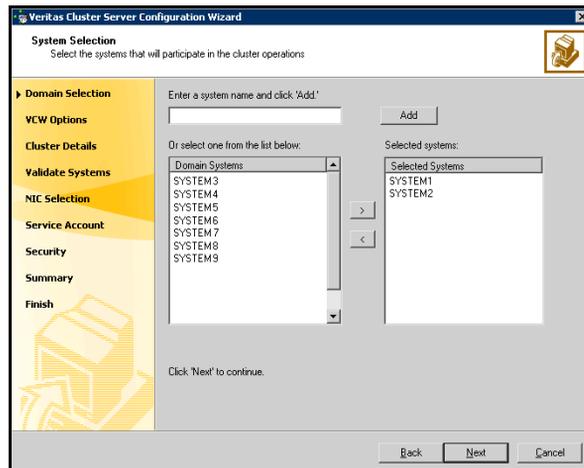
Enter the name of the system and click **Add** to add the system to the **Selected Systems** list, or click to select the system in the Domain Systems list and then click the **>** (right-arrow) button.

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

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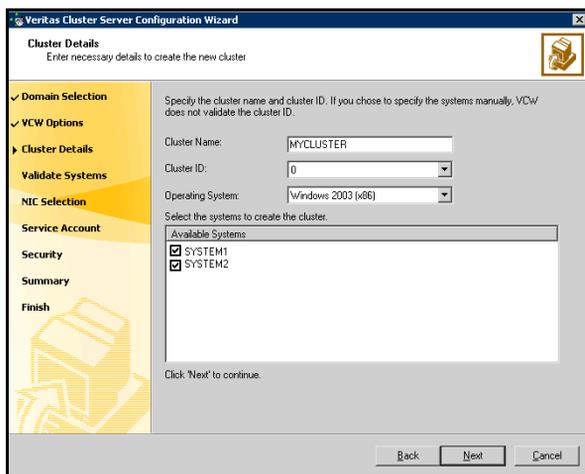
Cluster Name	Type a name for the new cluster. Symantec recommends a maximum length of 32 characters for the cluster name.
Cluster ID	Select a cluster ID from the suggested cluster IDs in the drop-down list, or type a unique ID for the cluster.
	Warning: If you chose to specify systems and users manually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

9 The wizard validates the selected systems for cluster membership. After the systems are validated, click **Next**.
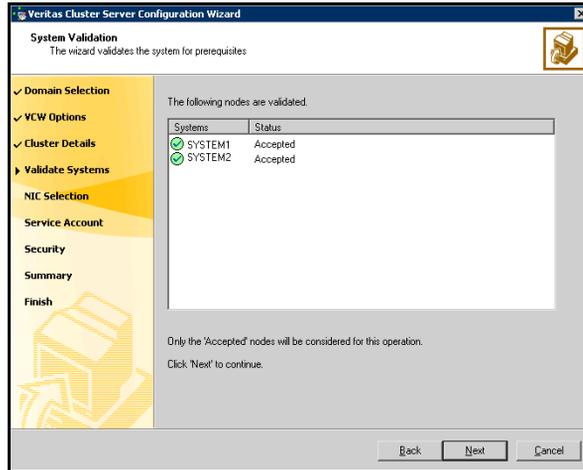
If a system is not validated, review the message associated with the failure and restart the wizard after rectifying the problem.

If you chose to configure a private link heartbeat in , proceed to the next step. Otherwise, proceed to .

10 On the Private Network Configuration panel, configure the VCS private network and click **Next**.
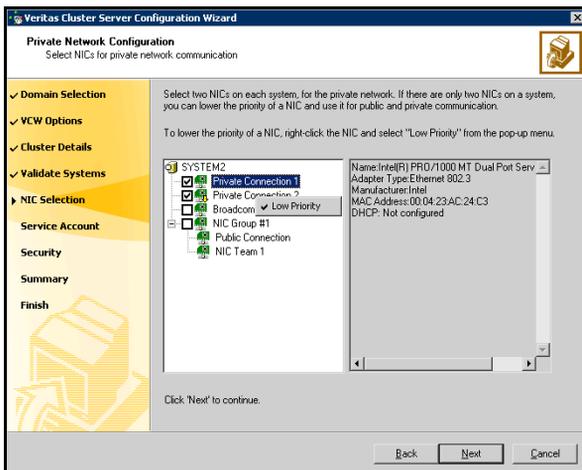
■ Select the check boxes next to the two NICs to be assigned to the private network. Symantec recommends reserving two NICs exclusively for the private network. However, you could lower the priority of one NIC and use the low-priority NIC for public and private communication.

■ If you have only two NICs on a selected system, make sure you lower the priority of at least one NIC for that system. To lower the priority of a NIC, right-click the NIC and select **Low Priority** from the pop-up menu.

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

11 On the VCS Helper Service User Account panel, specify the name of a domain user context for the VCS Helper service. The VCS HAD, which runs in the context of the local system built-in account, uses the VCS Helper

Service user context to access the network. Do not use the Administrator account for the VCS Helper service.
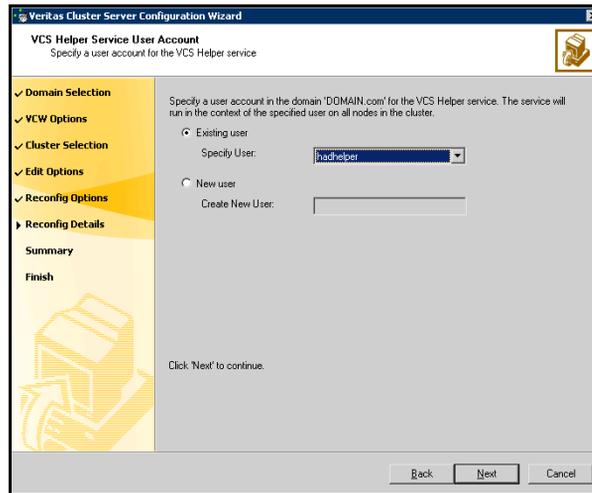
- To specify an existing user, do one of the following:
    - Click **Existing user** and select a user name from the drop-down list,
    - If you chose not to retrieve the list of users in step 4 on page 30, type the user name in the **Specify User** field, and then click **Next**.
- To specify a new user, click **New user** and type a valid user name in the **Create New User** field, and then click **Next**.

    Do not append the domain name to the user name; do not type the user name as DOMAIN\user or user@DOMAIN.

    - In the Password dialog box, type the password for the specified user and click **OK**, and then click **Next**.

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

Do one of the following:

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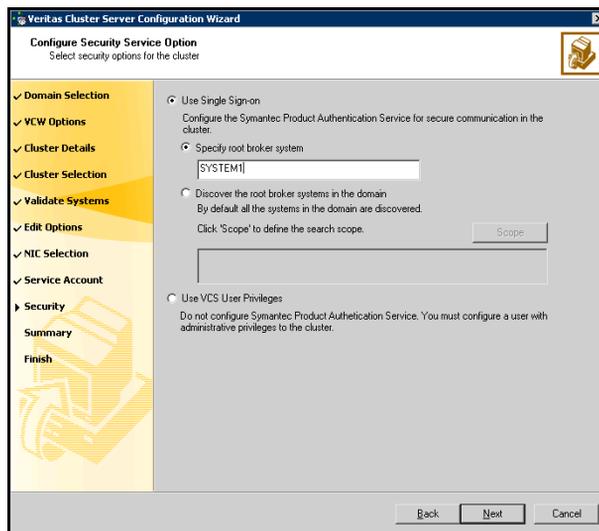
■ Click **Use Single Sign-on**. In this mode, VCS uses SSL encryption and platform-based authentication. The VCS engine (HAD) and Veritas Command Server run in secure mode.

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

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

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

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

■ If you want to discover the system that will serve as root broker, click **Discover the root broker systems in the domain** and click **Next**. The wizard will discover root brokers in the entire domain, by default.

■   If you want to define a search criteria, click **Scope**. In the Scope of
    Discovery dialog box, click **Entire Domain** to search across the
    domain, or click **Specify Scope** and select the Organization Unit
    from the Available Organizational Units list, to limit the search to
    the specified organization unit. Use the Filter Criteria options to
    search systems matching a certain condition. For example, to
    search for systems managed by Administrator, select **Managed by**
    from the first drop-down list, **is (exactly)** from the second
    drop-down list, type the user name **Administrator** in the adjacent
    field, click **Add**, and then click **OK**.

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

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

■   To use VCS user privilege:

■   Click **Use VCS User Privileges**. Accept the default user name and
    password for the VCS administrator account or type a new name
    and password.

The default user name for the VCS administrator is admin and the
default password is password. Both are case-sensitive. Use this account
to log on to VCS using Cluster Management Console (Single Cluster
Mode) or Web Console, when VCS is not running in secure mode.

- ■ Click **Next**.

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

If the selected systems have LLT or GAB configuration files, the wizard
displays an informational dialog box before overwriting the files. In the
dialog box, click **OK** to overwrite the files. Otherwise, click **Cancel**, exit the
wizard, move the existing files to a different location, and rerun the wizard.

The wizard starts running commands to configure VCS services. If an
operation fails, click **View configuration log file** to see the log.

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

To configure the ClusterService group later, click **Finish**.

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

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

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

15 On the Cluster Service Components panel, select the components to be configured in the ClusterService service group and click **Next**.
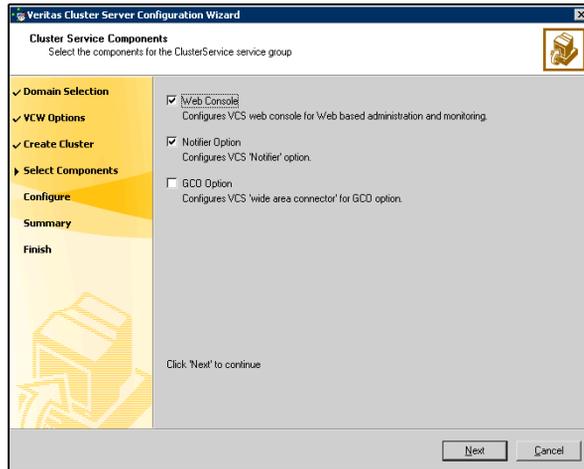
- Check the **Web Console** checkbox to configure the Cluster Management Console (Single Cluster Mode), also referred to as the Web Console.
- Check the **Notifier Option** checkbox to configure notification of important events to designated recipients.

Configuring Web console

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

To configure the Web console

1   On the Web Console Network Selection panel, specify the network information for the Web Console resources and click **Next**.
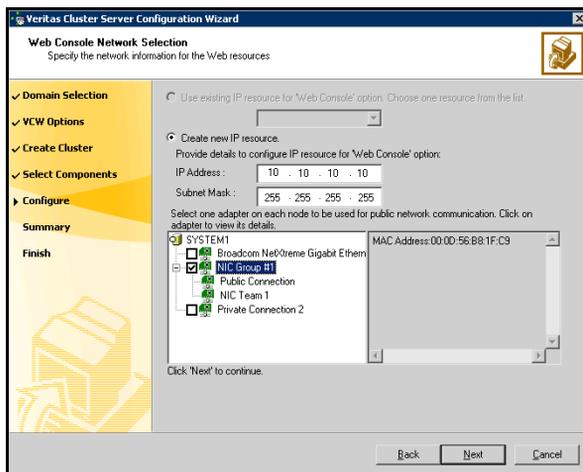
   - ■   If the cluster has a ClusterService service group configured, you can use the IP address configured in the service group or configure a new IP address for the Web console.

   - ■   If you choose to configure a new IP address, type the IP address and associated subnet mask.

   - ■   Select a network adapter for each node in the cluster. Note that the wizard lists the public network adapters along with the adapters that were assigned a low priority.

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

3   If you chose to configure a Notifier resource, click Next to proceed with the configuration. Otherwise, click **Finish** to exit the wizard.

Configuring notification

This section describes steps to configure notification.

To configure notification

1   On the Notifier Options panel, specify the mode of notification to be configured and click **Next**.
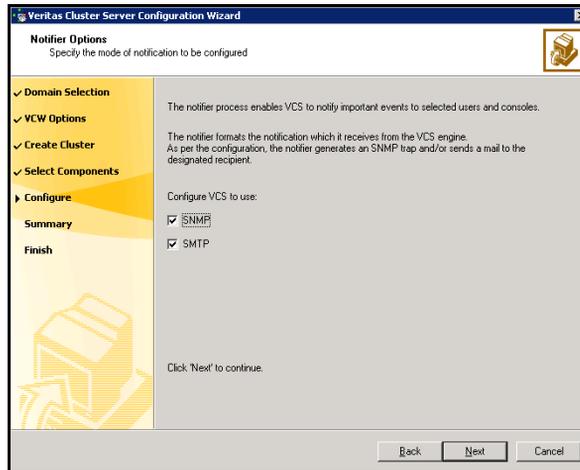
You can configure VCS to generate SNMP (V2) traps on a designated server and/or send emails to designated recipients in response to certain events.

2   If you chose to configure SNMP, specify information about the SNMP console and click **Next**.
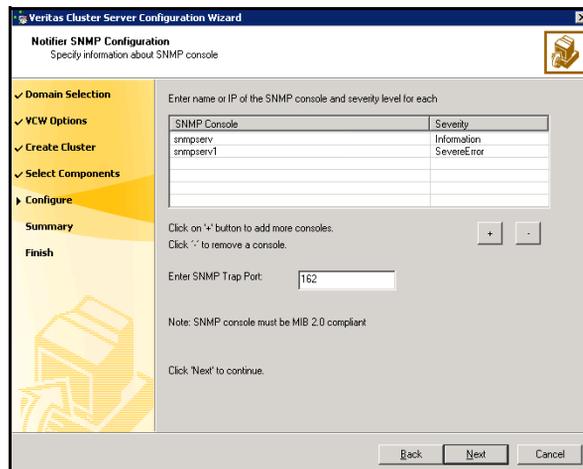
■ Click a field in the SNMP Console column and type the name or IP address of the console. The specified SNMP console must be MIB 2.0 compliant.

■ Click the corresponding field in the Severity column and select a severity level for the console.

■ Click '**+**' to add a field; click '**-**' to remove a field.

■ Enter an SNMP trap port. The default value is "162".

3 If you chose to configure SMTP, specify information about SMTP recipients and click **Next**.
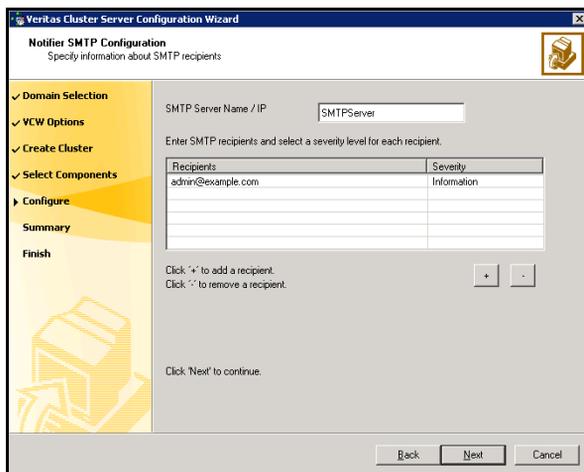
■ Type the name of the SMTP server.

■ Click a field in the Recipients column and enter a recipient for notification. Enter recipients as admin@example.com.

■ Click the corresponding field in the Severity column and select a severity level for the recipient. VCS sends messages of an equal or higher severity to the recipient.

■ Click **+** to add fields; click **-** to remove a field.

4   On the Notifier Network Card Selection panel, specify the network
    information and click **Next**.
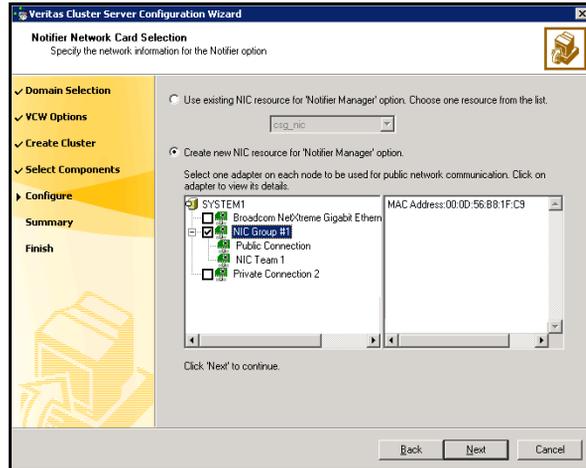
■   If the cluster has a ClusterService service group configured, you can
    use the NIC resource configured in the service group or configure a new
    NIC resource for notification.

■   If you choose to configure a new NIC resource, select a network adapter
    for each node in the cluster. The wizard lists the public network
    adapters along with the adapters that were assigned a low priority.

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

6   Click **Configure**.

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

Configuring Wide-Area Connector process for global clusters

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

To configure the wide-area connector process for global clusters

1 On the GCO Network Selection panel, specify the network information and click **Next**.
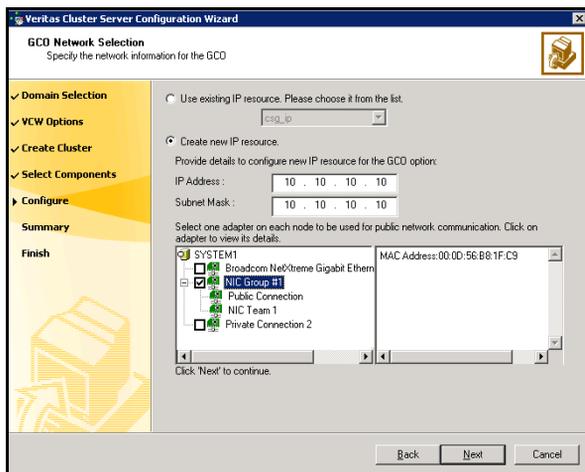
■ If the cluster has a ClusterService service group configured, you can use the IP address configured in the service group or configure a new IP address.

■ If you choose to configure a new IP address, enter the IP address and associated subnet mask. Make sure that the specified IP address has a DNS entry.

■ Select a network adapter for each node in the cluster. The wizard lists the public network adapters along with the adapters that were assigned a low priority.

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

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

Installing and configuring Oracle

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

This section describes steps to install and configure Oracle on all cluster nodes that will participate in the Oracle service group.

For specific instructions on how to install Oracle, see the Oracle documentation.

Prerequisites

- Verify all nodes have adequate resources to run Oracle and VCS for NetApp SnapMirror.

- Verify that VCS for NetApp SnapMirror is installed on all nodes in the cluster.

- Verify you have run the VCS Configuration Wizard (VCW) to configure VCS on all nodes.

- Log on as domain administrator to install Oracle binaries.

- If using iSCSI, verify that the Microsoft iSCSI Initiator is configured to establish a persistent connection between the Network Appliance filer and the cluster nodes. See the Microsoft documentation for instructions.

- 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.

- Make sure that you have an external, basic disk to create LUNs (or virtual disk).
  See "Managing storage using Network Appliance Filer" on page 48 for instructions.

Note: After creating the database, you must log on to Oracle with database administrator privileges and complete the installation procedure on all nodes in the cluster.

Privileges requirements

- You must be a domain user. The domain user must have administrator privileges.

- You must be a member of the Local Administrators group on all nodes on which Oracle will be installed.

- You must have write permissions for the Active Directory objects corresponding to these nodes.

- You must have write permissions on the DNS server to perform DNS updates.

- Domain Administrator or Account Operator privileges: if you plan to create a new user account for VCS Helper service, you must have Domain Administrator privileges or belong to the Account Operators group. If you plan to use an existing user account context for the VCS Helper service, you must know the password for the user account.

Configuring Microsoft iSCSI Initiator

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

To configure Microsoft iSCSI initiator

1. Make sure the Microsoft iSCSI Initiator software version 2.0 is installed on all cluster nodes. Refer to Microsoft documentation for further information.

2. Start the Microsoft iSCSI initiator. Double-click the Microsoft iSCSI Initiator icon from the desktop.

3. Click the **Target Portals** tab, if not already selected.

4. Click **Add...**.

5. In the Add Target Portals dialog box, specify the IP address or the DNS name for the Network Appliance Filer and click **OK**.

6. Click the **Available Targets** tab and click **Log On...**.

7   In the Log On to Target dialog box, verify the target portal name and select
    the **Automatically restore this connection when the system reboots** check
    box.

8   Click **OK**.

9   Click the **Persistent Target** tab to verify that the newly added target portal is
    listed under the **Select a target** box.

10 Click **OK**.

Managing storage using Network Appliance Filer

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

Note: Symantec does not support volumes created using qtree.

Figure 3-1   VCS cluster in a NetApp storage environment
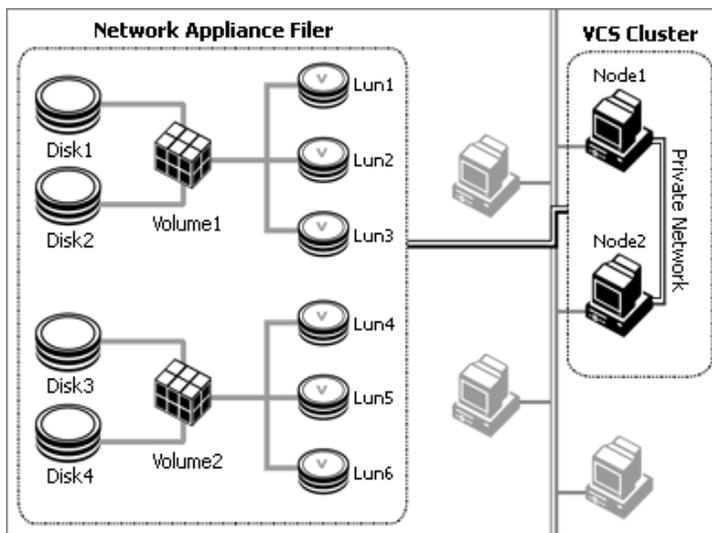
The VCS agent for Oracle requires the following LUNs to be created on the Network Appliance Filer. These LUNs must be accessible from all cluster nodes.

Symantec recommends creating three LUNs, one each for the following:

■   database files

■   control files

■   log files, including the redo logs and archive logs

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

- INST1_DATA_FILES: contains the Oracle system data files (including the master, model, msdb, and tempdb databases)

- INST1_REGREP_VOL: contains the list of registry keys that must be replicated among cluster systems for the Oracle Service. Create a 100 MB (minimum recommended size) volume for this purpose.

- INST1_DB1_VOL: contains the user database files

- INST1_DB1_LOG: contains the user database log files

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

- Create volumes on the Network Appliance Filer.

- Share the volumes.

- Create LUNs on the shared volumes.

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

Connecting virtual disks to the cluster node

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

To connect virtual disks to the cluster node

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

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

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

4   Click **Next** on the Welcome page.

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

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

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

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

9   On the igroup Management Type panel, choose the option that allows SnapDrive to perform igroup management automatically and then click **Next**.

10   Click **Finish** to begin connecting the specified virtual disk to the cluster node.

Disconnecting virtual disks from the cluster nodes

To disconnect virtual disks

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

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

3   Double-click **Disks** to see the LUNs that are connected to the node.

4   Right-click the LUN you want to disconnect and then click **Disconnect Disk...**.

5   In the Disconnect Disk alert box, click **OK**.

Installing and configuring Oracle

The strategy for installing Oracle into a VCS cluster is aimed at ensuring that installations on all cluster systems are uniform. This involves installing the Oracle binaries locally on each system and installing the Oracle control files, datafiles, and log files, and the flash recovery area on shared storage.

Note: Before installing Oracle, create LUNs on the filer. Symantec recommends at least three LUNs on the filer, one each for control files, log files, and database files.

Overview of tasks

You must perform these tasks on each node that will host the Oracle service group.

- Verify that the virtual disks on the filer are connected to the first cluster node.
  See "Connecting virtual disks to the cluster node" on page 49.

- Install Oracle binaries.
  See "Installing Oracle" on page 52.

- Create the listener service.
  See "Creating the listener service" on page 53.

- Configure the listeners to use the virtual IP address.
  See "Configuring the listeners to use the virtual IP address" on page 54.

- Create the database on shared virtual disks.
  See "Creating the database on shared virtual disks" on page 55.

- Create a virtual IP address for the databases and the listeners.
  See "Creating a virtual IP address" on page 56.

- Associate the database with the listener service.
  See "Associating the database with the listener" on page 56.

- Configure the database.
  See "Configuring the databases" on page 57.

- Configure the listeners to use the same virtual IP address.
  See "Configuring the listeners to use the virtual IP address" on page 54.

- Make sure that the Oracle registry points to the correct location of the initialization parameter file.
  See "Verifying the initialization file settings" on page 62.

- Disconnect the virtual disks from the first cluster node.
  See "Disconnecting virtual disks from the cluster nodes" on page 50

- Delete the virtual IP address.
  See "Removing the virtual IP address" on page 64.

Installing Oracle

Install Oracle from the Oracle software disc. The installer screens and options may vary slightly for different versions of Oracle.

Install the Oracle program files on a local disk and the Oracle data files on shared storage. Install all log files, including redo logs and archive logs, on the same virtual disk.

Specify the same parameters on all nodes. For example, the database name, file locations, database credentials, must be the same on all nodes.

To install Oracle

1   Verify the shared virtual disks created to store Oracle data are connected to the node where you run the wizard.
    See "Connecting virtual disks to the cluster node" on page 49.

2   Insert the Oracle software disc in a drive connected to the node and run the Setup program.

3   From the browser menu, click **Install/Deinstall Products**.

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

5   Complete the following instructions depending on the version of Oracle:
    For Oracle 10g

    - In the Available Products panel, select the **Oracle 10g Database** option and click **Next**.

    - Choose the **Basic** or **Advanced** installation type.
      For Basic installation:

        - In the **Oracle Home Location** box, type or select a name and a path on the local disk for the Oracle Home.
          This installs the Oracle binaries on the local disk. Use the same *Oracle_Home* name and path on all nodes.

        - Select **Enterprise Edition**.

        - Uncheck the **Create Starter Database** check box and click **Next**.
      For Advanced installation:

        - Select the destination directory for the Oracle installation and click **Next**.

- ■ Select **Enterprise Edition** and click **Next**.
- ■ Select **Do not create a starter database**.

6 Follow the wizard instructions, select options as per your configuration, and complete the installation.

The Oracle installation also adds a Perl package. Make sure the path of the Perl package appears as the first value in the PERL5LIB environment variable.

To modify the path of the Perl variable

1 Right-click **My Computers** and then click **Properties**.

2 In the **System Properties** window, on the **Advanced** tab, click **Environment Variables**.

3 In the **System Variables** area of the **Environment Variables** window, double-click the PERL5LIB variable name to edit it.

4 In the **Variable Value** field, add the path of the Perl package installed by Symantec such that it is the first value in the definition. For example, add the path `C:\Program Files\Veritas\VRTSPerl\lib;` as the first value in the definition. Note that you must add a semi-colon at the end of the path.

After the Oracle installation is complete, verify if the Oracle home path (the path that you set while installing Oracle) is included in the Path environment variable. If not, then you have to manually add the Oracle home path to the Path variable, on all the cluster nodes.

To add the oracle home path to the Path variable

1 Right-click **My Computers** and then click **Properties**.

2 In the **System Properties** window, on the **Advanced** tab, click **Environment Variables**.

3 In the **System Variables** area of the **Environment Variables** window, double-click the Path variable name to edit it.

4 In the **Variable Value** field, add the Oracle home path.

5 Repeat steps 1 to 4 on all the cluster nodes.

Creating the listener service

Create a listener service using the Net Configuration Assistant. Refer to the Oracle documentation for instructions. Make a note of the listener name; you will need it in subsequent configuration tasks.

Configuring the listeners to use the virtual IP address

In the file listener.ora file, change the host name to the virtual IP address that you created.

Replace

    HOST=*machine_name*

with

    HOST=*virtual_IP_address*

The default location of the file listener.ora is

%ORACLE_HOME%\NETWORK\ADMIN\

Creating the database on shared virtual disks

When run from the first node, this process creates an Oracle database on shared virtual disks. Before running this process from other nodes, rename the directories containing the control files, redo log files, and the database files so that you create new files from each node.

For example, if the Oracle database was created at the path `H:\Oracle\Data`, rename it to `H:\Oracle\Data_old`. You can delete these renamed directories after installing and configuring Oracle on all nodes in the cluster.

To create a database on a shared virtual disk

1   Start the Database Configuration Assistant (**Start > All Programs > Oracle-*Oracle_Home* > Configuration and Migration Tools > Database Configuration Assistant**). This launches the database installer.

2   In the Welcome panel, click **Next**.

3   In the Operation panel, select **Create a database** and click **Next**.

4   Complete the following instructions depending on the Oracle version.
    For Oracle 10g

   ■   In the Database Templates panel, select the **Custom Database** option and click **Next**.

   ■   In the Database Identification panel, specify the **Global Database Name** and **SID** in the respective fields.

   ■   Choose to install the database on the shared virtual disk.

   ■   Choose to install the initialization parameter files on the local disk.

5   Follow the wizard instructions and select other options as per your desired database configuration.

6   Install the control files, data files, and log files on the shared virtual disks. In the Database Storage panel, specify the locations of control files, data files, and redo log files.
    In the left pane, expand the **Storage** folder.

   ■   Enter a path on the shared virtual disk for each control file.
       To do so, click **Controlfile** and click the **General** tab in the right pane. In the **File Directory** field, enter a path on the shared virtual disk.

   ■   Enter a path on the shared virtual disk for each data file.
       To do so, expand the **Datafiles** folder in the left pane. Select a data file, and click the **General** tab in the right pane. In the **File Directory** field, enter a path on the shared virtual disk.

   ■   Enter a path on the shared virtual disk for each redo log file

To do so, expand the **Redo Log Groups** folder in the left pane. Select a redo log group and click the **General** tab in the right pane. In the **File Directory** field, enter a path on the shared virtual disk.

■ Click **Next**.

7 Select the **Create database** and the **Generate Database Creation Scripts** options and click **Finish**.

8 Follow the wizard instructions and complete the installation.

Creating a virtual IP address

All databases and listeners configured must use the same virtual IP. Create a virtual IP address that can be set for all databases and listeners.

To create a virtual IP address

1 Open the **Network Connections** (**Start > Settings > Network Connections**).

2 Right-click the public network connection to be used and then click **Properties**.

3 Select **Internet Protocol (TCP/IP)** and click **Properties**.

4 Click **Advanced**, and on the IP Settings tab, under IP addresses, click **Add** to add a virtual IP address and subnet mask.

Associating the database with the listener

Use these instructions to associate all the databases with the listeners.

Prerequisite

Ensure that the initialization parameter file contains the following entries:

■ SERVICE_NAMES (the name of the database service)

■ INSTANCE_NAME (the name of the database instance)

These parameters are created during installation or database creation.

To associate the database with the listener

1 Use one of the following ways to configure the new attribute listener_alias:
Run the following SQL command:
SQL> **ALTER SYSTEM SET LOCAL_LISTENER='<listener_alias>'
scope=spfile;**
OR
Add the following entry to the initialization parameter file (pfile/spfile):
LOCAL_LISTENER = <listener_alias>

2　Define the parameter listener_alias. If your Oracle configuration uses the file tnsnames.ora, edit the file as instructed below. The default location of tnsnames.ora is `%ORACLE_HOME%\NETWORK\ADMIN`.

Add the following to tnsnames.ora file:

```
<listener_alias>=
(DESCRIPTION =
(ADDRESS=(Protocol=TCP)(HOST=virtual_IP_address)(Port=1521))
)
```

3　Stop and restart the database.

The listener_alias parameter gets appended by the default domain name specified in the file sqlnet.ora.

Configuring the databases

Configuring the databases involves setting parameters in Oracle configuration files. It involves setting the same virtual IP address for all the databases and configuring the databases to use the OS authentication model of Oracle.

Updating the tnsnames.ora files

If your configuration has a tnsnames.ora file, edit the file as instructed below. The default location of the file is `%ORACLE_HOME%\NETWORK\ADMIN\`.

Change the host name for all the TCP protocol address databases to the virtual IP address that you created.

Replace
`HOST=machine_name`
with
`HOST=virtual_IP_address`

If you use a PFILE (initSID.ora)

Configure the PFILE to use the virtual IP address for the service group and set the database to use the OS authentication model of Oracle.

1　Edit the dispatchers parameter by adding or editing the HOST parameter. If the ADDRESS tag does not appear, add it. The edited dispatchers parameter should look like:

```
    dispatchers = '(ADDRESS=(Protocol=TCP)
(HOST=virtual_IP_address) (other entries))'
```

The variable *virtual_IP_address* represents the virtual IP address that you created.

For example:

```
dispatchers = '(ADDRESS=(Protocol=TCP) (HOST=10.100.101.102)
(SERVICE=Data1XDB)'
```

2 Configure the attribute `remote_login_passwordfile`. Symantec recommends setting the attribute to `NONE` so that the database uses OS authentication and the configuration does not require a password file. A sample entry appears as:

```
remote_login_passwordfile = 'NONE'
```

If you use an SPFILE

■ If you use an SPFILE on Oracle 10g, proceed to "**Modifying the SPFILE (Oracle 10g)**" on page 58.

Modifying the SPFILE (Oracle 10g)

VCS requires a customized version of the SPFILE, which cannot be edited. But, you can create a PFILE from the SPFILE, edit the PFILE, and convert it to an SPFILE again.

1 Log on to the Oracle database as administrator and create a temporary PFILE from the SPFILE.

```
C:\> sqlplus "/as sysdba"
SQL> create pfile='tmp_pfile_name' from
spfile='spfile_name';
```

For example:

```
SQL> create
pfile='C:\oracle\product\10.1.0\Db_1\database\tempPFI
LE.ora'   from
spfile='C:\oracle\product\10.1.0\Db_1\database\SPFILE
Prod.ora';
```

2 Edit the dispatchers parameter by adding or editing the HOST parameter. If the ADDRESS tag does not appear, add it. The edited dispatchers parameter should look like:

```
dispatchers = '(ADDRESS=(Protocol=TCP)(HOST=virtual_IP_address)
(other entries))'
```

The variable *virtual_IP_address* represents the virtual IP address that you created.

For example:

```
dispatchers = '(ADDRESS=(Protocol=TCP) (HOST=10.100.101.102)
(SERVICE=Data1XDB)'
```

3 Configure the attribute `remote_login_passwordfile`. Symantec recommends setting the attribute to `NONE` so that the database uses OS authentication and the configuration does not require a password file. A sample entry appears as:

```
    remote_login_passwordfile = 'NONE'
```

4 Create a temporary SPFILE from the edited PFILE.

```
    SQL> create spfile='tmp_spfile' from
pfile='temp_pfile_name';
```

For example:

```
SQL> create spfile=
'C:\oracle\product\10.1.0\Db_1\database\
temp_SPFILEProd.ora'
        from
pfile='C:\oracle\product\10.1.0\Db_1\database\
tempPFILE.ora';
```

5   Stop the database service.

6   Back up the original SPFILE by renaming it. For example, rename
    SPFILEProd.ora to original_SPFILE.ora.

7   Delete the original SPFILE (SPFILEProd.ora).

8   Rename the temporary SPFILE (temp_SPFILE.ora) to the name of the
    original SPFILE (SPFILEProd.ora).

9   Start the database service.

Moving the initialization file to shared virtual disks (Oracle 10g)

For Oracle 10g, move the initialization files to the shared virtual disk and configure the SPFILE to start a database instance.

1   Verify which of the following initialization files exist in your configuration. The default location of these files is `%ORACLE_HOME%\database.`

  ■   SPFILE*SID*.ora

  ■   SPFILE.ora

  ■   init*SID*.ora

  The variable *SID* represents the database instance.

2   Stop the database service using the Services snap-in.

3   Move the initialization files from the local disk to the shared virtual disk, preferably at the same location as the database control files.

4   Create a PFILE to specify the location of the SPFILE. The PFILE must be in the same directory on the shared virtual disk as the SPFILE.

  Modify the PFILE so that it contain only the following entry:

```
SPFILE = spfile_location
```

  The variable *spfile_location* represents the fully qualified path of the SPFILE on the shared virtual disk.

  For example, if your SPFILE is located at path `H:\Oracle\Data`, create a PFILE sp_init.ora in the same location `H:\Oracle\Data` with the following parameter:

```
SPFILE = H:\Oracle\Data\spfileSID.ora
```

Setting the Oracle database parameters

1   Set the Oracle database parameters using the `oradim` utility. Type the following at the command-prompt:

    `set ORACLE_SID=SID`

    The variable *SID* represents the database instance.

2   Run the following command:

    ```
    %ORACLE_HOME%\bin\oradim -edit -sid SID -pfile
    "pfile_location_on_shared_disk" -startmode auto
    -timeout 100 -shuttype srvc,inst -shutmode i
    ```

    The variable *SID* represents the database instance.

    This command performs the following tasks:

    ■   Sets the `-startmode` parameter to start the database instance automatically when Oracle service is started.

    ■   Sets the `-timeout` parameter to 100. The timeout parameter specifies the maximum wait time (in seconds) for the database shutdown to complete before the service for a particular SID stops.

    ■   Sets the `-shuttype` parameter to stop both the database instance and the service while shutting the database.

    ■   Sets the `-shutmode` parameter to shut the database instance as soon as the VCS for NetApp SnapMirror Database agent for Oracle requests.

3   Start the database service using the Services snap-in.

Verifying the initialization file settings

If a PFILE is used:

1   Open the Registry Editor.
    From the **Start** menu, choose **Run**. In the **Open** field, enter `regedit` and
    click **OK**.

2   Double-click the ORA_*SID*_PFILE registry key at
    HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME_*ID*\.
    The variable *SID* represents the database instance.

3   Verify that the Value data field specifies the fully qualified path of the PFILE
    along with the file name.

If an SPFILE is used:

1   Stop and restart the database services.

2   Run sqlplus.exe.

3   Connect to the database.

4   Verify the following query returns the correct shared virtual disk path for
    the SPFILE.
    ```
    select value from v$parameter where name = 'spfile';
    ```

Configuring the Oracle and listener services

Set the startup type of the Oracle database and Listener services to manual and configure the Log On properties for the Oracle services.

1   Open the **Services** applet (**Start > All Programs > Administrative Tools > Services**).

2   Set the startup type of the Oracle database service to manual and configure its Log On properties:

■   Double-click the Oracle database service. In the SCM, Oracle database services appear as OracleService*SID,* where *SID* represents the database instance.

■   In the **Properties** window, click the **General** tab.

■   From the **Startup Type** drop-down list, select **Manual.**

■   Click **Stop** to stop the service.

■   Click the **Log On** tab.

■   Choose **This Account**.

■   Enter the credentials of the user in whose context Oracle was installed.

■   Click the **General** tab and click **Start** to start the service with the new Log On properties. Click **OK**.

3   Set the startup type of the Listener service to manual.

■   In the Services applet, double-click the listener service. Listener services appear as Oracle*Ora_Home*TNS*ListenerName*, where *Ora_Home* represents the Oracle home directory and *ListenerName* is the name of the listener set during the installation.

■   In the **Properties** window, click the **General** tab.

■   From the **Startup Type** drop-down list, select **Manual** and click **OK.**

Disconnecting virtual disks from the first node

Disconnect the virtual disks only if you plan to install Oracle on more nodes. If this is the last node for the Oracle installation, do not disconnect the virtual disks. Before disconnecting the virtual disks, stop the database and listener services.

See "Disconnecting virtual disks from the cluster nodes" on page 50.

Removing the virtual IP address

Remove the IP address if you plan to install Oracle on more nodes.

To remove the virtual IP address

1   Open the **Network Connections** (**Start > Settings > Network Connections**).

2   Right-click the public network connection to be used and click **Properties**.

3   Select **Internet Protocol (TCP/IP)** and click **Properties**.

4   Click **Advanced** and on the IP Settings tab, under IP Addresses, select the virtual IP address that you added and click **Remove**.

Repeat the instructions in section "Installing and configuring Oracle" on page 51 on each node in the cluster. If you have installed the Oracle agent, proceed to "Configuring the Oracle service group" on page 65.

Configuring the Oracle service group

Configuring the Oracle service group involves creating resources for Oracle and NetApp, and defining attribute values for the configured resources.

VCS provides several ways to configure the Oracle agent: the agent configuration wizard, the Java and Web consoles, and the command line. This chapter provides instructions on how to use the agent configuration wizard to configure the agent. The Oracle Configuration Wizard enables you to create the Oracle service group and define the attributes for its resources on all the cluster nodes simultaneously.

Oracle configurations in VCS

You can set up Oracle in different ways in a VCS environment.

- Single Oracle instance configuration: Provides high availability for an Oracle instance associated with a listener.

- Multiple Oracle instances (single listener) configuration: Provides high availability for one or more Oracle instances sharing a common listener.

- Multiple Oracle instances (multiple listeners) configuration: Provides high availability for one or more Oracle instances that are configured to one or more listeners.

Configuring the agent using the Oracle Agent Configuration Wizard

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

Before configuring the Oracle agent, review the resource type and the attribute definitions of the Oracle agents, described in Appendix A, "Resource type definitions" on page 93.

For sample configuration file and resource dependency graph of the Oracle service group, see Appendix B, "Sample configuration" on page 101.

Prerequisites

- You must be a Cluster Administrator. This user classification is required to create and configure a service group.

- You must be a Local or Domain Administrator on the node where you run the wizard.

- Verify that VCS for NetApp SnapMirror along with the VCS agent for Oracle is installed on all cluster nodes.

- Verify that a VCS cluster is configured using VCS Configuration Wizard (VCW).

- Verify that the Veritas High Availability engine (HAD) is running on the system from where you run the wizard.

- Mount the shared virtual disks containing the data files, control files, and redo log files. Unmount the virtual disks from other systems in the cluster.

- Assign the virtual IP address on the system where you run the wizard. Remove the virtual IP address from other systems

- Mount the database and start the Oracle instance on the node running the wizard.

- Make sure that you have the following information ready; the wizard will prompt you for this information:
    - The databases and listeners to be monitored by VCS.
    - For the instances to be monitored in detail, name and location of the respective SQL files.
    - A valid domain name, user name, and password with which the database service was configured for the database.

Configuration instructions

This section describes how to create an Oracle service group.

To create an Oracle service group

1   Start the Oracle configuration wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Database Agent for Oracle > Oracle Configuration Wizard**.

2   In the Welcome panel click **Next**.

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

4   In the Service Group Configuration panel, complete the following and click **Next**. The wizard starts validating your configuration. Various messages indicate the validation status.
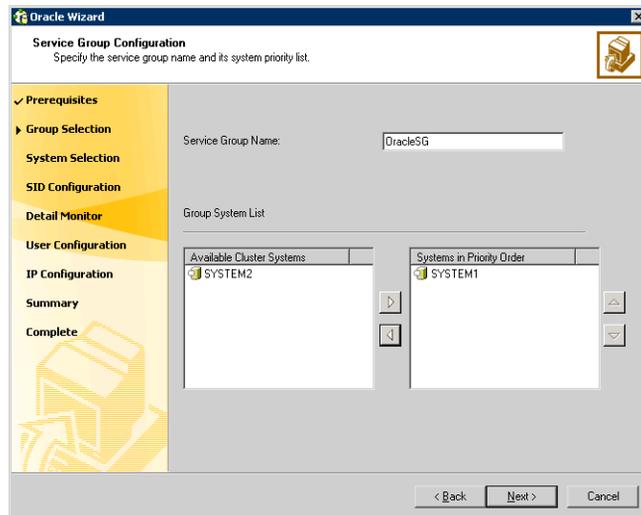
| Service Group Name | Type a name for the Oracle service group. |

Available Cluster Systems	Select the systems on which to configure the service group and click the right arrow to move the systems to the Systems in Priority Order box.
	The Systems in Priority Order box represents the service group's system list. 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.
	To remove a system from the service group's system list, select a system in the Systems in Priority Order box and click the left arrow.
	To change a system's priority in the service group's system list, select the system from the Systems in Priority Order box, and click the up and down arrows.

5   In the Oracle Configuration panel, complete the following and then click **Next**.
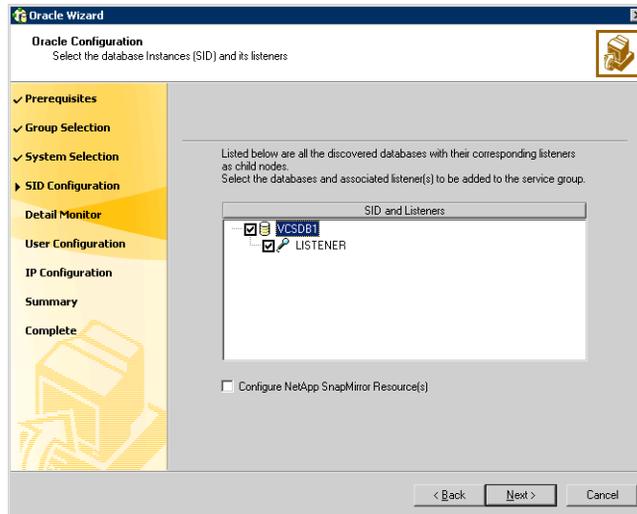
- Select the SIDs and the associated listeners to be added to the service group. The SID is a system identifier that uniquely identifies the Oracle database instance, while the listener is the name of the corresponding listener service.

- Check the **Configure NetApp SnapMirror Resource(s)** check box if you wish to set up a disaster recovery configuration. The SnapMirror

resource is used to monitor replication between filers at the primary
and the secondary site, in a disaster recovery configuration.

Note that you must configure the SnapMirror resource only after you
have configured the cluster at the secondary site.

6   On the Detail Monitoring panel, configure detail monitoring for the Oracle
database if required, and click **Next**.
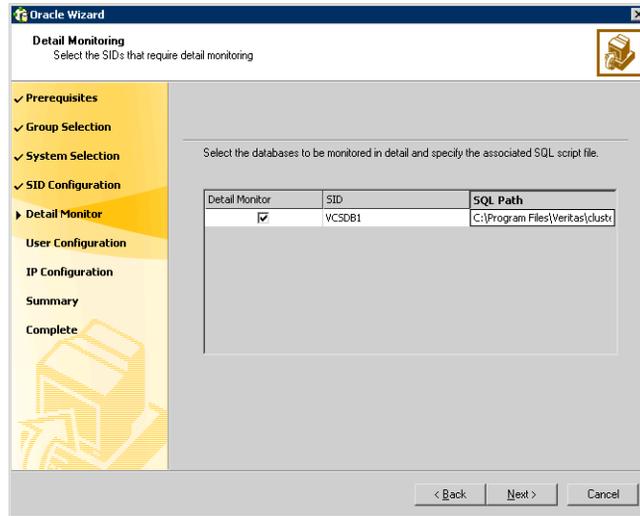
Detail Monitor	Check the Detail Monitor option corresponding to each database that you want to configure detail monitoring for.
SQL Path	Type the path of the SQL file that will query the database to validate the status. Click the icon next to the field to browse for the SQL file. A sample SQL file, check.sql, is located at `%VCS_HOME%\bin\Oracle\`.

7   In the Domain and User selection panel, type a valid domain name, user
name, and password with which the database service was configured for the
database and click **Next**.
See "Configuring the Oracle and listener services" on page 63 for more
information.

8   On the Initiator Selection panel, select the initiators for the virtual disk
from the list of available initiators displayed for each cluster node, and then
click **Next**.
If you are configuring MPIO over FC, you must select at least two FC
initiators for each cluster node. Note that the node from which you run this

wizard already has an initiator selected by default. This is the initiator that was specified when you connected the LUNs to this cluster node.

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

The wizard discovers and displays the virtual IP address for the Oracle Server.
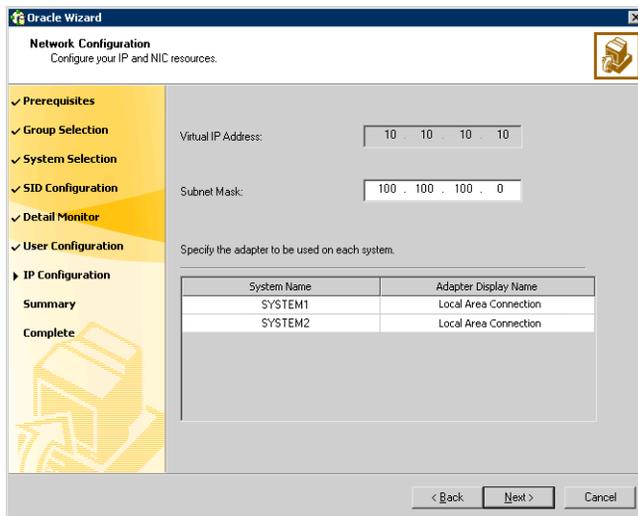
Subnet Mask	Type the subnet mask to which the virtual IP belongs.
Adapter Display Name	For each system in the cluster, select the public network adapter. Select the Adapter Name field to view the adapters associated with a system.

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

10   Review the configuration on the Summary panel and click **Next**.
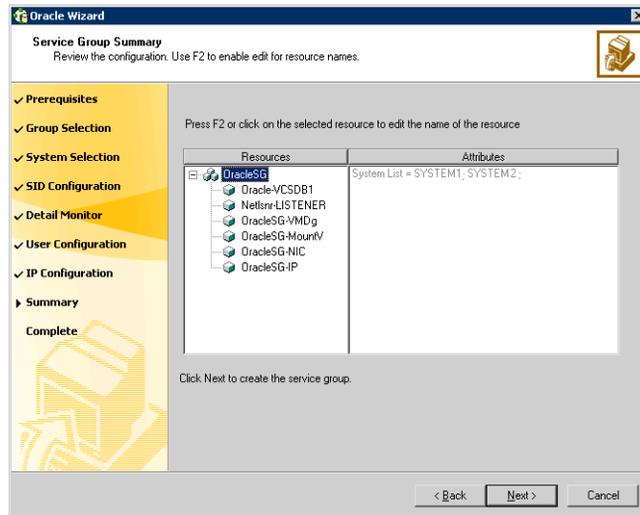
Resources   Lists the configured resources. Click on a resource to view its
                     attributes and their configured values in the Attributes box.
                     The wizard assigns unique names to the resources. To edit a
                     resource name, select the resource name and click on it, or
                     press the F2 key. After the edit, press the Esc key to cancel the
                     changes, or press the Enter key to confirm the changes.

11   In the confirmation dialog box, click **Yes**. Click **No** if you wish to review your
     settings.

12   The wizard starts running commands to create the Oracle service group. On
     the Completing the Oracle Configuration panel, check **Bring the service
     group online** to bring the service group online on the local system, and click
     Finish. The Oracle service group is created in your cluster.

After verifying that the service group comes online on the node, remove the
virtual IP address that you created earlier.

To remove the virtual IP address

1   Take the Oracle service group offline on the node.

2   Remove the virtual IP address. See "Removing the virtual IP address" on
    page 64 for instructions.

3   Bring the Oracle service group online.

Configuring dependent services

If the database service has other dependent services, make sure the dependent services are running on the node where the database service is online. Note that the online agent operation brings only the database service online and not the dependent services.

For example, on Oracle 10g, the DBConsole service corresponding to an Oracle database has a dependency on the database service. That is, for the Enterprise Manager to manage the databases, you must make sure the DBConsole service is running on the node where the database service is online.

To configure a dependent service

1   For the dependent service, add a GenericService resource manually.

2   Make the GenericService resource dependent on the corresponding Oracle resource.

3   Set the Critical attribute to False if the Oracle service group must not fail over when the GenericService resource faults.

Refer to the *Veritas Cluster Server Administrator's Guide* for configuration instructions.

Verifying the Oracle service group configuration

This section provides steps to verify an Oracle service group configuration by bringing the service group online, taking it offline, and switching the service group to another cluster node.

Bringing the service group online

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

To bring a service group online from the Java Console

1   In the Cluster Explorer configuration tree, select the Oracle service group to be taken online.

2   Right-click the service group and select to online the service group on the system. (Right-click > Online > *system_name*)

To bring a service group online from the Web Console

1   On the **Service Group** page (**Cluster Summary > All Groups > Service Group**), click **Online**.

2   In the Online Group dialog box, select the system on which to bring the service group online.

3   To run PreOnline script, select the **Run PreOnline Script** check box.

4   Click **OK**.

Taking the service group offline

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

To take a service group offline from the Java Console

1   On the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group.
or
Select the cluster in the Cluster Explorer configuration tree, select the **Service Groups** tab, and right-click the service group icon in the view panel.

2   Choose **Offline**, and choose the appropriate system from the pop-up menu. (Right-click > Offline > *system_name*)

To take a service group offline from the Web Console

1   On the **Service Group** page (**Cluster Summary > All Groups > Service Group**), click **Offline**. This opens the Offline Group dialog box.

2   Select the system on which to take the service group offline.

3   Click **OK**.

Switching the service group

The process of switching a service group involves taking it offline on its current system and bringing it online on another system.

To switch a service group from the Java Console

1   In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group.
     or
     Select the cluster in the Cluster Explorer configuration tree, select the Service Groups tab, and right-click the service group icon in the view panel.

2   Choose **Switch To**, and choose the appropriate system from the pop-up menu. (Right-click > Switch To > *system_name*)

To switch a service group from the Web Console

1   From the Service Group page (**Cluster Summary > All Groups > Service Group**), click **Switch**.

2   In the Switch Group dialog box, select the system to switch the service group to.

3   Click **OK**.

Disabling the service group

To disable the agent, you must change the Oracle service group to an OFFLINE state. You can stop the application completely or switch the agent to another system.

To disable a service group from the Java Console

1   In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group.
     or
     Select the cluster in the Cluster Explorer configuration tree, select the **Service Groups** tab, and right-click the service group icon in the view panel.

2   Choose **Disable**, and choose the appropriate system from the pop-up menu.

To disable a service group from the Web Console

1   In the **Service Group** page (**Cluster Summary > All Groups > Service Group**), click **Disable**. This opens the Disable Group dialog box.

2   Select the system on which to disable the service group. To disable the service group on all systems, click **All Systems**.

Administering the Oracle service group

This chapter describes the administrative tasks you can perform on Oracle service groups such as modifying the service group configuration and deleting a service group. The chapter also describes steps to configure detail monitoring for an Oracle database.

Modifying an Oracle service group

The following steps describe how to modify the configuration of the service groups using the configuration wizard.

Prerequisites

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

  You can however enable and disable the SIDs and listeners to be monitored in detail and change their detail monitoring options when the Oracle service group is online.

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

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

Instructions

To modify an Oracle service group

1   Start the Oracle configuration wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Database Agent for Oracle > Oracle Configuration Wizard**.

2   Review the prerequisites and click **Next**.

3   In the Wizard Options panel, click **Modify service group**, select the service group to modify, and click **Next**.

4   Follow the wizard instructions and make desired modifications to the service group configuration.
     See "Configuring the agent using the Oracle Agent Configuration Wizard" on page 66 for instructions.

Deleting an Oracle service group

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

To delete an Oracle service group

1   Start the Oracle configuration wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Database Agent for Oracle > Oracle Configuration Wizard**.

2   Review the prerequisites and click **Next**.

3   In the Wizard Options panel, click **Delete service group**, select the service group to delete, and click **Next**.

4   In the Service Group Summary panel, click **Next**.

5   On the message that informs you that the wizard will run commands to delete the service group, click **Yes** to delete the service group and then click **Finish**.

Configuring detail monitoring

Use the detail monitoring capability of VCS for NetApp SnapMirror Database agent for Oracle to monitor the status of a database. Before setting up detail monitoring, you must have the agent running at the basic level of monitoring, that is, the DetailMonitor attribute must be set to 0.

The Oracle agent uses a script to monitor the status of the database. A sample SQL script, located at `%VCS_HOME%\bin\Oracle\check.sql`, is provided with the agent for the purpose. If the script is successfully executed during monitoring, the agent considers the database instance available. If the execution fails, the database instance is considered not available and the service group faults and fails over to the failover nodes. You can customize the script to meet your configuration requirements.

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

Enabling detail monitoring

The following steps describe how to enable detail monitoring using the configuration wizard.

To enable detail monitoring

1 Start the Oracle configuration wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Database Agent for Oracle > Oracle Configuration Wizard**.

2 Review the prerequisites and click **Next**.

3 In the Wizard Options panel, click **Modify service group**, select the service group configured for the instance to be monitored in detail, and click **Next**.

4 In the Oracle Configuration panel, select the SIDs to be configured along with their respective listeners and click **Next**.

5   In the Detail Monitoring dialog box, specify information to enable detail
    monitoring, and click **Next**.
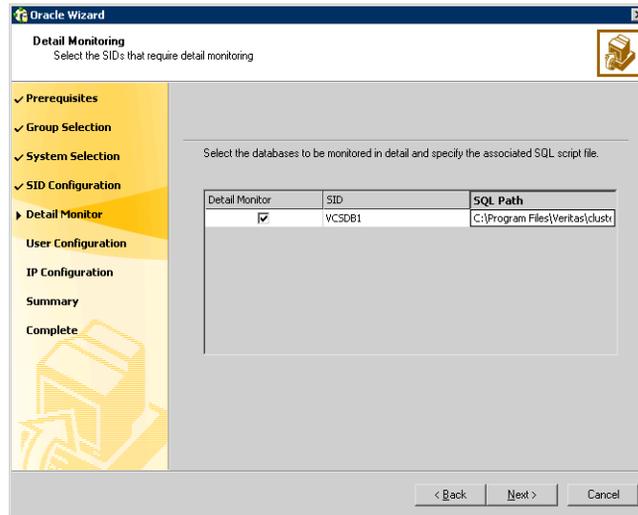
Detail Monitor	Check the Detail Monitor option corresponding to each database that you want to configure detail monitoring for.
SQL Path	Type the path of the SQL file that will query the database to validate the status. Click the icon next to the field to browse for the SQL file. A sample SQL file, check.sql, is located at `%VCS_HOME%\bin\Oracle\`.

6   In the Domain and User selection panel, type a valid domain name, user
    name, password, and then click **Next**.

7   Follow the wizard instructions and accept the default values in the
    subsequent dialog boxes.
    See "Configuring the agent using the Oracle Agent Configuration Wizard"
    on page 66 for instructions.

Disabling detail monitoring

The following steps describe how to disable detail monitoring using the configuration wizard.

To disable detail monitoring

1   Start the Oracle configuration wizard. Click **Start > All Programs > Symantec > Veritas Cluster Server > Configuration Wizards > Database Agent for Oracle > Oracle Configuration Wizard**.

2   Review the prerequisites and click **Next**.

3   In the Wizard Options panel, click **Modify service group**, select the service group configured for the instance for which detail monitoring is being disabled, and click **Next**.

4   In the Oracle Configuration panel, click **Next**.

5   In the Detail Monitoring Configuration panel, uncheck the check box corresponding to the Oracle Server instance for which detail monitoring is being disabled and click **Next**.

6   Follow the wizard instructions and accept the default values in the subsequent dialog boxes.
    See "Configuring the agent using the Oracle Agent Configuration Wizard" on page 66 for instructions.

Troubleshooting the agents

This chapter lists some commonly encountered problems with the Oracle agent and some possible solutions. It also lists the error messages associated with the VCS for NetApp SnapMirror Database agent for Oracle. Each message includes a description and a recommended solution, if applicable.

Troubleshooting common problems

Occasionally you may encounter problems when using the Oracle database agent. Table 6-1 describes the most common problems and provides standard workarounds.

Table 6-1 Common problems when using Oracle database agent

Error	Description
The Oracle service starts, but does not start the database.	Make sure the Oracle database parameter `startmode` is set to `auto`. Make sure the path of the initialization file is set correctly. Verify access to the shared virtual disk.
Clients cannot connect to the virtual IP address set for the service group.	Make sure that the listener service is running. Verify that the listener is configured with virtual IP address in the host location.
Clients get disconnected during failover.	Configure Transparent Application Failover (TAF) for the client in the `tnsnames.ora` file. For more information on TAF, see the Oracle documentation.

Table 6-1   Common problems when using Oracle database agent (Continued)

Error	Description
Resource returns offline during detail monitoring.	This could occur because the database is offline or has not been mounted or opened properly. Check the error in the log file for further details. Verify the configuration definition of the agent. Make sure that the correct file name is specified in the configuration. Verify access to sqlplus from the command prompt.
The sqlplus script cannot be run because sqlplus returns a process error.	If the script timed out, increase the timeout value set in the attribute SQLTimeOut. Otherwise, try recreating the Oracle service using the `oradim` utility.
The Oracle wizard could not locate PFILE or SPFILE for a database.	Make sure the initialization file settings are configured correctly. See "Verifying the initialization file settings" on page 62.
Could not locate the PFILE entry in the registry.	Recreate the registry entry by running the following command: `%ORACLE_HOME%\bin\oradim -edit -sid ` *SID* `-pfile "initialization_file"`

The Oracle service starts, but the database does not start when a non-default SPFILE is used.	Start the database using the command-line.
	1 Start SQL*Plus.
	   `sqlplus /nolog`
	2 Connect to the database as SYSDBA.
	   `connect username/password as sysdba`
	3 Type:
	   `startup pfile="`*initialization_file*`"`
	   The variable *initialization_file* represents the name of the PFILE that you created to point to the non-default SPFILE on the shared virtual disk. See "Moving the initialization file to shared virtual disks (Oracle 10g)" on page 60.
	   You must specify the fully qualified path of the file, along with its name.
	4 If the database is mounted and does not open, type:
	   `alter database open;`
	
	Refer to the Oracle documentation for more information.

Table 6-1   Common problems when using Oracle database agent (Continued)

Error	Description
Listener service does not start after configuring the virtual IP address.	Make sure the virtual IP address is configured correctly for the listeners.
	Another possible cause is that the listener.ora file is corrupted.
	Solution:
	1 Stop the listener services on the node.
	2 Rename the listener.ora file.
	3 Recreate the listeners using the Net Configuration Assistant.
	4 Bring up the virtual IP on the node.
	5 Configure the virtual IP address for the newly created listeners using the Net Manager.
	6 Restart the listener services.
	7 Run `lsnrctl status` command for each listener to verify the virtual IP address.
	Refer to the Oracle documentation for instructions on using the Net Configuration Assistant and the Net Manager.
The VRTSWeb service does not start.	Make sure the path of the Perl package installed by Veritas appears as the first entry in the definition of the PERL5LIB environment variable.
	See "To modify the path of the Perl variable" on page 53 for instructions.

VCS logging

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

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

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

A typical agent log resembles:

```
2005/05/10 09:32:44 VCS NOTICE V-16-20046-5 Oracle:
Oracle-DATA1:online:Service status is Running
```

Here,

- Timestamp denotes the date and time when the message was logged.

- Mnemonic denotes which Symantec product logs the message. For VCS for NetApp SnapMirror Database agent for Oracle, mnemonic is 'VCS'.

- Severity denotes the seriousness of the message. Severity of the VCS error messages is classified into the following types:

  - CRITICAL indicates a critical error within a VCS process. Contact Technical Support immediately.

  - ERROR indicates failure of a cluster component, unanticipated state change, or termination or unsuccessful completion of a VCS action.

  - WARNING indicates a warning or error, but not an actual fault.

  - NOTE informs the user that VCS has initiated an action.

  - INFO informs the user of various state messages or comments.
    Of these, CRITICAL, ERROR, and WARNING indicate actual errors. NOTE and INFO provide additional information.

- UMI or Unique Message ID is a combination of Originator ID, Category ID, and Message ID. For example, the UMI for a message generated by the Oracle agent would resemble: `V-16-20046-5`
  Originator ID for all VCS products is 'V-16.' Category ID for Oracle agent is 20046, for Netlsnr agent is 20047. Message ID is a unique number assigned to the message text.

- Message text denotes the actual message string.

You can view these message logs using Notepad or any text editor. All messages are logged to the engine and the agent logs. Messages of type CRITICAL and ERROR are written to the Windows event log.

VCW logs

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

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

The format of the VCW log is

ThreadID | Message Text

- *ThreadID*: the ID of the thread initiated by VCW.

- *Message Text*: the actual message generated by VCW.

A typical VCW log resembles:

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

VCWsilent logs

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

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

A typical VCWsilent log resembles:

```
00005540-00000064: 5540: STARTING - Discovering NICs on the
selected machines...
00009956-00000064: 9956: STARTING - Generating private network
related files...
00009956-00000048: 9956: COMPLETED - Gererating LLT host
files...
00009956-00000048: 9956: COMPLETED - Generating GAB tab files...
00009956-00000048: 9956: COMPLETED - Generating main.cf file...
00009956-00000064: 9956: STARTING - Configuring LLT on all the
nodes.
00009956-00000048: 9956: COMPLETED - Configuring LLT on all the
nodes.
```

Agent error messages and descriptions

Table 6-2 and Table 6-3 lists the messages of type ERROR and WARNING. Each message includes a description and a recommended solution, if applicable.

Oracle agent

Table 6-2   Oracle agent error messages

Message	Description
Cannot open service handle.	The agent could not open the Service Control Manager handle. This may occur because of an invalid service name. Solution: Verify that the correct service name is specified in the configuration definition of the agent.
Cannot close service handle.	The agent could not close the Service Control Manager handle. Solution: Verify that the specified service is running.
Cannot start service.	The agent could not start the specified service. This may occur because of the following: ■ The specified SCM handle does not have access to the service. or ■ The specified handle is invalid. Solution: Verify that the service name in the configuration file is the same as the name displayed by the SCM. Verify that the specified service is supported by the host. Verify that the service is listed in the SCM window.
Cannot stop the service.	The agent could not stop the specified service. This may occur because of the following: ■ The specified service was not opened successfully. or ■ The specified service was not opened with the required access. Solution: Verify that the service was opened successfully. Check the access with which the service was opened.

Table 6-2 Oracle agent error messages (Continued)

Message	Description
Wait for mutex failed.	The wait function for mutex failed. This message is followed by an error code. Check the error code for more information.
Wait for mutex abandoned.	The mutex object is was not released by the thread that owned the mutex object before the thread terminated. This indicates a possibility that the SQL script is not terminated. Solution: Verify that the SQL script executed correctly.
Cannot wait for mutex object.	The agent could not acquire mutex for the resource. This may occur if two or more Oracle resources configured. Solution: Verify that the SQL script executed correctly.
Failed to decrypt password.	The agent could not decrypt the domain password. Solution: Verify that the password was encrypted using the VCS Encrypt utility.
No domain specified in argument list.	The attribute Domain is not configured for the resource. Solution: Verify that the correct Domain is defined in the configuration file.
No username specified in argument list.	The attribute UserName is not configured for the resource. Solution: Verify that the correct UserName is defined in the configuration file.
No password specified in argument list.	The attribute Password is not configured for the resource. Solution: Verify that the password is encrypted using the VCS Encrypt utility. Verify that the correct encrypted password is defined in the configuration file.
No SID specified in argument list.	The configuration definition of the agent does not contain a value for the attribute SID. Solution: Verify that the attribute SID is correctly defined in the configuration file.
SQL*Plus process exited with error *error_code*.	The agent could not execute the SQL*Plus process correctly. See the associated error code for more information.

Table 6-2 Oracle agent error messages (Continued)

Message	Description
Invalid filename in argument list *file_name*.	The SQL script for the resource is incorrectly defined in the filename. Solution: Verify that the attribute SQLFile is correctly defined in the configuration file. Verify the validity of the file name and path.
An Oracle error occurred.	An error occurred while generating the SQL script. This is an Oracle error and the corresponding error number and error message is logged to the agent log.

NetIsnr agent

Table 6-3 NetIsnr agent error messages

Message	Description
Cannot open service handle.	The agent could not open the Service Control Manager handle. This may occur because of an invalid service name. Solution: Verify that the correct service name is specified in the configuration definition of the agent.
Cannot start service.	The agent could not start the specified service. This may occur because of the following: ■ The specified SCM handle does not have access to the service. or ■ The specified handle is invalid. Solution: Verify that the service name in the configuration file is the same as the name displayed by the SCM. Verify that the specified service is supported by the host. Verify that the service is listed in the SCM window.

Table 6-3   NetIsnr agent error messages (Continued)

Message	Description
Cannot stop the service.	The agent could not stop the specified service. This may occur because of the following: ■ The specified service was not opened successfully. ■ The specified service was not opened with the required access. Solution: Verify that the service was opened successfully. Check the access with which the service was opened.
Cannot close service handle.	The agent could not close the Service Control Manager handle. Solution: Verify that the specified service is running.

NetApp agents

This section describes the error messages for the NetApp agents.

Table 6-4   NetApp agents error messages

Message	Description
Failed to open connection to filer *%s*.	Make sure that the VCS Helper service account is part of the administrator's group on the local host and the filer. Make sure the private network is functioning properly. Verify you can ping the IP used for the private storage network. This is the IP defined the StorageIP attribute of the NetAppFiler resource.
Failed to initialize ONTAPI on system	The agent could not find the file NTAPADMIN.DLL on the system. Verify the file exists in the %*VCS_HOME*%\bin directory
Invalid attributes exist in the configuration	Some agent attributes have not been defined or have been defined incorrectly. Verify the configuration definition for the agent.

Table 6-4 NetApp agents error messages (Continued)

Message	Description
ONTAP API called failed for *object_name* on *filer_name*.	The specified API failed on the specified object. See the NetApp ONTAP API documentation for information about the associated error message
Volume *%s* on filer *%s* is not a SnapMirror replicated volume	Verify replication is set up on the specified volume.
Multiple snapmirror destinations for a volume is not supported by this agent. 'snapmirror status' for volume %s on filer %s returned multiple status entries. Administrative intervention required	There should be only one destination per source volume.
Initialize VLibNetAppHost::Initialize() failed. (error_type: *%s*, error_code: *0x%s*)	The agent could not detect the iSCSI or FC Initiator on the host. Make sure that you have installed and configured Microsoft iSCSI Initiator or an FC Initiator on each node.
Failed to connect/disconnect virtual disk. (error_type: *%s*, error_code: *0x%s*. error_message: *%s*)	This could occur because one or more of the following parameters are defined incorrectly in the VCS configuration: ■ Filer name ■ Volume name/LUN name ■ Share name ■ Storage IP Verify the configuration definition of the resource. Make sure each attribute is defined correctly.
Unable to create/delete online lock file *%s*. Error code *%s*,	Make sure you have write permissions on the specified directory.

Resource type definitions

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

Oracle agent

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

Resource type definition

```
type Oracle (
    static keylist LogDbg = { DBG_1 }
    static i18nstr ArgList[] = { ServiceName, DelayAfterOnline,
        DelayAfterOffline, DetailMonitor, IndepthMonitorCount, SID,
        Domain, UserName, EncryptedPasswd, SQLFile, SQLTimeOut }
    str ServiceName
    int DelayAfterOnline = 20
    int DelayAfterOffline = 20
    boolean DetailMonitor = 0
    int IndepthMonitorCount = 5
    str SID
    str Domain
    str UserName
    str EncryptedPasswd
    str SQLFile
    int SQLTimeOut = 20
)
```

Attribute definitions

Table A-1   Oracle agent - required attributes

Required Attribute	Type and Dimension	Definition
ServiceName	string-scalar	The name of the Oracle service set during the installation of Oracle. The service name is specified in the format OracleServiceSID, where SID represents the database instance.
Domain	string-scalar	The name of the domain to which the user belongs in whose context Oracle was installed.
SID	string-scalar	A system identifier that uniquely identifies the Oracle database instance to be monitored in detail.
UserName	string-scalar	The name of the domain user in whose context Oracle was installed.
EncryptedPasswd	string-scalar	The encrypted password for the user identified by UserName. The password must be encrypted with the VCS Encrypt utility.

Table A-2   Oracle agent - optional attributes

Optional Attributes	Type and Dimension	Definition
DelayAfterOffline	integer-scalar	Number of seconds the agent waits to start the monitoring routine after Oracle is taken offline. Default = 20
DelayAfterOnline	integer-scalar	Number of seconds the agent waits to start the monitoring routine after Oracle is brought online. Default = 20

Table A-2   Oracle agent - optional attributes (Continued)

Optional Attributes	Type and Dimension	Definition
DetailMonitor	boolean-scalar	A flag that defines whether the agent monitors Oracle in detail by trying to verify access to the database by running a SQL script. The value 1 indicates that the agent will monitor Oracle in detail. The value 0 indicates that the agent will not. Default = 0 If the DetailMonitor flag is set to 1, the following attributes must be defined: ■ SID ■ SQLFile
IndepthMonitorCount	integer-scalar	An integer that defines the monitor interval between two consecutive detail monitoring cycles. If this attribute is set to 5, the agent monitors the application in detail after every five monitor intervals. Default = 5
SQLTimeOut	integer-scalar	The number of seconds the agent waits for the SQL script to return a value during detail monitoring. If this limit exceeds, the resource is declared faulted. Default = 20
SQLFile	string-scalar	The name of SQL script to be used for detail monitoring, along with its complete path. The agent verifies the existence of this file. A sample file, check.sql, is located at *%VCS_HOME%\bin\Oracle*. The sample file contents are: `    select * from v$database;` Do not include any spool commands within the SQL script. If an Oracle error occurs during execution, the error is logged to the agent log. If debug logging is also enabled for the resource, the output of the SQL script is also logged to the agent log.

NetIsnr agent

The NetInr agent is configured as a resource of type NetIsnr.

Resource type definition

```
type Netlsnr (
    static i18nstr ArgList[] = { ServiceName, DelayAfterOnline,
        DelayAfterOffline }
    str ServiceName
    int DelayAfterOnline = 20
    int DelayAfterOffline = 20
)
```

Attribute definitions

Table A-3   NetIsnr agent - required attributes

Required Attribute	Type and Dimension	Definition
ServiceName	string-scalar	The name of the configured listener service.
		The service name is specified in the format Oracle*OraHome*TNS*ListenerName*, where *OraHome* represents the Oracle home set during the installation and *ListenerName* represents the name of the configured listener.

Table A-4   NetIsnr agent - optional attributes

Optional Attributes	Type and Dimension	Definition
DelayAfterOffline	integer-scalar	Number of seconds the agent waits to start the monitor routine after the listener is taken offline. Default = 20
DelayAfterOnline	integer-scalar	Number of seconds the agent waits to start the monitor routine after the listener is brought online. Default = 20

NetAppFiler agent

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

Resource type definition

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

Attribute definitions

Table A-5   NetApp Filer agent attributes

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

NetApp SnapDrive agent

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

Resource type definition

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

Attribute definitions

Table A-6   NetApp SnapDrive agent attributes

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

NetApp SnapMirror agent

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

Resource type definition

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

Attribute definitions

Table A-7   NetApp SnapMirror agent attributes

Attribute	Type - Dimension	Description
FilerResName	string-scalar	Name of the VCS NetAppFiler-type resource in the group.
VolumeName	string-scalar	Name of the filer volume that is to be mounted via iSCSI. Define the volume name in the same case as on the filer.
SnapMirrorArguments	string-scalar	Specifies the SnapMirror arguments such as maximum transfer speed and restart mode.

Table A-7   NetApp SnapMirror agent attributes (Continued)

| Attribute	Type - Dimension	Description
SnapMirrorSchedule	string-scalar	Specifies the schedule the destination uses for updating data. Do not assign a value for this attribute if you use SnapManager. By default, this attribute does not have any value.
AppResName	string-scalar	Name of the resource configured to monitor the application being made highly available.

Sample configuration

This appendix describes a typical service group configured to monitor the state of Oracle in a VCS cluster. The sample dependency graph depicts the resource types, resources, and resource dependencies within the service group. The sample configuration file (main.cf) is also included for your reference. Review the dependency carefully before configuring the agent. For more information about VCS resource types, see the *Veritas Cluster Server Bundled Agents Reference Guide.*

Resource dependency graph

In the sample configuration shown in the dependency graph below, the shared virtual disk group is configured using the NetAppFiler agent. The shared volume on which Oracle shared data is installed is mounted as drive G:\ using the NetappSnapDrive agent. The service group IP address for the server is configured using the IP and NIC resource types. The Oracle resource can be started after each of these resources is brought online.

Figure B-1   Sample Oracle service group resource dependency graph
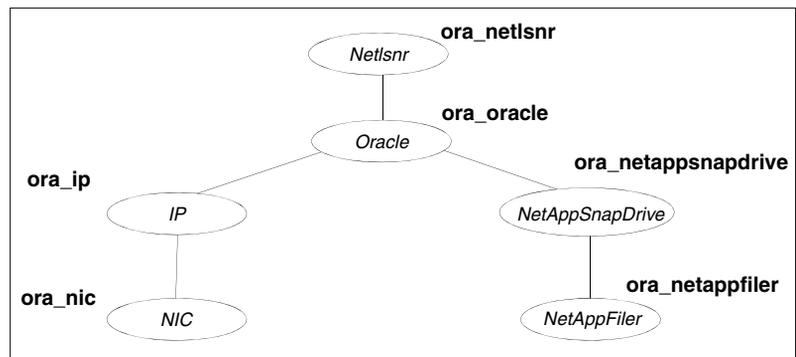
Sample configuration file

Sample configuration files are provided for your reference.

Sample configuration file using iSCSI initiator

```
    include "types.cf"

cluster merlin285-286 (
    SecureClus = 1
    )
system VCSNET285 (
    )
system VCSNET286 (
    )
group ora-iscsi (
    SystemList = { VCSNET285 = 0, VCSNET286 = 1 }
    )
    IP ora-iscsi-IP (
        Address = "10.255.254.253"
        SubNetMask = "255.255.255.0"
        MACAddress @VCSNET285 = "00-11-43-DD-F3-96"
        MACAddress @VCSNET286 = "00-11-43-DD-F4-5F"
        )

    NIC ora-iscsi-NIC (
        MACAddress @VCSNET285 = "00-11-43-DD-F3-96"
        MACAddress @VCSNET286 = "00-11-43-DD-F4-5F"
        )

    NetAppFiler ora-iscsi-NetAppFiler (
        FilerName = vcsnetapp1
        StorageIP = "10.255.254.252"
        )

    NetAppSnapDrive ora-iscsi-NetAppSnapDrive (
        FilerResName = ora-iscsi-NetAppFiler
        VolumeName = vol1
        ShareName = data01
        LUN = "sri1.lun"
        MountPath = M
        Initiator @VCSNET285 = {
"iqn.1991-05.com.microsoft:vcsnet285.zen.com" }
        Initiator @VCSNET286 = {
"iqn.1991-05.com.microsoft:vcsnet286.zen.com" }
        )

    Netlsnr Netlsnr-LISTENER (
        ServiceName = OracleOraDb10g_home1TNSListener
        )
```

```
    Oracle Oracle-MerlinA (
        ServiceName = OracleServiceMerlinA
        DetailMonitor = 1
        Domain = zen
        SID = MerlinA
        UserName = Administrator
        EncryptedPasswd = fnsRktHrrRorTnfLglHli
        SQLFile = "C:\\Program Files\\Veritas\\cluster
server\\bin\\Oracle\\check.SQL"
        )

    Oracle-MerlinA requires ora-iscsi-NetAppSnapDrive
    Oracle-MerlinA requires ora-iscsi-IP
    Netlsnr-LISTENER requires Oracle-MerlinA
    ora-iscsi-NetAppSnapDrive requires ora-iscsi-NetAppFiler
    ora-iscsi-IP requires ora-iscsi-NIC
```

Sample configuration file using FC initiator

```
include "types.cf"

cluster merlin277 (
    SecureClus = 1
    )

system VCSNET277 (
    )

system VCSNET278 (
    )

group ora-fc (
    SystemList = { VCSNET277 = 0, VCSNET278 = 1 }
    )

    IP ora-fc-IP (
        Address = "10.255.254.253"
        SubNetMask = "255.255.255.0"
        MACAddress @VCSNET277 = "00-11-43-33-1B-07"
        MACAddress @VCSNET278 = "00-11-43-33-1B-60"
        )

    NIC ora-fc-NIC (
        MACAddress @VCSNET277 = "00-11-43-33-1B-07"
        MACAddress @VCSNET278 = "00-11-43-33-1B-60"
        )

    NetAppFiler ora-fc-NetAppFiler (
        FilerName = vcsnetapp1
```

```
            StorageIP = "10.255.254.252"
            )

    NetAppSnapDrive ora-fc-NetAppSnapDrive (
        FilerResName = ora-fc-NetAppFiler
        VolumeName = vol1
        ShareName = data01
        LUN = "sri3.lun"
        MountPath = K
        Initiator @VCSNET277 = { "21:00:00:e0:8b:19:bf:eb" }
        Initiator @VCSNET278 = { "21:00:00:e0:8b:19:d0:30" }
        )

    Netlsnr Netlsnr-LISTENER (
        ServiceName = OracleOraDb10g_home1TNSListener
        )

    Oracle Oracle-MerlinB (
        ServiceName = OracleServiceMerlinB
        DetailMonitor = 1
        Domain = zen
        SID = MerlinB
        UserName = Administrator
        EncryptedPasswd = ckpOhqEooOloQkcIdiEif
        SQLFile = "C:\\Program Files\\Veritas\\cluster
server\\bin\\Oracle\\check.SQL"
        )

    Oracle-MerlinB requires ora-fc-NetAppSnapDrive
    Oracle-MerlinB requires ora-fc-IP
    Netlsnr-LISTENER requires Oracle-MerlinB
    ora-fc-NetAppSnapDrive requires ora-fc-NetAppFiler
    ora-fc-IP requires ora-fc-NIC
```

Oracle Enterprise Manager 10g Grid Control with VCS

Oracle Enterprise Manager (OEM) 10g allows users to manage Oracle components, including Oracle databases, through the Grid Control Management interface.

This appendix covers general instructions on how to install the Oracle 10g Grid Control Management Agent, and detailed step-by-step instructions on how to set up the Oracle Enterprise Manager 10g Grid Control to enable users to manage Oracle databases from the Oracle Enterprise Manager console, in a VCS cluster.

Supported software and operating system

- Oracle 10g, Release 2 (10.2.0.1.0) Standard Edition or Enterprise Edition with
  Windows 2000 Server, Advanced Server, or Datacenter Server (all require Service Pack 4 with Update Rollup 1)
  or
  Windows Server 2003 (Standard Edition, Enterprise Edition, or Datacenter Edition) (SP 1 required, SP2 supported, but not required for all editions)

- Oracle Enterprise Manager 10*g* Grid Control Release 10.1.0.3

Note: VCS support for Oracle is limited to 32-bit versions of the operating system.

Installation and configuration tasks

Perform the following steps to configure Oracle Enterprise Manager 10g Grid Control to monitor databases in a VCS environment:

- Install the Oracle Enterprise Manager.
  See "Installing Oracle Enterprise Manager server" on page 107.

- Install Oracle binaries.
  See "Installing Oracle" on page 107.

- Install the Oracle Management Agent.
  See "Installing the Oracle management agent" on page 107.

- Create and configure the Oracle database and listener.
  See "Creating and configuring Oracle database and listener" on page 108.

- Add the Lanman resource for the virtual network name and bring it online.
  See "Configuring a virtual network name" on page 109.

- Configure the listener for the virtual network name.
  See "Configuring the listener for virtual network name" on page 110.

- Configure the database service for the virtual network name.
  See "Configuring the database service for virtual network name" on page 110.

- Configure an additional Oracle Management Agent listening on a virtual network name.
  See "Configuring an additional Oracle management agent" on page 112.

- Add the database to the Oracle Enterprise Manager 10g Grid Control.
  See "Adding the database to the OEM 10g Grid Control" on page 112.

- Add a GenericService resource for the Additional Management Agent.
  See "Making the additional agent highly available" on page 114.

Installing Oracle Enterprise Manager server

Install the Enterprise Manager server on a separate server. The Enterprise Manager server should not be a part of the cluster.

To install the Enterprise Manager server

1   From the Oracle Enterprise Manager CD, double-click Setup.exe to launch the Oracle Universal Installer.

2   On the Welcome panel, click **Next**.

3   On the Specify File Locations panel, specify the appropriate paths required for the installation and click **Next**.

4   On the Select a Product to Install panel, choose **Enterprise Manager 10g Grid Control Using a New Database 10.1.0.3.0** and click **Next**.

5   Follow the instructions of the installer. Refer to the Oracle product documentation for more information. At the end of the installation, make a note of the information displayed on the Summary page. You may need this information to complete the configuration.

Installing Oracle

Install Oracle on all the cluster nodes. After the Oracle installation is complete, verify if the Oracle home path (the path that you set while installing Oracle) is included in the Path environment variable. If not, then you have to manually add the Oracle home entry to the Path variable, on all the cluster nodes.

To add the oracle home to the Path variable

1   Right-click **My Computers** and click **Properties**.

2   In the **System Properties** window, click the **Advanced** tab.

3   Click **Environment Variables**.

4   In the **System Variables** area of the Environment Variables window, double-click the Path variable name to edit it.

5   In the **Variable Value** field, add the Oracle home path.

6   Repeat steps 1 to 5 on all the cluster nodes.

Installing the Oracle management agent

Install the Oracle Management Agent on all the cluster nodes under the same Oracle home path.

To install the Oracle Management Agent

1   From the Oracle Enterprise Manager CD, double-click Setup.exe to launch the Oracle Universal Installer.

2   On the Welcome panel, click **Next**.

3   On the Specify File Locations panel, specify the appropriate paths required for the installation and click **Next**.

4   On the Select a Product to Install panel, choose **Additional Management Agent 10.1.0.3.0** and click **Next**.

5   On the Specify Oracle Management Service Location panel, specify the host name (the Enterprise Manager Server name) and the port (default port) that the Management Agent should use to communicate with the Enterprise Management service.

6   The installer might display a Warning. Click **OK** to continue.

7   Click **Next**. Follow the instructions of the installer to complete the installation.

8   Repeat steps 1 to 7 on all the cluster nodes.

You must install the Oracle Additional Management Agent under the same Oracle Home Path on all the cluster nodes.

Creating and configuring Oracle database and listener

Before you proceed, ensure that you have installed the VCS Database Agent for Oracle. See "Installing the Oracle agent" on page 43 for instructions.

To create and configure an Oracle database and a listener

1   Create a virtual IP address for the databases and the listeners. See "Creating a virtual IP address" on page 31 for instructions.

2   Create a Listener service. See "Creating the listener service" on page 31 for more instructions.

3   Configure the listener to use the virtual IP address. See "Configuring the listeners to use the virtual IP address" on page 31 for instructions.

4   Use the Oracle Database Configuration Assistant (DBCA) to create the database.

    ■   Start the Database Configuration Assistant (**Start > All Programs > Oracle-*Oracle_Home* > Configuration and Migration Tools > Database Configuration Assistant**). This launches the database installer.

- On the Welcome panel, click **Next**.

- On the Operation panel, click **Create a database** and click **Next**.

- On the Database Templates panel, click **Custom Database** and click **Next**.

- On the Management Options panel (Step 4 of 12), choose **Use Grid Control for Database Management**.

- Click **Next**. Follow the installer instructions and select other options as per your desired database configuration. See "Creating the database on shared disks" on page 29 for instructions.

5   Configure the database on the shared virtual disk.
    See "Configuring the databases" on page 57.
    Note that while configuring the Log On properties of the Oracle and Listener services, you must choose the **Local System Account** option instead of **This Account**.

6   Repeat step 1 to step 5 on all the cluster nodes.

7   Configure the Oracle Service group.
    See "Configuring the Oracle service group" on page 65 for more information.

Configuring a virtual network name

See the *Veritas Cluster Server Administrator's Guide* for more information on how to create a resource, bring the resource online, and link a resource.

To configure a virtual network name

1   Create a Lanman resource with the virtual server name.

2   Specify the attribute IPResName. The value of this attribute should be the IP resource name of the service group.
    Resource names are case-sensitive in VCS.

3   Create a dependency with the Lanman resource as the parent resource and the IP resource as the child resource.

4   Enable the Lanman resource and bring it online. This will bring the virtual network name online.

5   Create a dependency with the Oracle resource as the parent resource and the Lanman resource as the child resource.

6   Remove the dependency between the Oracle resource and the IP resource.

Configuring the listener for virtual network name

Perform these steps on all the cluster nodes. Ensure that the service group is online on the node on which you perform these steps.

To configure the listener for the virtual network name

1   Offline the listener service resource on the node.

2   In the listener.ora file, change the host name to the network name from the Lanman resource that you created.
    Replace
    `HOST=`*`virtual_IP_address`*
    with
    `HOST=`*`network_name`*
    The default location of the file listener.ora is
    `%`*`ORACLE_HOME`*`%\NETWORK\ADMIN\`.

3   Remove the database entries in SID_LIST, if any.

4   Save and close the configuration.

5   Online the listener service resource on the node.

Configuring the database service for virtual network name

Perform these steps to configure the database service for the virtual network name.

To configure the database service for virtual network name

1   If the file "tnsnames.ora" does not contain entries for Database Service and Network Name, then create these entries using the Net Configuration Assistant. You must create these entries on all the cluster nodes.

2   Associate the database with the listener.
    ■   Ensure that the initialization parameter file contains the following entries:
        ■   SERVICE_NAMES (the name of the database service)
        ■   INSTANCE_NAME (the name of the database instance)
        Example SQL queries to ensure these entries:

```
show parameter INSTANCE_NAME
show parameter SERVICE_NAME
```
    These parameters are created during installation or database creation.

■   Use one of the following ways to configure the new attribute listener_alias:

Run the following SQL command:

```
SQL> ALTER SYSTEM SET
LOCAL_LISTENER='<listener_alias>' scope=spfile;
```

OR

Add the following entry to the initialization parameter file (pfile/spfile):

```
LOCAL_LISTENER = <listener_alias>
```

■   Define the parameter listener_alias. If your Oracle configuration uses the file tnsnames.ora, edit the file as instructed below. The default location of tnsnames.ora is `%ORACLE_HOME%\NETWORK\ADMIN`.

Add the following to tnsnames.ora file:

<listener_alias>=
(DESCRIPTION =
(ADDRESS=(Protocol=TCP)(HOST=virtual_name)(Port=default port))
)

The listener_alias parameter gets appended by the default domain name specified in the file sqlnet.ora.

■   Offline, and then online, the listener service, and database service resources.

3   Edit the initialization parameter file. For the dispatchers parameter, replace the virtual IP address with virtual name for dispatchers. See   for more information.

Configuring an additional Oracle management agent

Configure an additional Oracle Management Agent for the virtual server. Note that this agent is in addition to the agent that you installed earlier. The agent that you installed in "Installing the Oracle management agent" on page 107 is for the physical node, and this agent is for the virtual host.

Perform these steps on all the nodes. Make sure that the Oracle service group is online on the node on which you perform these steps.

To configure an additional Oracle Management Agent

1   At the command prompt, type the following commands:

   ■   `C:\> cd [Management Agent home]/bin`

   ■   `C:\[Management Agent home]/bin>emctl deploy agent`
        `[-n WindowsServiceName]`
        `AGENTSTATE_dir AGENTSTATE_hostname:port`
        `DeployHostName:port`
        Where,
        WindowsServiceName: the new service which is used for the HA of additional management agent. (We will create a GenericService resource for this later.)
        AGENTSTATE_dir: a new directory
        AGENTSTATE_hostname: virtual host name
        port: a new port
        DeployHostName: physical FQDN of the host
        port: default port
        Example:
        C:\Oracle\product`\10.1.0\em_1\bin>emctl deploy agent -n
        OraEm10gOneVCSHost E:\Oracle\product\10.1.0\em_1\vcshost\
        vcshost:1831 vcsw2h283.vcsnet.com:1830

2   Start the Management Agent service ("OraEm10gOneVCSHost" in the above example) for the management agent and make sure it starts.

3   Stop the Management Agent service on this node.

4   Repeat steps 1 to 3 on the next node.

Adding the database to the OEM 10g Grid Control

Perform these steps to add the database to the OEM 10g Grid Control.

To add the database to the OEM 10g Grid Control

1   Access the OEM Grid control using the following URL:
    http://<EM server.domainName>:7777/em

2   Logon with user as sysman. The Enterprise Management Server will
    discover the virtual network in its target host. You have to remove the
    listener and the database for the physical node and add the listener and
    database for the virtual network name.

3   On the Enterprise Manager console, click **Targets** and then click **All Targets**.

4   Choose the database for the physical node, and click **Remove**. Click **Yes** to
    confirm the database removal. Remove the listener for the physical node in
    a similar way.

5   On the Enterprise Manager console, click **Targets** and then click **Databases**.

6   Click **Add**. The Enterprise Management Server will prompt you to select a
    host for which you want to add the database.

7   Choose the virtual network name and click **Continue**. The Enterprise
    Manager will discover the targets on that machine. Check if the database
    and listener names displayed are the ones that you wish to manage from the
    Enterprise Management Server.

8   Under Databases, click on the tools icon (under Configure) to
    configure the database.

9   Specify the Database name and the Monitor Password. This password is
    later used when you login to the database to monitor it.

10 Click **Next** and follow the instructions to complete the database
    configuration. After you configure the database successfully, the tools icon
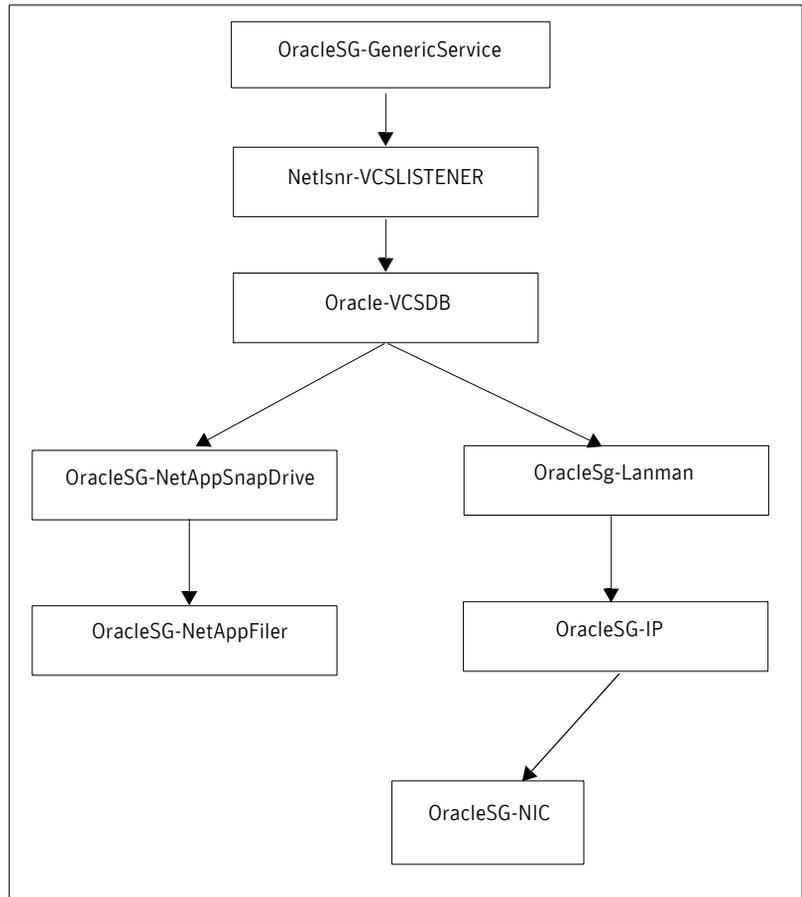   will appear as .

Making the additional agent highly available

Add a GenericService resource to make the additional agent highly available.

To make the additional agent highly available

1 Set the startup type for the additional agent service to Manual, on all the nodes. You must do this before configuring GenericService resource.

2 Create a GenericService resource for the Oracle Management Agent service. (This is the service for the additional agent that you created in "Configuring an additional Oracle management agent" on page 112).

3 Specify the attributes DelayAfterOnline and DelayAfterOffline. Set the value as 30 seconds.
Sometimes the GenericService resource may go into an unknown state. This is because the Oracle agent service takes some time in coming up. The workaround for this is to increase the attributes DelayAfterOnline and DelayAfterOffline, or probe the resource after the Windows service has started.

4 Create a dependency with the GenericService resource as the parent resource and the Netlsnr resource as the child resource.

5 Enable the GenericService resource and bring it online.

Sample Configuration

```
┌─────────────────────────────────────────────────────────────────┐
│                  ┌──────────────────────────────┐                │
│                  │   OracleSG-GenericService    │                │
│                  └──────────────────────────────┘                │
│                                │                                  │
│                                ▼                                  │
│                  ┌──────────────────────────────┐                │
│                  │     NetIsnr-VCSLISTENER       │                │
│                  └──────────────────────────────┘                │
│                                │                                  │
│                                ▼                                  │
│                  ┌──────────────────────────────┐                │
│                  │        Oracle-VCSDB           │                │
│                  └──────────────────────────────┘                │
│                        ╱                 ╲                        │
│                       ▼                   ▼                       │
│       ┌──────────────────────────┐  ┌──────────────────────────┐ │
│       │  OracleSG-NetAppSnapDrive │  │    OracleSg-Lanman        │ │
│       └──────────────────────────┘  └──────────────────────────┘ │
│                     │                            │                │
│                     ▼                            ▼                │
│       ┌──────────────────────────┐  ┌──────────────────────────┐ │
│       │    OracleSG-NetAppFiler   │  │      OracleSG-IP          │ │
│       └──────────────────────────┘  └──────────────────────────┘ │
│                                                  ╲                │
│                                                   ▼               │
│                                     ┌──────────────────────────┐  │
│                                     │      OracleSG-NIC         │  │
│                                     └──────────────────────────┘  │
└─────────────────────────────────────────────────────────────────┘
```

Notes:

■ The sequence in which database and the additional management agent is created is not critical as long as everything is configured with the virtual server.

■ The additional Oracle Management Agent service will not come online till the network name (Lanman) is online on the same node.

■ The Oracle Management Agent (for the physical node) can be online on both the nodes. It's only the additional Oracle Management Agent (for the virtual server) that needs to be online on one of the two nodes as it depends on the virtual network name. So that the host information is always available.

■   Failover time may increase after the Management Agent is added to the VCS cluster group. After Oracle service group is failed over to the other node, the Enterprise Manager agent service should be restarted on the Enterprise Manager Server in order to connect to the database using Enterprise Manager.

Index