Veritas™ Cluster Server One Installation Guide

AIX, HP-UX, Linux, Solaris

5.0

Veritas Cluster Server One Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.0

Document version: 5.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

http://www.symantec.com/business/support/assistance_care.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:

- Error messages and log files
- Troubleshooting that was performed before contacting Symantec
- Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to clustering_docs@symantec.com.

Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting.

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 6 Installing the Simulator

Chapter 7 Setting up authentication plug-ins for VCS One

Chapter 8 Adding shared storage and testing disks for SCSI-3 compliance

Chapter 9 Adding a new or replacement system to the Policy Master cluster

Chapter 1

Getting ready to install VCS One

This chapter includes the following topics:

About installing VCS One

Installing Veritas Cluster Server (VCS) One involves the following procedures:

- Setting up the hardware for the Policy Master cluster
- Setting up the network communications among systems
- Setting up Symantec Product Authentication Service (AT)
- Configuring shared storage
- Creating the disk group and file system for VCS One Policy Master database
- Installing the VCS One Policy Master and verifying the installation
- Connecting the VCS One client systems to the Policy Master cluster using the public network
- Installing the VCS One client software on the client systems
- Installing the agents
- Installing the Simulator (optional)
- Testing shared storage devices and coordinator disks for compliance with SCSI-3 persistent reservations
- Configuring I/O Fencing (optional, but recommended)

Installing the VCS One agents

In addition to the agents that are bundled with the product, VCS One provides agents for the management of key enterprise applications. Typically, agents start, stop, and monitor resources and report state changes. The high availability agents are located on the Veritas High Availability Agent Pack software disc that is included with VCS One. The Agent Pack disc contains the currently shipping agents and is released quarterly to add new agents. See the following documentation available on the Agent Pack disc:

- For an overview of the supported high availability agents, read the *Veritas High Availability Agent Pack Getting Started Guide*.
- For installation instructions, read the agent installation and configuration guides.

Getting your VCS One licenses

VCS One is a licensed product.

Table 1-1 lists the VCS One license types.

Table 1-1 VCS One license types

VCS One license type	Description
Demo	A demo license that lets you use the product for 30 days for evaluation purposes only. After 12 months, the product auto-disables high availability (HA) for the Policy Master and significantly reduces functionality.
NFR	A not-for-resale license, limited to one year. Symantec partners and customers use this license for stack certification and testing. After 12 months, the product auto-disables high availability (HA) for the Policy Master and significantly reduces functionality.
Permanent	A permanent license.

Regardless of the license type, the VCS One functional modes are described in Table 1-2.

Table 1-2 VCS One functional modes

VCS One functional modes	Features
VCS One HA	VCS One with all features enabled
VCS One Start	VCS One with all features enabled except: ■ Auto-failover ■ Priority-based application availability VCS One Start lets you manually start, stop, and move applications.

Note: If you choose VCS One Start, you must set the GrpFaultPolicy and NodeFaultPolicy attributes to NoFailover when you create a service group. For information about how to set these attributes when you create a service group, see the *Veritas Cluster Server One User's Guide*.

Setting up the Policy Master cluster hardware

The Policy Master manages the VCS One cluster. You must set up a Policy Master cluster with two systems to ensure high availability for the Policy Master. Each system in the Policy Master cluster is connected to shared storage and dedicated network links. Follow the instructions in this section to acquire and set up the hardware that is needed to run the Policy Master cluster.

To set up the Policy Master cluster hardware

1. Select two to four Solaris or Linux systems with the following capabilities:
   - At least 2 gigabytes of physical memory
   - At least one network interface for private communication between the Policy Master cluster systems; two links are desirable.
   - At least one network link between the Policy Master and the VCS One client systems. Two links are preferable.
2. Choose a storage architecture for the Policy Master configuration data.
   See “Configuring your storage architecture” on page 51.
   If you use Storage Foundation, select a storage device for the Policy Master configuration database. The device is shared between the two systems and should support SCSI-3 persistent reservations.
   For information on how to connect and configure the storage at the appropriate time, see: “Adding storage devices” on page 98.
3. Connect the TCP/IP network to the client systems.
4. Use the ping utility to test the network connections.

Opening the required ports

Before you install the VCS One Policy Master or client on Linux, you must open the ports that are specified in Table 1-3.

Table 1-3 VCS One required ports

Host system	VCS One components	Port to open on host system	Outbound/inbound port
Policy Master system	Policy Master	14151	Inbound
	Policy Master database	14157 Not modifiable	
	Web server	14171 (secure)	Inbound
	Web server admin port	14172	Inbound
	Authentication server	14159 **Note:** If you upgrade from VCS One 2.0.1 to VCS One 5.0, the default port number for the authentication broker is 2821.	Inbound and outbound
Client system	Client	14154	Inbound for messages from the Policy Master
		14151	Outbound for messages to the Policy Master
Simulator system	Simulator	14156	Inbound
Root broker on a private branch exchange (PBX) system	Symantec Product Authentication (AT) Service	1556	

To open the required ports on Linux

1. Log on as a user who has the privileges to change the firewall configuration.
2. Set up the table of IP packet filter rules for each of the ports you want to open. Enter the following:

   iptables -I *INPUT* -p tcp --dport *port* -j ACCEPT
   iptables -I *OUTPUT* -p tcp --dport *port* -j ACCEPT

   Where `port` is the port number. Specify `INPUT` for an inbound port, and `OUTPUT` for an outbound port. For example, the commands to open the required ports for the VCS One client on Linux are:

   ```
   iptables -I INPUT -p tcp --dport 14154 -j ACCEPT
   iptables -I OUTPUT -p tcp --dport 14151 -j ACCEPT
   iptables -I OUTPUT -p tcp --dport 14159 -j ACCEPT
   ```

Running installation prechecks

For each software installation, you can check the target systems before installation to verify that:

- The system has enough disk space for the installation.
- The product being installed is not already installed.

Logging on and mounting the product disc

Follow the instructions in this section to mount the product disc on Solaris, Linux, AIX, or HP-UX.

To log on and mount the product disc

1. Log on as root on a system where you want to install VCS One.
2. Insert the product disc into a DVD drive connected to your system.
3. Mount the VCS One software disc. For details, see the appropriate section for your platform:
   - For Solaris, see the next section "Mounting the product disc manually on Solaris."
   - For Linux, see "Mounting the product disc manually on Linux" on page 23.
   - For AIX, see "Mounting the product disc on AIX" on page 23.
   - For HP-UX, see "Mounting the product disc on HP-UX" on page 23.

Mounting the product disc manually on Solaris

If Solaris volume management software is running on your system, the software disc automatically mounts as `/cdrom/cdrom0`.

If Solaris volume management software is not available to mount the product disc, you must mount it manually.

To mount the product disc manually on Solaris

1. Log on and mount the product disc.
2. Insert the disc and enter the following:
   # mount -F hsfs -o ro /dev/dsk/*c0t6d0s2* /cdrom/cdrom0
   where `c0t6d0s2` is the default address for the disc drive.

Mounting the product disc manually on Linux

The disc is automatically mounted. If the disc does not automatically mount, you must mount it manually.

To mount the product disc manually on Linux

1. Log on and mount the product disc. See "Logging on and mounting the product disc" on page 22.
2. Insert the disc and enter the following:
   # mount -o ro /dev/cdrom /mnt/cdrom

Mounting the product disc on AIX

Mount the disc by determining the device access name of the DVD drive. The format for the device access name is `cdx`, where *x* is the device number.

To mount the product disc on AIX

1. Log on and mount the product disc. See "Logging on and mounting the product disc" on page 22.
2. Insert the disc and enter the following:
   # mkdir -p /cdrom
   # mount -V cdrfs -o ro /dev/cd*x* /cdrom

Mounting the product disc on HP-UX

To mount the product disc on HP-UX

1. Log on and mount the product disc. See "Logging on and mounting the product disc" on page 22.

2 Determine the block device file for the DVD drive. Enter the following:
```
# ioscan -fnC disk
```

3 Make a note of the device file as it applies to your system.

4 Create a directory in which to mount the software disc and mount the disc using the appropriate drive name. For example, enter the following:
```
# mkdir -p /dvdrom
# /usr/sbin/mount -F cdfs /dev/dsk/c3t2d0 /dvdrom
```

5 Verify that the disc is mounted. Enter the following:
```
# mount
```

Running the prechecks

You can run installation prechecks on the installer utility menu or from the command line. The installation precheck utility performs preinstallation checks on the systems you specify.

If there is an error, the utility provides error details. For example, you might see an error saying that your server is running on a platform that VCS One does not support. If that happens, check the *Veritas Cluster Server One Release Notes* for information about supported platforms.

Running the prechecks from the installer menu

To run the prechecks from the installer menu, navigate to the directory that contains the product installer and follow these steps.

To run the prechecks on the installer menu

1 Go to the directory for your platform. Enter the following:
- On Solaris (10 SPARC 64-bit), enter the following:
```
# cd /cdrom/cdrom0/sol_sparc
```
- On Linux (RHEL 5 x86_64), enter the following:
```
# cd /mnt/cdrom/rhel5_x86_64
```

2 From the software disc, start the installer. Enter the following:
```
./installer
```

3 From the installer menu, perform a preinstallation check. Press **P**.

Running the prechecks from the command line

To run the prechecks from the command line, navigate to the directory that contains the product installer and follow these steps.

Note that running `installvcsonepm` or `installvcsonecd -precheck` from `/opt/VRTS/install` does not work. Run it from the software disc as indicated.

To run the prechecks from the command line

1. Go to the cluster_server_one directory. Enter the following:
   `cd cluster_server_one`
2. Enter the Policy Master installation command with the `-precheck` option, specifying the systems on which to install. Enter the following:
   `./installvcsonepm -precheck sysA`
3. Enter the client installation command with the `-precheck` option, specifying the systems on which to install. Enter the following:
   `./installvcsonecd -precheck sysB sysC sysD`

About the Symantec Product Authentication Service

Symantec Product Authentication Service provides a hierarchy of brokers that issue credentials. These brokers allow trusted communications between users and processes on the Policy Master systems and client systems. All VCS One environments require the Symantec Product Authentication Service for trusted communications. The Symantec Product Authentication Service is installed when you install VCS One.

VCS One uses an embedded broker model where the root broker and authentication broker are always running on the active Policy Master system. The Symantec Product Authentication Service issues credentials to the Policy Master, the VCS One client processes, and all users in the VCS One cluster.

Symantec Product Authentication Service supports third-party private domain repositories, such as LDAP and Active Directory.

For information on setting up authentication with third-party private domain repositories, see Chapter 7, “Setting up authentication plug-ins for VCS One” on page 83.

Removing earlier versions of the Symantec Product Authentication Service

If you have an earlier version of the Symantec Product Authentication Service installed, you must remove it before installing VCS One. The Symantec Product Authentication Service is installed when you install VCS One.

On your Policy Master and client systems, remove all VRTSatclient and VRTSatserver packages, including credentials and the `/var/VRTSat` and

`/var/VRTSat_lhc` directories, before installing VCS One. Before removing them, ensure that they are not in use by other products.

Configuring ssh, rsh, or remsh before installing

You can install VCS One on remote systems using either secure shell (ssh) or remote shell (rsh). You can use remsh (for client installations on HP-UX only). Symantec recommends using ssh.

Configuring ssh

The ssh program lets you log on to a remote system and execute commands on it. It enables encrypted communications and an authentication process between two untrusted hosts over an insecure network. The ssh program is the preferred method of remote communication because it is more secure than the rsh suite of protocols. Symantec recommends configuring a secure shell environment before installing VCS One and other Veritas products by Symantec. The following is an example ssh setup procedure.

Before you enable ssh, read the ssh documentation and online manual pages. If you have questions or issues about your ssh configuration, contact your operating system support provider. For access to online manuals and other resources, visit the OpenSSH Web site at:

http://openssh.org

To configure ssh

1. Log on as root on the system where you plan to run the installation.
2. Navigate to the root directory. Enter the following:
   `cd /`
3. Generate a DSA key pair. Enter the following:
   `ssh-keygen -t dsa`
4. At the prompt, press **Enter** to accept the default location of `/.ssh/id_dsa`. Typically, this location is the following:
   - For AIX, HP-UX, and Solaris:
     `/.ssh/id_dsa`
   - For Linux:
     `/root/.ssh/id_dsa`
5. At the passphrase prompt, do not enter one. Press **Enter**.
6. Press **Enter** again.

7 Ensure that the `/.ssh` directory is on all target installation systems. Go to the root directory and enter the following:

`ls /.ssh/`

If you do not see `/.ssh` directory, you must create it on all the target systems and set the write permission to root only. Enter the following:

`cd /`

`mkdir /.ssh`

8 Change the permissions of the `/.ssh` directory. Do one of the following:

- For AIX, HP-UX, and Solaris, enter the following:

  `chmod 700 /.ssh`

- For Linux, enter the following:

  `chmod 700 /root/.ssh`

9 Append the public key from the source system to the authorized_keys file on the target system, using secure file transfer. Do the following, in this order:

- Make sure the secure file transfer program (SFTP) is enabled on the target installation systems.

  To enable SFTP, the `/etc/ssh/sshd_config` file must contain the following lines:

  ```
  PermitRootLogin           yes
  Subsystem          sftp      /usr/lib/ssh/sftp-server
  ```

- If these lines are not there, add them and restart ssh.
- From the source system, use SFTP to move the public key to a temporary file on the target system. Enter the following:

  `sftp target_system`

- At the "Are you sure you want to connect?" prompt, enter **`yes`**.

  Output similar to the following is displayed:

  ```
  Warning: Permanently added 'system2,10.182.00.00'
  (DSA) to the list of known hosts.
  root@system2 password:
  ```

- Enter the target system's root password.
- At the SFTP prompt, enter the following:

  `sftp>` **`put /.ssh/id_dsa.pub.hostname`**

  where *`hostname`* is the name of the system from which you are copying.

- Quit the SFTP session. Enter the following:

  `sftp>` **`quit`**

- Start the ssh session on the target system. On the source system, enter the following:

  `ssh target_system`

- At the password prompt, enter the target system's root password.
- After you log on to the target system, append the `id_dsa.pub` file to the authorized key file. Do one of the following:

  For AIX, HP-UX, and Solaris, enter the following:

  `cat /id_dsa.pub.`*`hostname`*` >> /.ssh/authorized_keys`

  where *`hostname`* is the name of the system from which you are copying.

  For Linux, enter the following:

  `cat /id_dsa.pub.`*`hostname`*` >>`
  `/root/.ssh/authorized_keys2`

  where *`hostname`* is the name of the system from which you are copying.
- After the `id_dsa.pub` public key file is copied to the target system and added to the `authorized_keys` files, delete it. On the target system, enter the following:

  `rm /id_dsa.pub.`*`hostname`*
- Log out of the ssh session. Enter the following: **`exit`**
- When you install from a source system that is also an installation target, add the local system `id_dsa.pub` key to the local `authorized_keys` file. If the installation source system is not authenticated, the installation may fail.

  Add the local system `id_dsa.pub` key to the local `authorized_keys` file. Do one of the following:

  For AIX, HP-UX, and Solaris, enter the following:

  `cat /.ssh/id_dsa.pub >> /.ssh/authorized_keys`

  For Linux, enter the following:

  `cat /.ssh/id_dsa.pub >> /root/.ssh/authorized_keys2`

10 Verify that you can connect to the target system. On the source system, enter the following:

   `ssh `*`target_system`*` uname -a`

   The command should execute from the source system to the target system without the system requesting a passphrase or password.

11 Repeat step 10 on each target system.

Restoring the password requirement between systems

If you configure ssh to enable passwordless communications between systems during an installation, you can restore the password requirement when the installation is finished.

For instructions, see the section appropriate to your operating system:

- "Restoring the password requirement between AIX, HP-UX, and Solaris systems"
- "Restoring the password requirement between Linux systems"

Restoring the password requirement between AIX, HP-UX, and Solaris systems

To restore the password requirement between AIX, HP-UX, and Solaris systems

- Remove the `id_dsa.pub.`*`hostname`* entry you appended to the file `/.ssh/authorized_keys` on all systems where you added it.

Restoring the password requirement between Linux systems

To restore the password requirement between Linux systems

- Remove the `id_dsa.pub.`*`hostname`* entry you appended to the file `/root/.ssh/authorized_keys2` on all systems where you added it.

Configuring rsh or remsh

The rsh (remote shell) program lets you log on to and execute commands on a remote system. The remote system on which the rsh executes the command must be running the rsh daemon.

The rsh program is not secure for network use, because it sends unencrypted information over the network. The ssh program is the preferred method of remote communication because it is more secure than the rsh suite of protocols.

See "Configuring ssh" on page 26.

If you run rsh with the basename "remsh," rsh checks for the file `/usr/bin/remsh`. If this file exists, rsh uses remsh is an alias for rsh. If `/usr/bin/remsh` does not exist, rsh uses remsh as a host name.

Before you enable rsh, read the rsh documentation and online manual pages. If you have questions or issues about your rsh configuration, see the operating system documentation.

Configuring rsh on Solaris

To configure rsh on Solaris

1 Determine the rsh/rlogin status. Do one of the following:

- On Solaris 10, enter the following:
  `inetadm | grep -i login`

If the service is enabled, the following line is displayed:

```
enabled online svc:/network/login:rlogin
```

If the service is disabled, the following line is displayed:

```
disabled disabled svc:/network/login:rlogin
```

- On Solaris 9, enter the following:

  cat /etc/inet/inetd.conf | grep rsh

  The inetadm command does not work on Solaris 9.

  If the service is enabled, the following information is displayed:

```
RSHD - rsh daemon (BSD protocols)
shell  stream   tcp    nowait   root   /usr/sbin/in.rshd       in.rshd
shell  stream   tcp6   nowait   root   /usr/sbin/in.rshd       in.rshd
```

2 Enable and disable rsh/rlogin. Do one of the following:

- On Solaris 10, do one of the following:

  To enable rsh/rlogin, enter the following:

  inetadm -e rlogin

  To disable rsh/rlogin, enter the following:

  inetadm -d rlogin

- On Solaris 9:

  To enable rsh/rlogin, add the following line to `/etc/inet/inetd.conf`:

```
login  stream   tcp6   nowait   root   /usr/sbin/in.rlogind    in.rlogind
shell  stream   tcp    nowait   root   /usr/sbin/in.rshd       in.rshd
shell  stream   tcp6   nowait   root   /usr/sbin/in.rshd       in.rshd
```

  To disable rsh/rlogin, delete the above line.

  Restart inetd. Enter the following:

  /usr/bin/pkill -HUP inetd

3 Verify that rsh is set up correctly. Enter the following:

exec /usr/bin/rsh *system_name* "LANG=C echo Symantec 2>&1" 2>&1

```
Symantec
```

The command should return “Symantec.” If it does not, there is an issue with rsh-setup.

Modifying the .rhosts file on Solaris

A separate .rhosts file is in the $HOME directory of each user. You must modify the .rhosts file for each user who remotely accesses the system using rsh.

Make sure that each line of the .rhosts file contains a fully-qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access system1 from system2, you must add an entry for `system2.`*`companyname`*`.com` in the .rhosts file on system1.

To modify the .rhosts file on Solaris

1 Enter the following:
echo "system2.*companyname*.com" >> $HOME/.rhosts

2 To ensure security, delete the .rhosts file from each user's $HOME directory. Enter the following:
rm -f $HOME/.rhosts

Configuring rsh on Linux

To configure rsh on Linux

1 Make sure the rsh and rsh-server packages are installed. Enter the following:
rpm -qa | grep rsh

2 If it is not already in the file, enter the following command to append the line "rsh" to the `/etc/securetty` file. Enter the following:
echo "rsh" >> /etc/securetty

3 In the `/etc/pam.d/rsh` file for the pam_rhosts_auth.so entry, change the "auth" type from "required" to "sufficient."
`auth sufficient pam_rhosts_auth.so`

4 Enable the rsh server. Enter the following:
chkconfig rsh on

5 Verify that rsh is set up correctly. Enter the following:
exec /usr/bin/rsh *system_name* "LANG=C echo Symantec 2>&1" 2>&1
`Symantec`
The command should return "Symantec." If it does not, there is an issue with rsh-setup.

Modifying the .rhosts file on Linux

A separate .rhosts file is in the $HOME directory of each user. You must modify the .rhosts file for each user who remotely accesses the system using rsh.

Make sure that each line of the .rhosts file contains a fully-qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access system1 from system2, you must add an entry for `system2.`*`companyname`*`.com` in the .rhosts file on system1.

To modify the .rhosts file on Linux

1 Enter the following:
echo "system2.*companyname*.com" >> $HOME/.rhosts

2 Remove the “rsh” entry in the `/etc/securetty` file.

3 Disable the rsh server. Enter the following:
`chkconfig rsh off`

4 To ensure security, delete the .rhosts file from each user’s $HOME directory. Enter the following:
`rm -f $HOME/.rhosts`

Configuring remsh on HP-UX

Remote shell (remsh) functionality is enabled automatically after installing an HP-UX system.

Modifying the .rhosts file on HP-UX

A separate .rhosts file is in the $HOME directory of each user. You must modify the .rhosts file for each user who remotely accesses the system using remsh.

Make sure that each line of the .rhosts file contains a fully-qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access system1 from system2, you must add an entry for `system2.`*`companyname`*`.com` in the .rhosts file on system1.

To modify the .rhosts file on HP-UX

1 Enter the following:
`echo "system2.`*`companyname`*`.com" >> $HOME/.rhosts`

2 To ensure security, delete the `.rhosts` file from each user’s `$HOME` directory. Enter the following:
`rm -f $HOME/.rhosts`
For more information on configuring remsh, see the operating system documentation and the `remsh`(1M) manual page.

Configuring rsh on AIX

To configure rsh on AIX

1 Enable rsh. Create a `/.rhosts` file on each target system. Add a line to the file specifying the full domain name of the source system. For example, add the following line:
`sysname.`*`domainname`*`.com root`

2 Change permissions on the `/.rhosts` file to 600. Enter the following:
`chmod 600 /.rhosts`

3 Verify that rsh is set up correctly. Enter the following:

```
exec /usr/bin/rsh system_name "LANG=C echo Symantec 2>&1" 2>&1
Symantec
```

The command should return “Symantec.” If it does not, there is an issue with rsh-setup.

4 To ensure security, delete the `/.rhosts` file from each target system. Enter the following:

```
rm -f /.rhosts
```

Chapter 2

Installing and configuring the VCS One Policy Master

This chapter includes the following topics:

Before you install the Policy Master

For all platforms, you must perform the necessary preinstallation tasks.

See Chapter 1, "Getting ready to install VCS One".

Before you install on Linux, you must enable the required ports.

See "Opening the required ports" on page 21.

Installing patches

Before you install the Policy Master, install the required operating system patches. See the *Veritas Cluster Server One Release Notes* for the required operating systems patches.

Preparing your network on Solaris

Before you configure the Policy Master on Solaris, you must configure your IP addresses and NICs for a Solaris Policy Master installation. You must also preserve the configuration across reboots.

Configuring your IP addresses and NICs for Solaris

To begin configuring your IP addresses and NICs for Solaris, connect to the Policy Master system through the console.

To configure your IP addresses and NICs for Solaris

1. Configure test IP address on the base of each NIC. Do not use the `addif` command. Enter the following:

   # ifconfig *pm_nic* plumb *test_ip* netmask *netmask* broadcast + deprecated -failover up

   where *pm_nic* is the Policy Master NIC, *test_ip* is the IP address for that NIC (and the IP address that you use to test your network connection), and *netmask* is your Policy Master netmask.

2. If you need additional IP addresses on the Policy Master NIC, such as host IP addresses, you can plumb the other IP addresses. Enter the following:

   # ifconfig *pm_nic* addif *additional_ip* netmask *netmask* up

   where *pm_nic* is the Policy Master NIC, and *additional_ip* is any additional IP address you need to plumb, and *netmask* is your Policy Master netmask.

Preserving the configuration across reboots

To preserve your configuration across reboots

1. Save your test IP address on the base of each NIC. Do not use the `addif` command. Enter the following at the beginning of the `/etc/hostname.`*`pm_nic`* file:

   `test_ip` **`netmask`** ***`netmask`*** **`broadcast + deprecated -failover up \`**

   where *`pm_nic`* is the Policy Master NIC, *`test_ip`* is the IP address for that NIC (and the IP address that you use to test your network connection), and *`netmask`* is your Policy Master netmask.

2. If you need additional IP addresses on the Policy Master NIC, such as host IP addresses, you can plumb the other IP addresses. Enter the following lines in the `/etc/hostname.`*`pm_nic`* file, after the line you entered in step 1:

   `addif` ***`additional_ip`*** **`netmask`** ***`netmask`*** **`broadcast + up`**

   where *`pm_nic`* is the Policy Master NIC, *`additional_ip`* is any additional IP address you need to plumb, and *`netmask`* is your Policy Master netmask.

Preparing your network on Linux

On Linux, if the incorrect netmask is used to plumb the Base IP address, the network may not work. Symantec recommends using MultiNICA Performance Mode in the Policy Master service group (PMSG). MultiNICA Performance Mode requires a unique Base IP address with the correct Netmask addresses plumbed on the required NICs.

See the *Veritas Cluster Server One Bundled Agents Reference Guide* for information about MultiNICA Performance Mode.

Preparing Policy Master cluster information

Before you install the Policy Master software, have the following information ready:

- Names of the systems to install the Policy Master software
  Make sure that you can ping each system name from each of the Policy Master systems.
  If the Policy Master systems are in the same time zone, clock times on each system must be within 30 minutes of one another. If the clock times are more than 30 minutes apart, the installation may fail. Use the `ntpdate` command to synchronize clock times.
- A unique name for the Policy Master cluster, such as vcsonepm_cluster.

The name can be up to 128 characters long, and must start with an alphanumeric character. It can only contain the following characters: A-Z, a-z, 0-9, '_' and '-'. The name cannot contain the following reserved words: "cluster," "system," "group," "resource," and "type."

- A numerical ID for the Policy Master cluster (a number from 0 - 65535). For example: 11.
  If your configuration has multiple Policy Master clusters (including VCS clusters), each ID must be unique.
  In a configuration that has only one Policy Master system, you do not need to provide a numerical ID.
- Names of two or more private NICs on each system.
  In a configuration that has only one Policy Master system, you do not need to provide any private NIC information.
- A port number for the authentication service (a number from 0 - 65536). The port must not be a port on which other applications listen.
  Instead of providing an authentication service port number, you can use the default port (14159).
- One or more virtual IP addresses for the systems in the Policy Master cluster.

  Note: In a Policy Master cluster system, the virtual and physical IP addresses must be different.

- Netmasks that the virtual IP addresses use.
- Public NICs on each Policy Master system.
- Base IP addresses on each of the public NICs.

Preparing your storage architecture

Symantec recommends that you set up a storage architecture to store your configuration data. You must configure shared storage in order for the Policy Master to fail over from one system to another. Prepare the information that VCS One requires to set up your storage architecture.

Preparing to install Veritas Storage Foundation

Before you install Storage Foundation, have the following system information ready:

- The name of the disk group to be created.

- Names of one or more disks that are part of the disk group. Use short disk names.
- Name of the volume that needs to be created within the disk group.
- Size of the volume that needs to be created. For example, 4400240 (number of blocks), 2G, or 240M.
- Mount point where the volume is mounted.

Preparing to configure NetApp filer

Before you install NetApp filer, have the following system information ready:

- Mount point where the volume is mounted.
- IP address or host name for the NetApp filer.
- Access method for the NetApp filer (rsh, ssh, or api).
- User name for accessing the NetApp filer.
- Password for accessing the NetApp filer (for API access mode).
- IP address or host name for the NIC connected to the NetApp filer for each Policy Master system.
- File system path or NetApp filer to be used to store the VCS One configuration.

Note: The installer exports the NetApp volume and mounts the mount point. If the mount point is already mounted, the installer prompts you before unmounting it forcibly.

Preparing to configure other shared storage architectures

If you do not install Storage Foundation or NetApp filer when you install VCS One, you can configure another storage architecture. For example, you can configure local storage, or a customized shared storage architecture. Before you configure your storage architecture, mount the shared storage on each system and note the shared storage mount point. For example, `/PM`.

Preparing to configure disaster recovery

Disaster recovery uses global clustering to protect against the types of outages that large-scale natural disasters cause. In such situations, VCS One global clusters migrate applications to remote clusters located considerable distances apart.

If you configure disaster recovery, VCS One monitors events between clusters. Using disaster recovery, the global cluster is aware of the state of the service groups in the global cluster at all times.

To configure disaster recovery, have the following information ready:

- Two or more unique virtual IP addresses dedicated to disaster recovery. (If you do not want to configure separate virtual IP addresses for disaster recovery, you can use the Policy Master virtual IP addresses.)
- If you configure additional virtual IP addresses, obtain the netmask for each virtual IP address.
- A NIC for each unique virtual IP address. (If your Policy Master is set up with redundant NICs, you do not need a dedicated NIC for disaster recovery.)

Installing the Policy Master

The Veritas Cluster Server One (VCS One) Policy Master software is on the VCS One software disc for the appropriate platform.

Note: This release of VCS One does not support installing the Policy Master on Solaris with zones configured. On Solaris, you must install the Policy Master on a system free of zones.

The VCS One installer installs the Policy Master, and, (optionally) Storage Foundation. The installer also gives you the option to configure NetApp filer and disaster recovery.

The installation procedures are in the following subsections:

- "Launching the installer" on page 40
- "Specifying the target system" on page 41
- "Specifying whether to install Storage Foundation" on page 42
- "Selecting a license type" on page 42
- "Specifying when to configure the Policy Master" on page 43

Launching the installer

Launch the VCS One installer to install the Policy Master. You can configure the Policy Master during the installation process, or you can come back and configure it after the installation is complete.

To launch the VCS One installer

1. Log on as root on one of the Policy Master cluster systems.
2. On the VCS One software disc, change directories to the platform-specific directory. Enter the following:
   # **cd *platform***
   where *platform* is the platform-specific directory, such as *RHEL5_x86_64* or *sol_sparc*.
3. On the software disc, start the installer script. Enter the following:
   # **./installer**
4. From the Task menu, select the following task:
   Install/Upgrade a Product
5. From the list of products, select **Veritas Cluster Server One by Symantec - Policy Master.**
6. Accept the End User License Agreement (EULA). At the EULA prompt, enter the following: **y**.
   The installer provides information about the installation and configuration.
7. Review the information on each page and press **Enter** to continue.

Specifying the target system

You must specify the name of the target system for each Policy Master system.

To specify the target system

1. At the system names prompt, enter the names of the systems on which you want to install the VCS One Policy Master. Separate each name with a space. Do not enter fully-qualified domain names or IP addresses. For example, enter the following: **sys1 sys2**

   Note: If you install the Policy Master on a single system, you only need to enter one system name.

   If you install the Policy Master on a single system, you see a prompt.
2. Do one of the following:

If you install the Policy Master on multiple systems	Go to the next section, "Specifying whether to install Storage Foundation."
If you install the Policy Master on a single system	At the single node confirmation prompt, enter **y**. Then go to the next section, "Specifying whether to install Storage Foundation."

Specifying whether to install Storage Foundation

You can optionally install and configure Storage Foundation to store the VCS One Policy Master configuration database.

Note: On Solaris, VCS One supports Storage Foundation 5.0MP1 and above. On Linux, VCS One does not support versions of Storage Foundation before Storage Foundation 5.0 MP2.

Veritas Storage Foundation by Symantec includes Veritas File System by Symantec (VxFS) and Veritas Volume Manager by Symantec (VxVM) with varying feature levels.

Veritas File System is a high performance journaling file system that provides easy management and quick-recovery for applications. Veritas File System delivers scalable performance, continuous availability, increased I/O throughput, and structural integrity.

Veritas Volume Manager removes the physical limitations of disk storage. With Veritas Volume Manager, you can configure, share, and manage your storage online. Managing storage online optimizes storage I/O performance without interrupting data availability. Veritas Volume Manager also provides easy-to-use, online storage management tools to reduce downtime.

To specify whether to install Storage Foundation

- Read the information and decide if you want to install and use Storage Foundation to store the VCS One configuration. At the Storage Foundation prompt, if you want to install Storage Foundation packages, enter **y**.

Selecting a license type

If you do not have a license installed, you must select a license type.

For more information on licensing, see *Veritas Cluster Server One Release Notes*.

To select a license type

- Do one of the following:
  - If the installer finds your license, you are not asked to select a license type. Go to the next section, "Reviewing the package list."
  - If you are asked to select a license type (demo, NFR, or permanent), type the number corresponding to your license type. Then, go to the next section, "Reviewing the package list."

Reviewing the package list

The installer provides a list of packages to be installed.

To review the package list

- Read each page listing the packages to be installed and press **Enter** to continue.
  For a list of the packages, see Appendix F, "Required packages" on page 203.

Specifying when to configure the Policy Master

On Linux, you must specify whether to configure the Policy Master right after the installation, or complete the installation and configure the Policy Master later.

On Solaris, if do not install Storage Foundation, you must specify whether to configure the Policy Master right after the installation. If you install Storage Foundation on Solaris, you must reboot your machine and then proceed with the configuration.

To specify when to configure the Policy Master

1 Do one of the following:

If you install the Policy Master on Linux	Proceed to step 2.
If you install the Policy Master on Solaris, and you do not install Storage Foundation	Proceed to step 2.
If you install the Policy Master on Solaris, and install Storage Foundation (or locally-mounted storage)	Reboot your system. After you reboot, go to the next section: "Configuring the Policy Master."

2 At the VCS One configuration readiness prompt, do one of the following:

To configure the Policy Master as part of the installation process	Enter the following: **y**. Go to the next section, "Configuring the Policy Master."

To install Policy Master now, but configure it later	Enter the following: **n**. The installer installs the packages, and you can configure the Policy Master later. When you are ready to configure, see the next section: "Configuring the Policy Master."

Configuring the Policy Master

During the configuration process, you configure your Policy Master cluster. The installer also gives you the option to configure disaster recovery, and Storage Foundation or NetApp.

The configuration procedures are in the following subsections:

Starting the Policy Master configuration

If you have not yet started the Policy Master configuration, do so now.

To start the Policy Master configuration

1. Start the VCS One configuration. Enter the following:
   # **./installvcsonepm -configure**
2. Enter the names of the systems on which you want to configure the VCS One Policy Master. Separate each name with a space. Do not enter fully-qualified domain names or IP addresses. For example, enter the following: **sys1 sys2**

Configuring the Policy Master cluster

You must provide a host name for the Policy Master cluster. If you install the Policy Master on two or more systems, you must also provide a numerical ID number and configure heartbeat settings.

Naming the Policy Master cluster

You must specify a unique name to identify the Policy Master cluster.

To name the Policy Master cluster

- At the cluster name prompt, enter a unique name for the Policy Master cluster. For example, enter the following: **my_cluster**.

Creating an ID for the Policy Master cluster

If you install the Policy Master on more than one system, you must create an ID for the Policy Master cluster.

To create an ID for the Policy Master cluster

- At the cluster ID prompt, enter a unique ID between 0-65535. For example, enter the following: **65000**

Configuring the heartbeat settings

If you install the Policy Master on more than one system, you must designate at least one NIC for a private heartbeat link. A private heartbeat link is a link that sends status information between systems within the Policy Master cluster. Private heartbeats are generated every half second.

You can optionally designate a NIC for a low-priority heartbeat link. Low priority heartbeats are generated every second and do not send status information. If none of the high-priority links work, low-priority links are automatically promoted to high-priority links.

To configure the heartbeat settings

1. At the first heartbeat prompt, enter the NIC for the first private heartbeat link on your VCS One cluster. For example, enter the following:
   - (On Linux) **eth0**
   - (On Solaris x64) **bge0**

   Type **y** to confirm the NIC entry.
2. At the second heartbeat prompt, specify if you want to configure a second private heartbeat link. Type **y** or **n**.
3. If you configure a second private heartbeat, enter the NIC. For example, enter the following:
   - (On Linux) **eth1**
   - (On Solaris x64) **bge1**

   Type **y** to confirm the NIC entry.

4 At the low priority heartbeat prompt, specify if you want to configure a low priority heartbeat link. Type **y** or **n**.

5 If you configured a low priority heartbeat, enter the NIC. For example, enter the following:

- (On Linux) **eth2**
- (On Solaris x64) **bge2**

Type **y** to confirm the NIC entry.

6 At the all systems prompt, specify if you want to use the same NICs for private heartbeat links on all systems. Type **y** or **n**.

Specifying the authentication services port number

You must specify if you want to use the default port number for authentication services.

To specify the authentication services port number

- At the authentication services port number prompt, do one of the following:
  - If you want to use the default port number (14159) for authentication services, enter the following: **y**.
  - If you want to specify a different port number for authentication services, enter the following: **n**. At the next prompt, enter the port number you want to use. For example, enter the following: **14001**.

Confirming the Policy Master cluster configuration

At the cluster configuration verification prompt, verify that the name, ID, broker port, and NIC information is correct.

(The broker port is the authentication services port number you set in the section “Specifying the authentication services port number.”)

To confirm the Policy Master cluster configuration

- At the Policy Master cluster configuration verification prompt, confirm that the configuration information is correct. Enter **y**.

Configuring virtual IP addresses for the Policy Master

You must enter the NICs for the Policy Master virtual IP address. If you install on Solaris, you must specify if you want to use the mpathd. You must also enter the Policy Master virtual IP addresses and netmasks.

Entering the NICs for the Policy Master virtual IP address

To enter the NICs for the Policy Master virtual IP address

1. Enter the NIC for the Policy Master Virtual IP address to use on your system. From the list of NIC devices that are discovered on your systems, select any NIC that is up and running on a public network. For example, enter the following:
   - (On Linux) **`eth0`**
   - (On Solaris x64) **`bge0`**
2. At the all nodes prompt, specify if you want to use the same NIC on all Policy Master systems. Do one of the following:
   - To use the same NIC on all Policy Master systems, enter **`y`**.
   - To select your NICs one-by-one for each Policy Master system, enter **`n`**.

Specifying whether to use the mpathd (Solaris only)

If you install on Solaris, you must indicate if you want to use the `mpathd` that the operating system provides.

To specify whether to use the mpathd

1. At the mpathd prompt, do one of the following:
   - If you want to use the mpathd, enter **`y`**.
     Then go to step 2.
   - If you do not want to use the mpathd, enter **`n`**.
     Then go to the next section, "Choosing a storage architecture to configure."
2. If you use the mpahtd, enter its absolute path. For example, enter the following:
   `/sbin/in.mpathd`

Entering the Policy Master virtual IP addresses and netmasks

To enter the Policy Master virtual IP addresses and netmasks

1. Enter one or more Policy Master virtual IP addresses. For example, enter the following: **`192.168.1.20 192.168.1.21`**
2. Enter the netmasks for the virtual IP addresses you entered. Review the information. For example, enter the following: **`255.255.248.0`**.
3. At the Policy Master configuration verification prompt, confirm that the virtual IP addresses, netmasks, and NICs are correct. Enter the following: **`y`**.

Choosing a storage architecture to configure

Symantec recommends that you use a shared storage architecture for storing the configuration database. You can configure Storage Foundation if you are in the process of installing Storage Foundation, or it is already on your system. Otherwise, you can configure NetApp filer or another storage architecture.

To select and configure a storage architecture

1. At the Storage Architecture prompt, select the storage architecture you want to configure.
2. See Table 2-1 for details on the remaining configuration tasks.

Table 2-1 VCS One configuration task details

To configure	Complete these tasks
Storage Foundation as part of the installation and configuration process	1 "Configuring disaster recovery" on page 48 2 "Configuring Storage Foundation" on page 51 3 "Starting the Policy Master" on page 54
Storage Foundation when it is already installed on your system	1 "Configuring Storage Foundation" on page 51 2 "Configuring disaster recovery" on page 48 3 "Starting the Policy Master" on page 54
NetApp filer, or another storage architecture	1 "Configuring your storage architecture" on page 51 2 "Configuring disaster recovery" on page 48 3 "Starting the Policy Master" on page 54

Configuring disaster recovery

Follow the steps in this section to specify if you want to configure disaster recovery.

For information about disaster recovery, see "Preparing to configure disaster recovery" on page 39.

Deciding when to configure disaster recovery

You can configure disaster recovery during the VCS One installation and configuration process, or you can configure it after installing and configuring VCS One.

Specify when to configure disaster recovery

- At the VCS One disaster recovery configuration prompt, do one of the following:

If you want to configure disaster recovery as part of the VCS One installation and configuration process	Enter the following: **y**. Go to the next section, "Configuring disaster recovery as part of the installation and configuration process."
If you do not want to configure disaster recovery, or if you want to configure disaster recovery after you install and configure VCS One	Enter the following: **n**. To configure disaster recovery after you install the Policy Master, see the section: "Configuring disaster recovery after you install VCS One" on page 50.

Configuring disaster recovery as part of the installation and configuration process

Follow these steps to configure disaster recovery during the installation and configuration process. To configure disaster recovery later, see:

"Configuring disaster recovery after you install VCS One" on page 50.

To configure disaster recovery

1. Enter one or more virtual IP addresses, separated by a space. For example, enter the following:

   192.168.1.15 192.168.1.16.

   Symantec recommends dedicating two or more unique virtual IP addresses to disaster recovery. If you dedicate fewer than two unique virtual IP addresses to disaster recovery, you are prompted to specify if you want to continue.

2. Do one of the following:
   - If you are prompted about continuing with fewer than two unique virtual IP addresses, go to step 3.
   - If you are not prompted about continuing with fewer than two unique virtual IP addresses, go to step 5.

3. Do one of the following:
   - To add more virtual IP addresses, enter the following: **n**. Go back to step 1.
   - To continue with fewer than two unique virtual IP addresses, enter the following: **y**. Go to step 4.

4 Do one of the following:

If the virtual IP address is already configured, and you see the disaster recovery configuration verification prompt	Skip to step 8
If you do not see the disaster recovery configuration verification prompt	Go to step 5

5 For each unique virtual IP address, enter the NIC. For example, enter the following:
- (On Linux) **eth0**
- (On Solaris x64) **bge0**

You are prompted to specify if you want to use the same NIC for all Policy Master systems.

6 At the all nodes prompt, do one of the following:
- If you want to use the same NIC on all Policy Master systems, type **y**.
- If you want to use different NICs on the different Policy Master systems, type **n**. Then specify a NIC for each system.

7 For each unique virtual IP address, enter the netmask. For example, enter the following: **255.255.248.0**.

8 At the disaster recovery configuration verification prompt, verify that the virtual IP address, NIC, and netmask are correct. Enter the following: **y**.

Configuring disaster recovery after you install VCS One

Follow these steps to configure disaster recovery after you install and configure VCS One.

To configure disaster recovery after installing and configuring VCS One

1 Launch the VCS One disaster recovery installer. Enter the following:
./installvcsonepm -configuredr

2 Enter the name of the system on which you want to configure disaster recovery. For example, enter the following: **sys1**.

3 Follow the disaster recovery installation steps.
See: "Configuring disaster recovery as part of the installation and configuration process" on page 49.

4 Verify that the disaster recovery service group is online. Enter the following:
/opt/VRTSvcsone/bin/hagrp -state

Configuring your storage architecture

This section provides storage architecture configuration instructions. For information on configuring your storage architecture, select the appropriate link:

"Configuring Storage Foundation" on page 51

"Configuring NetApp Filer" on page 52

"Configuring other shared storage architectures" on page 54

Configuring Storage Foundation

When you configure Storage Foundation, you are prompted to specify a disk group for the configuration database. A disk group is a collection of disks that share a common configuration (for example, the configuration objects that belong to a single database).

Note: For the Policy Master to fail over from one system to another, the disk group and volume must not be in use by other applications. The disk group must also be free of any volumes that are in use by other applications.

To configure Storage Foundation

1. Enter a disk group for the configuration database. For example, enter the following: **`pmdg`**.
2. Do one of the following:

If you are not prompted to enter disk names	Go to step 5.
If you are prompted to enter disk names	Go to step 3.

3. At the disk prompt, enter the names of the disks in the disk group. Separate disk names with a space. For example, enter the following: **`sdb sdb2`**.
   The Policy Master uses the names you enter to create the disk group.
4. At the initialization prompt, choose to initialize the disks. Enter the following: **`y`**.
   You are prompted to specify a volume for the configuration database. A volume is a virtual disk device that appears to applications, databases, and file systems. A volume is like a physical disk partition. However, a volume does not have the physical limitations of a disk partition.

5 Enter the name of the volume for the configuration database. For example, enter the following: **pmvol**.

6 Do one of the following:

If you are prompted to enter the volume size	Go to step 7.
If you are not prompted to enter the volume size	Go to step 8.

7 Enter the volume size. For example, enter the following: **200M**.

8 Do one of the following:

- If the volume is not mounted, go to step 9 and enter the mount point.
- If the volume is already mounted, go to step 10 and verify your configuration.

9 Enter the mount point for the configuration database. For example, enter the following: **/PM**.

10 At Storage Foundation configuration verification prompt, enter the following: **y**.
If the installer uses an existing disk group for the configuration database, you are prompted about cleaning up the shared storage directories.

11 If you are prompted to clean up the shared storage directories, enter the following: **y**.

Configuring NetApp Filer

Follow the instructions in this section to configure Network Appliance filer (NFS) to store your configuration information. Only Network Appliance filers are supported as NetApp servers.

To configure Network Appliance Filer

1 Enter the mount point for the configuration database. For example, enter the following: **/software/vcsone**.
The installer mounts the mount point. If the mount point is already mounted, you can choose to unmount it through the installer.

2 Enter the fully-qualified host name or IP address for the NetApp Filer. For example, enter the following: **netapp3.veritas.com**.

3 Select an access method (rsh, ssh, or api).

4 Enter the name of the user who accesses the Network Appliance filer. For example, enter the following: **root**.

5 Enter the password for accessing the Network Appliance filer. At the prompt, enter the password again.

6 For each Policy Master system, enter the host name or IP address for each NIC that is connected to the NetApp Filer. For example, enter the following:
thoropt158.

7 On the NetApp filer you designate to store the VCS One configuration, enter the exported file system pathname. For example, enter the following:
/vol/*name_of_volume* /*name_of_directory_path*

8 At the API over SSL prompt, do one of the following:

- If you do not want to use API over SSL, enter the following: **n**.
- If you want to use API over SSL, enter the following: **y**. At the prompt, enter the SSL library path. The path should be on a local disk, and must contain the libcrypto.so and libssl.so library files. For example, enter the following: **/usr/lib**.

9 If you have mounted something on the mount point you specified, the installer asks you if you want to unmount it. Do one of the following:

- If you are prompted to unmount the mount point, go to step 10.
- If you are not prompted to unmount the mount point, go to step 11.

10 At the prompt for unmounting the mount point, do one of the following:

- If you do not want to unmount the mount point, enter the following: **n**.
- If you want to unmount the mount point, enter the following: **y**.

11 Confirm that the Network Appliance filer configuration is correct. Enter the following: **y**.
If the installer uses an existing Network Appliance filer for the configuration database, you are prompted about cleaning up the shared storage directories.

12 Do one of the following:

If you are not prompted to clean up the shared storage directories	Go to: "Starting the Policy Master" on page 54.
If you are prompted to clean up the shared storage directories	Clean up the shared storage directories to prevent the installation from failing. At the prompt for performing cleanup, enter the following: **y**. Then, go to: "Starting the Policy Master" on page 54.

Configuring other shared storage architectures

The VCS One Policy Master uses a database to store configuration information. If you do not install Storage Foundation or NetApp, you can choose another option for shared storage. You can also store the configuration database using local storage.

If you do not configure Storage Foundation or Network Appliance filer to store your configuration data, keep in mind the following:

- VCS One does not automatically mount your storage configuration. You must manually mount the storage on each system in the Policy Master cluster.
- If VCS One faults because it fails to connect to the database directory, you must troubleshoot the issue manually.

Follow the steps in this section to set up the configuration database using shared storage, or using local storage.

To set up the configuration database

1. Enter the mount point for the configuration database. For example, enter the following: **`/PM`**.
2. Do one of the following:

If you are not prompted to clean up the shared storage directories	Go to the next section: "Starting the Policy Master."
If you are prompted to clean up the shared storage directories	At the prompt for performing cleanup, enter the following: **`y`**. Then, go to the next section: "Starting the Policy Master."

Starting the Policy Master

You must start the Policy Master after the configuration process.

To start the Policy Master

- At the Start VCS One Policy Master processes prompt, enter **`y`** to start them.
  The VCS One Policy Master starts and reports success or failure.
  The following directory contains the path to the log files, the summary file, and the response file that the installation creates:
  `/var/VRTS/install/logs/`

After you install the Policy Master

After you install the Policy Master, see the following sections for information about the next installation steps:

- "Verifying the Policy Master installation," in the next section
- "Setting the default platform in the VCS One cluster" on page 57
- "About configuring VCS One" on page 57

Verifying the Policy Master installation

Once you install the Policy Master, is a good idea to verify the Policy Master installation. Verifying the installation checks if all of the Policy Master systems, service groups, and resources are up and running.

To verify the Policy Master installation

1. Check the state of the Policy Master service group on each system. Enter the following:
   ```
   # /opt/VRTSvcsone/bin/haadmin -state
   ```
   The output should show the PMSG is ONLINE on one system, OFFLINE on the other.
2. Verify that the PMSG is online on one system and offline on the other. Enter the following:
   ```
   # /opt/VRTSvcsone/bin/haadmin -status -summary
   ```
3. Display the status of each of the PMSG resources on each system. Enter the following:
   ```
   # /opt/VRTSvcsone/bin/haadmin -status
   ```
   The status of each resource in the Policy Master service group displays.

For a new installation, the output of the `haadmin -status` command shows the following:

- All systems are running.
- NIC resources are ONLINE on all systems.
- All other resources are ONLINE on one system and OFFLINE on the other.

Table 2-3 describes the resources in the `haadmin -status` output when the Policy Master uses Storage Foundation for storing configuration information.

Note: If you use the "other shared storage" option, the `pmdg`, `pmvol`, and `pmmount` resources may not exist. If you use Network Appliance filer, the `pmdg` resource may not exist.

Table 2-3 PMSG resources when the Policy Master uses Storage Foundation

Resource	Description
`pmip`	Policy Master virtual IP address
`pmnic`	Policy Master virtual IP address NIC device
`vcsonedb`	VCS One database
`pm`	Policy Master daemon
`atd`	Symantec Product Authentication Service daemon
`VCSOneWeb`	VCS One web console
`pmdg`	The database and repository disk group
`pmvol`	The volume for the file system containing the database
`pmmount`	The file system mount point

Table 2-4 describes the PMSG resources in the `haadmin -status` output when the Policy Master uses NetApp for storing configuration information.

Table 2-4 PMSG resources when the Policy Master uses NetApp

Resource	Description
`pmip`	Policy Master virtual IP address
`pmnic`	Policy Master virtual IP address NIC device
`vcsonedb`	VCS One database
`pm`	Policy Master daemon
`atd`	Symantec Product Authentication Service daemon
`pmmount`	Mount point for the volume/qtree exported from NetApp filer when NetApp is selected for shared storage
`pmexport`	Exports and deports the volume/qtree on NetApp filer to active and passive Policy Master systems, respectively

Table 2-4 PMSG resources when the Policy Master uses NetApp (continued)

Resource	Description
`pmfiler`	Monitors ICMP connectivity between the Policy Master and the NetApp filer
`VCSOneWeb`	VCS One web console

Table 2-5 describes the DRSG resources in the `haadmin -status` output when the Policy Master uses disaster recovery. The table contains the resources you see when you configure two virtual IP addresses for disaster recovery.

Table 2-5 DRSG resources when the Policy Master uses disaster recovery

Resource	Description
`DRSG`	Disaster recovery service group
`dr_app`	The DRApp resource that manages the disaster recovery service group (DRSG
`drip1`	Disaster recovery virtual IP address 1
`drip2`	Disaster recovery virtual IP address 2
`drnic1`	NIC device for disaster recovery virtual IP address 1
`drnic2`	NIC device for disaster recovery virtual IP address 2

Setting the default platform in the VCS One cluster

You may want to make changes at the VCS One cluster level. For example, you can set the default platform to match the platform that is most prevalent in your VCS One cluster. If you set the default platform, fewer users have to specify the platform name.

To set the default platform in the VCS One cluster

- Set the default platform in the VCS One cluster. Enter the following:
  `# /opt/VRTSvcsone/bin/haclus -modify DefaultPlatform platform`

About configuring VCS One

Each system in a VCS One cluster has a unique host name and IP address. In addition, VCS One uses attributes to match systems and users. The system-level attribute, SysUserName, which is initially NULL, contains the name of the VCS

One client user who first registers with the system. If another user tries to register with the system, they are rejected.
The user level attribute, VCSOneClientName, lists the VCS One client system with which the user is registered. A user can only register with one system in the VCS One cluster.

See the *Veritas Cluster Server One User's Guide* for information about the following topics:

- Adding users and assigning roles
- Adding systems to the VCS One cluster
- Creating service groups for your applications
- Administering groups, resources, and systems

Chapter 3

Accessing the web console

This chapter includes the following topics:

Before you access the VCS One web console

Before you access the VCS One web console for the first time, do the following:

- Install a supported browser.
  See the *Veritas Cluster Server One Release Notes* for supported browser versions.
- In the browser, do the following:
  - Enable cookies
  - Disable browser caching
  - Disable the pop-up blocker
  - Enable ActiveX controls (Internet Explorer only)
- Install a supported Flash version.
  See the *Veritas Cluster Server One Release Notes* for supported Flash versions.
- Enable the ports that the web server uses.
  See "Opening the required ports" on page 21.

Setting who can access the VCS One web console

The root user on the Policy Master system can log in without being added to the VCS One configuration. To allow other users to log in to the VCS One web console, you must explicitly add those users as VCS One users with assigned roles.

Accessing the VCS One web console

Follow the instructions in this section each time you access the VCS One web console. When you access the VCS One web console for the first time, you see a message about authentication. Read the message and click **OK** to add and permanently store a trusted security certificate. After you add the security certificate, the VCS One web console login page appears in the browser.

To access the VCS One web console

1. Open a web browser and enter the following URL:
   `https://PM_cluster_virtual_IP_address:14171`
   Symantec recommends that you use the virtual IP address of the Policy Master (PM) cluster instead of the name of the active system in the Policy Master cluster. If you use the virtual IP address, the VCS One console maintains a connection with the Policy Master after a Policy Master cluster failover operation.
2. In the web browser, click the **VCS One web console** link.
3. In the **Log on** page, specify the following details:
   - In the **Select Language** box, select the appropriate language. In this release, only English is supported.
   - In the **User Name** field, enter the name of the user.
   - In the **Password** field, enter the password.
   - In the **Domain** field, enter the domain name.
     You must specify a domain name for all domain types except unixpwd (which is the default domain type) and pam. To view a list of all the domains on the Policy Master system, enter the following command:
     `haat showallbrokerdomains -j broker`
     If you leave the **Domain** field blank and the domain type is unixpwd or pam, VCS One assumes that the domain type is the same as the Policy Master system's domain type.
   - In the **Domain Type** field, select a domain type (`unixpwd`, `nt`, `nis`, `nisplus`, `pam`, `vx`, or `ldap`).
   - In the **Broker:Port** field, enter the authentication broker name and the port number separated by a colon (:). This field is optional and is populated automatically.
4. Click **Log On**.
   The web console is best viewed at 1024x768 screen resolution.

Recreating the SSL certificate

The VCS One installer creates an SSL certificate on each Policy Master system. The SSL certificate works if you access the VCS One web console using a VCS One Policy Master virtual IP address.

With Internet Explorer 7, using a host name that resolves to a VCS One Policy Master virtual IP address when accessing the VCS One web console may display invalid SSL certificate messages.To prevent these messages, you must recreate the SSL certificate.

This section provides the general steps and resources needed to recreate an SSL certificate. For more detailed information about SSL-related tasks, see the Apache Tomcat 6.0 SSL Configuration instructions available on the Internet.

To recreate the SSL certificate, you can use Java Keytool, or another tool of your choice. For your convenience, the Java Keytool utility is included in the VCS One installation, and located at:

/opt/VRTSvcsone/jre/bin

To recreate the SSL certificate

1. Locate the key store containing the certificate that the VCS One installer created at:
   /opt/VRTSvcsone/web/tomcat/cert
2. Follow the Apache Tomcat 6.0 SSL Configuration instructions for creating an SSL certificate.
3. At the prompt, enter the information for the host name that you want to use to access the VCS One web console.
4. To restart the VCS One web console, use the `hastop` and `hastart` commands to take it offline and bring it online. Enter the following:

   ```
   # /opt/VRTSvcsone/bin/hastop -web
   # /opt/VRTSvcsone/bin/hastart -web
   ```
5. From the browser, choose to install the new certificate.

Chapter 4

Installing and configuring the VCS One client

This chapter includes the following topics:

Preparing to install the VCS One client

This section lists what you must do and prepare before you can install the VCS One client.

- Perform the general preparations if you have not already.
  See "Preparing to install the VCS One client" on page 64.
- Perform platform-specific preparations.
  See "Platform-specific preparations" on page 64.
- Right before the installation, you must perform some setup tasks.
  See "Right before the installation" on page 66.

General preparations (all platforms)

Client installation involves a set of certain pre-installation tasks to be performed before you actually run the installer. These tasks are broadly divided in to the following categories:

- General preparations that are common irrespective of the platform on which you would install the client.
- Platform specific preparations.

Before you begin to install the VCS One client, ensure that the following general preparations are ready in advance.

- Uninstall any earlier version of the VCS One client.
  For uninstallation instructions, see the *Veritas Cluster Server One Installation Guide* for the VCS One version you want to uninstall.
- Ensure any DHCP IP addresses have a long-term lease and are not relinquished while the VCS One client daemon (vcsoneclientd) is running. The loss of connectivity could fault the VCS One client.
- Ensure the client host name resolves to the client IP address, and vice versa.

Platform-specific preparations

This section includes information and configurations you must prepare before you install the client on Linux or Solaris. Complete the preparations for your platform, and then proceed to:

"Right before the installation" on page 66.

Linux-specific preparations

Before you install the VCS One client on a Linux server system, you must first:

- Enable the required ports for Linux.
  See "Opening the required ports" on page 21.
- Install the required operating system patches. See the *Veritas Cluster Server One Release Notes* for the required operating systems patches.

Solaris-specific preparations

Before you install the VCS One client on a Solaris server system:

- Install the required operating system patches. See the *Veritas Cluster Server One Release Notes* for the required operating systems patches.

If you will install the VCS One client on a Solaris system with zones configured:

- Ensure that the zones have been completely installed, including an initial boot of the zone, before installing the VCS One client.

If you install the VCS One client on Solaris 10 systems running non-global zones:

- Ensure that /opt is not inherited by any non-global zone, using the following procedure:

To ensure that /opt is not inherited by any non-global zone command

1. Check whether /opt is inherited by a non-global zone command. Enter the following:

   zonecfg -z *zone_name* info

   Output similar to the following appears:

   ```
   zonepath: /export/home/zone1
   autoboot: false
   pool: yourpool
   inherit-pkg-dir:
           dir: /lib
   inherit-pkg-dir:
           dir: /platform
   inherit-pkg-dir:
           dir: /sbin
   inherit-pkg-dir:
           dir: /usr
   ```

2. Look for any occurrences of the /opt directory being inherited. If it is inherited, you see the following:

   ```
   inherit-pkg-dir:
           dir: /opt
   ```

3. If you see that the /opt directory is inherited, you must reinstall the zone.

Right before the installation

Right before you install the VCS One client, do the following:

- Set up ssh or rsh communications.
  - You must have ssh communications from the system where you run the installation to the systems where you are installing the VCS One client software.
  - Ensure that the specific ports needed for installing the VCS One client are enabled. See “Opening the required ports” on page 21.
  - The ssh communication must be present on the system where the installation is run and the Policy Master cluster systems.

  See “Setting up the Policy Master cluster hardware” on page 20.
- Make sure that the clock times for Policy Master systems in the same time zone are within 30 minutes of one another or the installation may fail.
- Make sure the Policy Master is running. On a Policy Master system, enter the following:

  # **haadmin -state**

  See “Verifying the Policy Master installation” on page 55.
- Choose the appropriate installation software disc. Installation software discs are provided for each platform type.
- Mount the software disc on the system where you plan to run the installation.
- Have the VCS One Policy Master virtual IP address ready. Communication must be enabled between the installer and the system with the Policy Master virtual IP address.

Deciding about a credential installation

Installing the VCS One client using credentials is optional. However, if you install the client without credentials, you must establish paswordless ssh communication between the client and the active Policy Master system.

For more information on setting up ssh communication, see “Configuring ssh, rsh, or remsh before installing.”

For a credential deployment, you have the following options:

- Install the client using a deployment credential. If you do not establish ssh communications with the active Policy Master system, you must have a copy of the deployment credential on the system from which you run the installer.

  See “Installing the client using a deployment credential” on page 67.

- Install the client using a permanent credential. If you do not establish ssh communications with the active Policy Master system, you must have a copy of the permanent credential on the system from which you run the installer.
  See "Installing the client using a permanent credential" on page 68.

Installing the client using a deployment credential

If the installer host does not have an ssh or rsh connection to the active Policy Master system, you can create a deployment credential. If passwordless ssh or rsh communication is enabled between the Policy Master system and the system from which you invoke the installer, skip to the section:

"Right before the installation" on page 66.

The deployment credential is a host-generic credential created on the authentication broker and copied to clients. Using a deployment credential, a client can be deployed without having a host-specific credential of its own.

Creating the deployment credential package

You can use the `-create_deployment_credential` option to create the deployment credential package on the shared storage. The clients copy and execute that credential package to authenticate with the Policy Master.

The command creates a deployment credential package file in the following location:

/vcsone_db_location/data/vcsone_deploy.credential

Reuse the credential package to deploy all clients that can connect to the Policy Master with the deployment credential.

Each client gets its own host-specific credential from the authentication broker through the Policy Master after the clients are deployed, and the first time they are connected to the Policy Master.

To create the deployment credential package

1. From the Policy Master, create the deployment credential package. You may either accept the default values or provide your own. Enter the following:
   # **/opt/VRTS/install/clientscript/*platform*/installvcsonecd -create_deployment_credential**
   where *platform* is the platform-specific directory.
   You see information about the installation.
2. Review the information and press **Enter** to continue.
3. Enter the timeout for the deployment credential in seconds. For example, enter the following: **86400**

4 Enter the virtual IP address of the Policy Master system. For example, enter the following: **192.168.1.20**

5 At the verification prompt, confirm that the timeout, Policy Master virtual IP address, and root broker hash are correct. Enter the following: **y**.
The credential file is created in the following location:
`/vcsonedb/data/vcsone_deploy.credential`

6 Use a program supported in your environment to copy the `vcsone_deploy.credential` file in binary mode from the Policy Master system to the client systems. For example, copy the file to `/var/tmp`.

7 Execute the package on the client machine. Enter the following:
/opt/VRTSvcsone/bin/haat execpkg -i *full_path_to_deployment_package* -o

Adding the client to the VCS One cluster

After you create the deployment credential package, you must add the client system to the VCS One cluster.

To add the client to the VCS One cluster

1 From the Policy Master, enter the following:
/opt/VRTSvcsone/bin/hasys -add *system* -platform *client platform*

2 From the Policy Master, set DeploymentTimeout to 86400 seconds (24 hours). Enter the following:
/opt/VRTSvcsone/bin/haclus -modify DeploymentTimeout 86400

3 Start the client. Enter the following:

Installing the client using a permanent credential

You can use the VCS One client daemon `-createcredential` installation option to perform installations on several systems without requiring ssh communication with the Policy Master cluster. The `-createcredential` option does the following:

- Creates authentication principals (identities) for each VCS One client process to be installed.
- Adds the client daemon systems to the Policy Master configuration.
- Transfers the credential packages to the system where you will run the installation.
- Uses the created credentials with `installvcsonecd` installation program.

To install the client using permanent credentials

1. Log in as root on the Policy Master system or on a system with passwordless ssh communication with the Policy Master.
2. Create authentication credential packages for each VCS One client system. Enter the following:
   ```
   # ./installvcsonecd -createcredential
   ```
   The installer lists the installation log location.
3. At the prompt, enter the system names, separated by a single space, where you want to install VCS One client daemon software or configure software already installed. For example, the names of the systems may be Sys1, Sys2, Sys3, and Sys4. (Do not enter fully-qualified domain names.)

   Note: Each system must run the same operating system.

   As the utility runs, it displays its actions and reports where it places the credential packages. It does not perform an installation.
4. Copy created credential packages to a system where you plan to install the VCS One client. Make a note of where you copy the files.
5. Install or configure the VCS One client daemon software on the systems specified in step 3. Enter the following:
   ```
   # ./installvcsonecd
   ```
6. During the installation, do the following:
   - At the permanent credential prompt, enter **y**.
   - Specify the path to the location where you copied the credential packages in step 4.

Installing the VCS One client

After you have completed the client installation, the client software will be running and the system will be part of the VCS One cluster.

If you have an earlier version of a VCS One client installed, you must completely uninstall it before installing the VCS One 5.0 client. For uninstallation instructions, see the *Veritas Cluster Server One Installation Guide* for the VCS One version you want to uninstall.

Before you install the VCS One client on a Solaris system with zones, ensure that the zones have been completely installed, including an initial boot of the zones.

Launching the installer

To launch the client installer

1. On the software disc, change directories to the platform-specific directory. Enter the following:
   # **cd *platform***
   where *platform* is the platform-specific directory, such as *sles10_x86_64* or *sol_sparc*.
   Go to the directory `cluster_server_one`.
2. Start the installer script. Enter the following:
   # **./installer**
3. From the Task menu, select the following task:
   Install/Upgrade a Product
4. From the list of products, select:
   Veritas Cluster Server One by Symantec - Client Daemon (VCS One Client)

   Note: When the installer installs software on a system where VCS is installed, any file system soft links in the directory `/opt/VRTS/bin` are overridden on the system. Running VCS and VCS One on the same system is not a supported configuration.
5. Accept the End User License Agreement (EULA). At the EULA prompt, enter the following: **y**.
   The installer provides information about the installation and configuration.
6. Review the information on each page and press **Enter** to continue.

Specifying the target systems

You must specify the name of the target systems for each client system.

To specify the target systems

- At the system names prompt, enter the names of the systems on which you want to install the VCS One client. Separate each name with a space. (Do not enter fully-qualified domain names or IP addresses.) For example, enter the following: **redhat95241 redhat95244**

Reviewing the package list

The installer provides a list of packages to be installed.

To review the package list

- Read the list of packages to be installed and press **Enter** to continue. For a list of the packages, see Appendix F, "Required packages" on page 203.

Specifying when to configure the client

You must specify whether to configure the client right after the installation, or complete the installation and configure the client later.

To specify when to configure the client

- At the client configuration readiness prompt, do one of the following:

To configure the client as part of the installation process	Enter the following: **`y`**. Go to the next section, "Configuring the VCS One client" on page 71.
To install the client now, but configure it later	Enter the following: **`n`**. The installer installs the packages, and you can configure the client later. When you are ready to configure the client, see the next section, "Configuring the VCS One client" on page 71.

Configuring the VCS One client

The client configuration procedures are in the following subsections:

Starting the client configuration

If you have not yet started the client configuration, do so now.

To start the client configuration

- Start the VCS One client configuration. Enter the following:
  `# /opt/VRTS/install/installvcsonecd -configure system_name`

Entering the virtual IP addresses for the client

You must enter the Policy Master virtual IP addresses that the client uses. You must also enter the base IP addresses for the subnets on which the Policy Master and client communicate.

1. Enter the Policy Master virtual IP addresses separated by a space. For example, enter the following:
   # **192.168.5.150 192.168.5.151**
2. At the Local IP address prompt for each client system, enter the local IP address of the client system NIC that will communicate with the Policy Master virtual IP address.
3. At the valid list of space-separated IP addresses prompt, for each client system, enter the base IP addresses for that system.
4. At the permanent credential package prompt, do one of the following:
   - If you have a permanent credential package, enter the following: **y**.
   - If you have a deployment credential, enter the following: **n**.
5. At the deployment credential package prompt, do one of the following:
   - If you have a permanent credential package, enter the following: **n**.
   - If you have a deployment credential, enter the following: **y**.

Deciding whether to configure the SSL library path

You can optionally configure the SSL library path.

To specify whether to configure the SSL library path

- At the SSL library path prompt, do one of the following:
  - If you do not want to configure the SSL library path, enter the following: **n**.
  - If you want to configure the SSL library path, enter the following: **y**. Then enter the SSL library path. The path must be to a directory that contains the libcrypto.so and libssl.so library files. For example, enter the following: **/usr/local/lib**.

The installer checks that ssh communications exist from the installation system to the root broker system, and that the clock time difference between the Policy Master and client is less than 30 seconds.

Synchronizing the clock times on your systems

The clock times between the client and Policy Master systems within the same time zone must be within 30 minutes of one another or the installation may fail. If the clock times are more than 1000 seconds apart, you see a warning.

To synchronize the clock times on your systems

1. Do one of the following:
   - If you do not see a warning about the clock times, go to the section "Completing and verifying the installation."
   - If you see a warning about the clock times, go to step 2.
2. At the clock time discrepancy prompt, decide if you want to continue configuring the client. Do one of the following:
   - To continue configuring the client, enter **y**.
   - To stop configuring the client, enter **n**.
3. If you want to synchronize the clock times, use the `ntpdate` command. For example, enter the following:

   rdate *ntphost*

Completing and verifying the installation

To complete and verify the installation

1. At the verification prompt, verify that the virtual IP addresses, base IP addresses, root broker hash, and the SSL library path (if configured) are correct. Enter the following: **y**.
2. At the start client prompt, choose whether to start the VCS One client processes. Do one of the following:
   - Follow the prompt to start the vcsoneclientd processes. Enter **y**.
   - Wait until later to start the vcsoneclientd processes. Enter **n**.
     When you are ready to start the client processes, you must enter the following: # **/opt/VRTSvcsone/bin/hastart -client**

   To view the installation logs. Enter the following:

   # **/var/VRTS/install/logs/**
3. On the Policy Master, verify that the client is up and running. Enter the following:

   # **hasys -state**
4. On the client, enter the following:

   # **ps -ef | grep vcsone**

Then check that the following resources are online:

```
vcsoneclientd.bin
vcsoneclientd.bin -shadow
```

After you install the VCS One client

- The VRTSvcsonemn package includes the VCS One online manual pages under /opt/VRTS/man. Add this path to the MANPATH environment variable for your platform. For instructions on how to set the MANPATH environment variable for your platform, see the *Veritas Server One Command Reference Guide*.
- To avoid having to reauthenticate your clients, do not change the Symantec Product Authentication Service (AT) ClusterName attribute value after you have deployed your clients. VCS One clients connect to the Policy Master cluster using authentication credentials with the domain name specified by the ClusterName attribute value. If the ClusterName attribute value is changed after VCS One clients have connected to the Policy Master cluster, the client systems must be reconfigured to reauthenticate them with the Policy Master.

  Therefore, if the ClusterName attribute value changes, you must restart the Policy Master service group (PMSG) (including the AT daemon vcsoneatd, the VCS One console, and the Policy Master) and reauthenticate all VCS One clients.

Chapter 5

Performing unattended client installations

This chapter includes the following topics:

About response files

Response files are pre-saved responses to questions that the client installer asks. Use a response file to perform unattended installations.

Choose a response file type that works with your configuration:

- Deployment credential installation. For unattended installations without predefined system credentials.
- Credential installation. For unattended installations with predefined system credentials.
- No credential installation. For installations performed without credentials.

Response file example

This example shows a deployment credential installation and configuration of the VCS One client on three systems (redhat1, redhat2, and redhat3) using the deployment credential: `/PM/data/vcsone_deploy.credential`

```
#
# installvcsonecd configuration values:
#
$CPI::CFG{OBC_MODE}="STANDALONE";
$CPI::CFG{OPT}{INSTALLCONFIG}=1;
$CPI::CFG{SYSTEMS}=[ qw(redhat1, redhat2, redhat3) ];
$CPI::CFG{UPI}="VCSONECD";
$CPI::CFG{VCSONECD_CC_ATPORT}=14159;
$CPI::CFG{VCSONECD_CLUSTERIP}=[ qw(10.198.92.127) ];
$CPI::CFG{VCSONECD_CREDPKG}="N";
$CPI::CFG{VCSONECD_DC_PMCOMM}="Y";
$CPI::CFG{VCSONECD_DC_TIMEOUT}=86400;
$CPI::CFG{VCSONECD_DEPLOYMENTCRED}="/PM/data/vcsone_deploy.credenti
al";
$CPI::CFG{VCSONECD_DEPLOYMENTCREDPKG}="Y";
$CPI::CFG{VCSONECD_LOCALIPS|{redhat1}{"10.198.92.127"}="None";
$CPI::CFG{VCSONECD_LOCALIPS|{redhat2}{"10.198.92.127"}="None"
$CPI::CFG{VCSONECD_LOCALIPS|{redhat3}{"10.198.92.127"}="None"
$CPI::CFG{VCSONECD_VALIDIP}{redhat1}="10.198.95.241";
$CPI::CFG{VCSONECD_VALIDIP}{redhat2}="10.198.95.242"
$CPI::CFG{VCSONECD_VALIDIP}{redhat3}="10.198.95.243"
```

See Appendix E, "Response file variables" for descriptions of each variables.

Using a response file from a previous installation

With each installation, the installation program generates a response file that documents what the user entered at each installation prompt. The response file is in the directory indicated at the end of the an installation; for example:

/var/VRTS/install/logs/installscript-*nnnn*/installscript-*nnnn*.response

where

- the suffix *nnnn* corresponds to an installation instance
- the *installscript* may be, for example:
  installer
  installvcsonepm
  installvcsonecd

Response file path:
`/var/VRTS/install/logs/installvcsonecd-G97Ahf/installvcsonecd-G97Ahf.response`

You may use a response file generated from a successful Veritas Cluster Server One (VCS One) installation, modifying it as needed, and use it to run another installation. This method is useful to install VCS One clients on multiple systems in an unattended mode.

Installation using a response file

You can edit a response file generated from a successful installation and place it in a specific directory on the system where you plan to run another installation. When you run the install program, use the -responsefile *response_file* option.

To perform an installation using a response file

1. Edit the response file and define values for the variables the installation requires. For example, save it as “response_file” in the `/tmp` directory.
2. Make sure that packages or Red Hat package management (RPM) systems to be installed have been upgraded.
3. Make sure the system where you run the installation command can communicate with the systems where the software is installed using ssh or rsh.
4. Make sure that the clock times on all systems in the same time zone are within 30 minutes of one another.
5. On the system where you want to run the installation, mount the software disc and navigate to the directory containing the installation program. Enter the following:
   ```
   cd cluster_server_one
   ```
6. Run the installer with the **-responsefile *path_to_response_file*** option. Enter the following:
   ```
   # ./installvcsonecd -responsefile /tmp/response_file
   ```

Note: If any older versions of VRTS RPMs or packages are on the target system, installation using the response file fails.

Chapter 6

Installing the Simulator

This chapter includes the following topics:

About the Simulator

You can use the Simulator to view, modify, and test the VCS One cluster configuration and behavior in a safe simulation that does not affect your production environment.

For more information about using the Simulator, see the *Veritas Cluster Server One User's Guide*.

Before you install the Simulator

You can install the VCS One Simulator software on one or more Windows systems. A Simulator is available for Windows only.

Before you install the Simulator, do the following:

- Ensure that the Windows version of the system where you will install the Simulator is at a level supported by this release. For supported operating system levels, see the *Veritas Cluster Server One Release Notes*.
- Choose any installation software disc. The Windows Simulator is available under the `simulator` directory on each VCS One installation software disc.

Installing the Simulator

The Simulator included in this release of VCS One can co-exist with earlier versions. Earlier versions of the Simulator use the same ports as the Simulator included in this release. If you have an earlier version of the Simulator, make sure that it is not running before you install the version included in this VCS One release.

To install the Simulator

1. Insert the VCS One software disc for any supported platform into the disc drive.
2. Navigate to the `simulator` directory. From there, open the `windows` directory.
3. Double click on vcsonesim.exe to start the VCS One Simulator installation wizard.
4. Click **Next** on the Welcome screen.
5. Accept the End-User Software License Agreement and click **Next**.
6. Check the destination folder where the VCS One Simulator will be installed.

- If you want to install the software in the displayed directory, click **Next**. By default, the Simulator is installed on the desktop in a directory named `VCSOne`.
- If you want to change the location for software installation, click **Browse...**

  Browse to the desired directory and click **OK**. Then, click **Next**.

  If you change the directory, the VCS One Simulator software is installed in the specified directory.

7 To begin installation, click **Next**. The VCS One Simulator installation wizard takes a few minutes to install the software.

8 When the VCS One Simulator installation wizard indicates that the installation is complete, click **Finish**.

The Simulator installer does not add any files outside of the directory where it installs the Simulator. The Simulator does not appear in **Add or Remove Programs**, the Start Up program, or in the registry. You may move the directory where the Simulator is installed to any location.

Chapter 7

Setting up authentication plug-ins for VCS One

This chapter includes the following topics:

About authentication plug-ins

Veritas Cluster Server One (VCS One) uses Symantec Product Authentication Service (AT) for security. The system is based on Secure Sockets Layer (SSL). AT lets product components verify the identity of other components and communicate securely. It also lets users log into VCS One securely.

Each authentication service type supported by VCS One has an authentication plug-in.

Supported authentication service types

For each authentication service type supported by VCS One, the authentication broker uses an authentication plug-in to validate the identities within a particular domain.

Table 7-1 lists the authentication service types and corresponding authentication plug-ins supported by VCS One.

Table 7-1 Authentication service types supported by VCS One

Authentication service type	AT plug-in name	Description
Symantec Private Domain	vx	Use with the Symantec Private Domain type.
UNIX password domain	unixpwd	Use with the UNIX password domain.
Network Information Service (NIS)	nis	Use with the NIS domain.
NIS+	nisplus	Use with the NIS+ domain.
Lightweight Directory Access Protocol (LDAP)	ldap	Use with both LDAP and Windows Active Directory. Supported LDAP server is: ■ Open LDAP 2.2 (RFC 2307)
Windows Active Directory	ldap	Use with both LDAP and Windows Active Directory. Supported Windows Active Directory server is: ■ Windows Active Directory 2003

Table 7-1 Authentication service types supported by VCS One (continued)

Authentication service type	AT plug-in name	Description
Pluggable Authentication Modules (PAM)	pam	Use with the PAM domain.

Displaying information about user names and domain names

The case sensitivity and length limits for user names and domain names varies depending on the authentication service type.

You can display information about the case sensitivity and length limit for user names and domain names for a specific authentication service type.

To display length limit and case sensitivity information for user names and domain names

- Enter the following command:

  # **/opt/VRTSvcsone/bin/haat showplugininfo -p *plugin_type***

  where *plugin_type* is the authentication plug-in type (that is, vx, unixpwd, nis, nisplus, ldap, or pam).

  The output looks similar to the following:

```
# /opt/VRTSvcsone/bin/haat showplugininfo -p ldap
Using data dir: /vad_db/data

showplugininfo
----------------------
----------------------

Plugin name:    ldap
Default Credential Expiry:      86400
User Credential Expiry: 86400
Service Credential Expiry:      31536000
Web Credential Expiry:  28800
Enabled Flag:   1
Do Not Load:    0
Max UserLength: 64
Is case sensitive:      yes
Found Domain(s) 2
**********************************
Domain Name:    VSS
Domain Type:    ldap
**********************************
```

```
Domain Name:    LDAP10
Domain Type:    ldap
**********************************
```

Case sensitivity

Table 7-2 shows authentication service types with case-sensitive user names and domain names:

Table 7-2 Case-sensitive authentication service types

Authentication service type	AT plug-in name
Symantec Private Domain	vx
UNIX password domain	unixpwd
Network Information Service (NIS)	nis
NIS+	nisplus
Pluggable Authentication Modules (PAM)	pam

Table 7-3 shows authentication service types with user names and domain names that are not case sensitive:

Table 7-3 Case-insensitive authentication service types

Authentication service type	AT plug-in name
Lightweight Directory Access Protocol (LDAP)	ldap
Windows Active Directory	ldap

Length limits

For Windows Active Directory and LDAP, Symantec recommends that you limit user names and domain names to 40 characters or less. (Windows and LDAP limit user names and domain names to 79 ASCII characters or less. If you use non-ASCII characters, the limit varies.)

Setting up vx authentication

To set up Symantec Private Domain (vx) authentication, add the user to the cluster private domain.

The user can then authenticate by using one of the following methods:

- Running `halogin` to set up the user profile
- Including the `-user` and `-domaintype` options with the commands from within client-side scripts
- Setting environment variables within the scripts

If a common password is acceptable, you can use batch scripts to gather the user IDs and create them with a random password to get the credentials for all of them. If the user IDs do not require separate passwords, you can automate the process.

To add a VCS One user to the private domain with the necessary privileges

1. On the active Policy Master system, see if a suitable private domain already exists. VCSONE_USERS is the default name of the vx private domain in VCS One. Enter the following:

   ```
   # /opt/VRTSvcsone/bin/haat showpd -t ab -d domain_name | grep \
   "domain_name"
   ```

   where *domain_name* in `grep "domain_name"` is the domain name you are searching for, such as VCSONE_USERS.

2. On the active Policy Master system, do one of the following:

If there is no private domain	Create a private domain with a distinct name. Enter the following:
	`# /opt/VRTSvcsone/bin/haat createpd -t \`
	`ab -d domain_name`
	where `-t` indicates that the private domain type is `ab` or authentication broker, and *domain_name* is the domain name.

If a private domain already exists	Check to see if the principal for this user is already there. Enter the following command:
	`# /opt/VRTSvcsone/bin/haat showprpl -t \`
	`ab -d domain_name -p principal_name`
	where `-t` indicates that the private domain type is `ab` or authentication broker, *domain_name* is the domain name, and *principal_name* is the name of the user who will run the scripts.

3. On the active Policy Master system, if the principal for this user already exists, delete it by entering the following command:

```
# /opt/VRTSvcsone/bin/haat deleteprpl -t ab -d domain_name \
-p principal_name -s
```

where `-t` indicates that the private domain type is `ab` or authentication broker, *`domain_name@cluster_domain`* is the name of the cluster private domain, and *`principal_name`* is the user name. `-s` indicates the silent option (that is, no feedback is given when you run the command with the `-s` option).

4 On the active Policy Master system, create a principal for the user on the cluster private domain by entering the following command:

```
# /opt/VRTSvcsone/bin/haat addprpl -t ab -d domain_name \
-p principal_name -s password -b host:port
```

5 On the active Policy Master system, get the root broker hash by entering the following command:

```
# /opt/VRTSvcsone/bin/haat showbrokerhash
```

6 On the client system, set up trust between the client system and the authentication broker by entering the following command:

```
# haat setuptrust -b host[{:port|:PBXPort:PBXServiceID}] \
-s low|medium|high
```

7 On the client system, authenticate the user by entering the following command:

```
# haat authenticate -d vx:VCSONE_USERS -p principal_name \
-s password -b brokerhost:port
```

8 On the client system, verify that the credential is in the local cache by entering the following command:

```
# /opt/VRTSvcsone/bin/haat showcred -j client
```

9 On the Policy Master system, add the user by entering the following command:

```
# /opt/VRTSvcsone/bin/hauser -add \
vxuser@domain_name@cluster_name
```

where *`vxuser`* is the user name, *`domain_name`* is the domain name, and *`cluster_name`* is the name of the VCS One cluster. By default, the VCS One cluster name is `vcsone_cluster`.

10 On the Policy Master system, add roles for the user by entering the following command:

```
# /opt/VRTSvcsone/bin/hauser -addrole \
vxuser@domain_name@cluster_name ServerFarmObjectGuest
```

11 On the client system, test that the user's login credentials work by running a VCS One "ha" command such as `hasys`:

```
# /opt/VRTSvcsone/bin/hasys -state -user vxuser -domaintype vx
```

Setting up unixpwd authentication

The UNIX password domain type (unixpwd) authenticates users based on `/etc/passwd` on the Policy Master system.

No set up is required for the unixpwd domain. You add VCS One users to the unixpwd configuration and give them the necessary privileges.

To add a VCS One user to the unixpwd configuration with the necessary privileges

1. Add the user by entering the following command:

   `# /opt/VRTSvcsone/bin/hauser -add unixuser@vcsone_cluster_name`

   where *unixuser* is the user name and *vcsone_cluster_name* is the name of the VCS One cluster. By default, the VCS One cluster name is `vcsone_cluster`.

2. Add roles for the user by entering the following command:

   ```
   # /opt/VRTSvcsone/bin/hauser -addrole \
   unixuser@vcsone_cluster_name ServerFarmObjectGuest
   ```

3. Test that the user's log in credentials work by running a VCS One "ha" command such as `hasys`:

   ```
   # /opt/VRTSvcsone/bin/hasys -state -user unixuser -domaintype \
   unixpwd
   ```

Setting up NIS or NIS+ authentication

To set up NIS or NIS+ authentication

1. Verify that you can log into VCS One on the Policy Master system with NIS or NIS+ credentials using ssh.
2. Add the user by entering the following command:

   `# /opt/VRTSvcsone/bin/hauser -add nisuser@nis_domain_name`

   where *nisuser* is the user name and *nis_domain_name* is the name of the NIS or NIS+ domain.

3. Add roles for the user by entering the following command:

   ```
   # /opt/VRTSvcsone/bin/hauser -addrole nisuser@nis_domain_name \
   ServerFarmObjectGuest
   ```

4. Test that the user's log in credentials work by running a VCS One "ha" command such as `hasys`.

For NIS, enter:

```
# /opt/VRTSvcsone/bin/hasys -state -user nisuser -domaintype nis
```

For NIS+, enter:

```
# /opt/VRTSvcsone/bin/hasys -state -user nisuser -domaintype \
nisplus
```

Setting up LDAP authentication

The LDAP configuration tool, `haldapconf`, is a command line interface (CLI) program that lets you configure the LDAP plug-in for the authentication broker. Use `haldapconf` to connect to the enterprise LDAP server and detect the default parameters for searching users and groups.

The `haldpaconf` configuration tool has the following options:

-d "discover"

Connects to the LDAP server and searches for the user and group attributes.

-c "createatcli"

Creates an authentication CLI. The authentication CLI is used to register the LDAP server in the VCS One authentication broker.

-x "atconfigure"

Configures authentication.

Figure 7-1 shows how the LDAP configuration tool works.

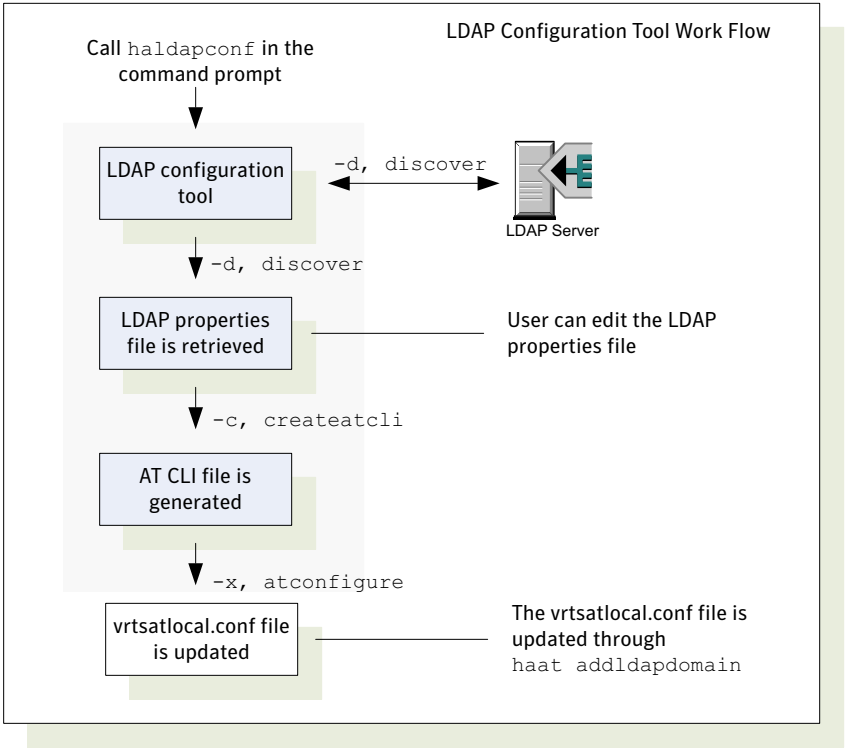


Figure 7-1 LDAP configuration tool workflow

To set up LDAP authentication

1 Connect to the LDAP server and search for the user and group attributes:

```
# /opt/VRTSvcsone/bin/haldapconf -d -s ldap_server_name \
[-p ldap_server_port] -u search_user -g search_group \
[-f attribute_list_file] [-m admin_username] \
[-w admin_password] [-l loglevel]
```

where:

- `-s ldap_server_name` specifies the name of the LDAP server. This option is required.

- `-p ldap_server_port` specifies the LDAP server port. The default value is 389. To bind the server, the command uses the user name and password. If you do not provide a user name and password, the command prompts you to provide them.
- `-u search_user` specifies the base search paths for users. This option is required.
- `-g search_group` specifies the base search paths for the group. This option is required.
- `-f attribute_list_file` specifies the name of the attribute list file. By default, the name is AttributeList.txt. This file is placed in the working directory.
- `-m admin_username` specifies the user name of the connecting user. When anonymous searches are disabled, this option is required to make the initial connection to the LDAP server.
- `-w admin_password` specifies the password of the connecting user. When anonymous searches are disabled, this option is required to make the initial connection to the LDAP server.
- `-l loglevel` generates a log file named haldapconf.debug. `loglevel` determines the amount of information that goes into the log. The value of `loglevel` ranges from 0 to 4.

The `haldapconf -d` command creates an attribute list file that contains the valid values for all the attributes in descending order of priority. This command also retrieves the valid values for the LDAP attributes that have multiple values.

For example, to run `haldapconf -d` for an LDAP server named ldapserver.com, a user named testuser, and a group named testgroup, enter the following command:

```
# /opt/VRTSvcsone/bin/haldapconf -d -s ldapserver.com \
-u testuser -g testgroup
```

2 Determine the highest priority attribute and create an authentication CLI that includes `haat addldapdomain` by running the following command:

```
# /opt/VRTSvcsone/bin/haldapconf -c -d domainname \
[-i attribute_list_file] [-o at_cli_file] [-a FLAT|BOB] \
[-s BASE|ONE|SUB] [-l loglevel]
```

where:

- `-d domain_name` specifies the domain name. The domain name must be unique.
- `-i attribute_list_file` specifies the name of the attribute list file. By default, the name is AttributeList.txt. The file is placed in the working directory.

- `-o` *`at_cli_file`* specifies the name of the AT CLI file. By default, the name is CLI.txt. This file is placed in the working directory.
- `-a FLAT|BOB` specifies the type of authentication. FLAT specifies that the database structure for LDAP is flat or non-hierarchical. BOB species that the database structure for LDAP is nested or hierarchical. By default, the authentication type is FLAT.
- `-s BASE|ONE|SUB` specifies the scope of the search. BASE is the primary level, ONE is one down from the primary level, and SUB is below ONE. By default, the scope is SUB.
- `-l` *`loglevel`* generates a log file named haldapconf.debug. *`loglevel`* determines the amount of information that goes into the log. The value of *`loglevel`* ranges from 0 to 4.

For example, to run `haldapconf -c` for a domain named myldapdomain1, enter the following command:

```
# /opt/VRTSvcsone/bin/haldapconf -c -d myldapdomain1
```

3 Add the LDAP domain by running the following command to configure authentication. This command reads and runs the AT CLI generated by `haldapconf -c` in step 2.

```
# /opt/VRTSvcsone/bin/haldapconf -x [-f at_cli_file] \
[-p at_install_path] [-o broker_port] [-l loglevel]
```

where:

- `-f` *`at_cli_file`* specifies the name of the AT CLI list file. By default, the name is CLI.txt. This file is placed in the working directory.
- `-i` *`at_install_path`* specifies the path `/opt/VRTSvcsone`.
- `-o` *`broker_port`* specifies the broker port. Unless you changed the broker port when you installed VCS One, the default VCS One broker port is 14159.
- `-l` *`loglevel`* generates a log file named haldapconf.debug. *`loglevel`* determines the amount of information that goes into the log. The value of *`loglevel`* ranges from 0 to 4.

For example, to run `haldapconf -x` for the default broker port for VCS One, enter the following command:

```
# /opt/VRTSvcsone/bin/haldapconf -x -o 14159 -p \
/opt/VRTSvcsone
```

4 Verify that the LDAP domain has been added and registered by entering the following command:

```
# /opt/VRTSvcsone/bin/haat listldapdomains
```

The output for this command is similar to the following:

```
Found: 1

Domain Name :           LDAP1
```

```
Server URL :            ldap://myldap.server1.com:389
SSL Enabled :           No
User Base DN :          ou=People, dc=mycompany,dc=corp,dc=com
User Object Class :     account
User Attribute :        uid
User GID Attribute :    gidNumber
Group Base DN :         ou=Group, dc=mycompany,dc=corp,dc=com
Group Object Class :    posixGroup
Group Attribute :       cn
Group GID Attribute :   memberUid
Group GID Attribute Type:
Auth Type :     FLAT
Admin User :
Admin User Password :
Search Scope :  SUB
```

Setting up Windows Active Directory authentication

VCS One supports the Windows Active Directory through the ldap authentication plug-in. Enable Active Directory for use with VCS One by following the procedure for LDAP.

See “Setting up LDAP authentication” on page 90.

Setting up PAM authentication

Pluggable Authentication Modules (PAM) authenticate users on the Policy Master system.

No set up is required for the PAM domain. You add VCS One users to the PAM configuration and give them the necessary privileges.

To add a VCS One user to the PAM configuration with the necessary privileges

1. Add the user by entering the following command:

   ```
   # /opt/VRTSvcsone/bin/hauser -add pamuser@vcsone_cluster_name
   ```

   where *pamuser* is the user name and *vcsone_cluster_name* is the name of the VCS One cluster. By default, the VCS One cluster name is vcsone_cluster.

2. Add roles for the user by entering the following command:

   ```
   # /opt/VRTSvcsone/bin/hauser -addrole \
   pamuser@vcsone_cluster_name ServerFarmObjectGuest
   ```

3. Test that the user’s log in credentials work by running a VCS One “ha” command such as hasys:

   ```
   # /opt/VRTSvcsone/bin/hasys -state -user pamuser -domaintype pam
   ```

Extending the credential expiry period

By default, logged-in VCS One users have a credential that expires in 24-hours. Users who need to run commands from within client-side scripts may require longer-term credentials.

You may change the default 24-hour expiry period to a larger value (such as two years) at the system level. Increasing the default value makes your job easier if the number of users with distinct passwords is relatively large.

You may change the expiry period in the authentication broker. With this approach, a user provides their password only once. They can run VCS One ("ha") commands without providing it until the end of the expiry period.

If you use this method, you must collect the credentials for these users quickly, before the expiry period can be reset to the original limit. When you are finished, you must reset the expiry period to its original setting. No matter how quickly you complete this process, there is a time window when other users can log in at the same time and acquire long-term credentials. Also, AT does not support revoking a granted credential.

Due to these issues, change the expiry period in the authentication broker only as a last resort and when the systems are not being used by users who should not have an extended expiry period.

To extend the expiry period

1. Display the current expiry period by entering the following command:
   # **/opt/VRTSvcsone/bin/haat showexpiryintervals -p *plugin_name***
   where *plugin_name* is the authentication plug-in name (that is, vx, unixpwd, nis, nisplus, ldap, or pam).
2. Increase the expiry period by entering the following command:
   # **/opt/VRTSvcsone/bin/haat setexpiryintervals -p *plugin_name* **
   -t user -e *seconds*
   where *seconds* indicates an expiry period in seconds. To set it for two years, use 63,072,000 seconds.
3. Verify the change by entering the following command:
   # **/opt/VRTSvcsone/bin/haat showexpiryintervals -p *plugin_name***
4. Have the users get new credentials.
5. Reset the expiry period to its original value. Enter the following:
   # **/opt/VRTSvcsone/bin/haat setexpiryintervals -p *plugin_name* **
   -t user -e 86400
6. where 86,400 indicates an expiry period of 86,400 seconds (24 hours). Verify the change. Enter the following:
   # **/opt/VRTSvcsone/bin/haat showexpiryintervals -p *plugin_name***

Setting the default domain and domain type

You must specify a user and domain type with VCS One commands. The `-user` *`user@domain`* option species the fully-qualified user name and the `-domaintype` *`domaintype`* option specifies the relevant domain type.

For the `-domaintype` *`domaintype`* option, accepted values for domaintype are unixpwd, nis, nisplus, ldap, pam, and vx (which is the Symantec Private Domain). These values are case sensitive.

You may set a default domain and domain type using the DefaultAuthDomain attribute so that you do not have to enter the domain and domain type each time you run a command.

To set the default domain and domain type

- Enter the following command:

  ```
  # /opt/VRTSvcsone/bin/haclus -modify DefaultAuthDomain \
  domaintype:domainname
  ```

Accepted values for the DefaultAuthDomain attribute are in the form *`domaintype:domainname`*. Examples include ldap:lab1.com (where lab1.com is a Windows Active Directory domain) and nis:lab2.com (where lab2 is a NIS domain).

By default, the `unixpwd` and `pam` domain types do not require a domain name. They assume the authentication broker host name or the VCS One cluster name based on the UseClusterNameAsDomainName attribute.

After you set the DefaultAuthDomain attribute, VCS One commands use the specified domain and domain type as the default. After that, you do not have to specify the domain and domain type with the `-domaintype` *`domaintype`* option when you run a command.

After you set a default domain and domain type, when you run a command with the `-domaintype` *`domaintype`* option, it will override the default.

Note: The domain type `unixpwd` should only be used for users who are local to the UNIX system. When the domain type `unixpwd` is used, the domain name is ignored and the local system's domain name is used instead. For example, if the user, *`user@domain`*, is authenticated with the domain type `unixpwd` on a system named system1, the user's credential is `user@system1` instead of the actual domain name.

For more information on modifying attributes, see the *Veritas Cluster Server One User's Guide*.

Chapter 8

Adding shared storage and testing disks for SCSI-3 compliance

This chapter includes the following topics:

About adding shared storage

This section describes how to set up a system with SCSI-3 protection for shared storage.

If two or more systems in the Policy Master cluster share storage devices, you can configure and use the I/O fencing feature in VCS One. In the event of a network failure, I/O fencing protects the shared storage from data corruption.

Requirements for adding shared storage

To meet the requirements for shared storage in a production environment, you must supply the following:

- Three coordinator disks that support SCSI-3 persistent reservations. This is a requirement for I/O fencing, and applies only to the Policy Master. Clients do not require coordinator disks.
- Two switches for I/O connection redundancy.

Adding storage devices

For the Policy Master in a production environment, you need to add a minimum of three coordinator disks in addition to the storage for data. This requirement does not apply for clients.

To add storage devices to the VCS One cluster

1. Physically connect each storage device to each system in the Policy Master cluster.
2. On each system in the VCS One cluster, scan the drives, update the Veritas Volume Manager (VxVM) device list, and reconfigure VxVM DMP with the new devices with the following command:
   ```
   vxdisk scandisks
   ```
3. On one system in the VCS One cluster, initialize the disks with the following command:
   ```
   vxdiskadm
   ```
4. Choose **1 Add or initialize one or more disks** from the menu.
5. At the prompt, to select devices, type **`list`**.
6. Type the name of the devices you are adding when prompted to select devices. Do one of the following:
   - For Solaris or AIX, enter the following:
     ```
     c3t1d0 c3t2d0
     ```

- For Linux, enter the following:
  sdx

7 At the `Which disk group` prompt, enter **none**.
  You create disk groups later.
  For details on creating disk groups, see "Setting up and testing the coordinator disks" on page 103.

8 Initialize the disk as the default.

9 Exit the utility. Type **q**.

To verify each system sees the same added devices (optional)

From each system, the names of the added disks may be different. By using a command to check the serial number of the disk, you can verify that a specific disk is the same one as seen from each system. This is important when you have added many disks.

- Use the following command on each system, making sure that the device path is the appropriate one from each system (they are likely to be different):
  vxfenadm -i *device_path*

In the output, examine the serial number and verify it is the same disk.

Testing disks for SCSI-3 compliance

Test the data disks you are going to use for SCSI-3 compliance and I/O fencing support.

Use the following procedure to test the data disks for either the Policy Master cluster system or client systems.

Setting up and testing data disks

Verify that each disk you added for use as a data disk supports SCSI-3 persistent reservations and I/O fencing. Use the `vxfentsthdw` utility to verify that the storage you added supports SCSI-3 persistent reservations. The procedure may destroy data on the disk.

Note: If the disks you want to test have data on them that you want to preserve, use the -r (read-only) option of vxfentsthdw. Be advised that, with the -r option, not all SCSI-3 compliance tests are run.

When you run the utility, you are prompted for:

- The names of two systems connected to the storage disks.
- The name of the disk as it is displayed on each system. A given disk may have a different name on each system.

To test data disks using vxfentsthdw

1. Make sure the two systems are connected to the storage device you are testing, and that the systems are running the same operating system.
2. Ensure that both systems have mutual connectivity via rsh or ssh communications.
3. Start `vxfentsthdw`. Enter the following. If you are using ssh, omit the `-n` option:

   `/opt/VRTSvcsone/vxfen/bin/vxfentsthdw -n`
4. At the prompts, provide the required information. If the test succeeds, the following information is displayed:

   ```
   The disk /dev/disk_name is ready to be configured for I/O
   Fencing on node name_of_first_node
   The disk /dev/disk_name is ready to be configured for I/O
   Fencing on node name_of_second_node
   ```

   If the testing does not display a message that the disk is ready to be configured for I/O fencing, the disk has failed the testing.
5. Repeat this test on all shared data disks connected to the system.

Using additional vxfentsthdw options

Table 8-1 lists the `vxfentsthdw` options you can use to test disks.

Table 8-1 Options for vxfentsthdw

vxfentsthdw option	Description	When to use
`-m`	The default option that may be used with the `-r` option. With `-m`, `vxfentsthdw` runs in the interactive mode.	For testing a few disks or sampling disks in larger arrays.
`-f` *`filename`*	Tests system and device combinations listed in a text file. May be used with `-r` option.	For testing several disks.
`-g` *`disk_group`*	Tests all disk device in a specified disk group. May be used with `-r` option.	For testing many disk and arrays of disks. Disk groups may be temporarily created for testing purposes and destroyed (ungrouped) after testing.
`-r`	Read-only option. May be used with `-m`, `-f`, and `-g` options.	Testing does not overwrite data on the disks. The utility does not run all SCSI-3 compliance tests.
`-n`	Use this option if you are running the `vxfentsthdw` utility using `rsh`.	When `rsh` is used for communication.

Testing system and device combinations

To test system and device combinations

1. Create a text file to test the two disks. For example, you can create a file to test two disks (`/dev/`*`device_1`* and `/dev/`*`device_2`*) shared by two systems (*`sysA`* and *`sysB`*):

   ```
   sysA /dev/device_1 sysB /dev/device_1
   sysB /dev/device_2 sysA /dev/device_2
   ```

   The file contains one line for each disk to be tested.

2. Name the file. For example, `red_disks`.

3. Do one of the following:

- To display the test results on the command, enter the following:
  /opt/VRTSvcs/vxfen/bin/vxfentsthdw -f red_disks
- To redirect the test results to a text file, precede the command with "yes" to acknowledge that testing destroys data on the disks to be tested. For example:
  echo yes | /opt/VRTSvcs/vxfen/bin/vxfentsthdw -f red_disks > red_test.txt

Caution: When redirecting the test output to a file, the warning that the test destroys does not show until after the test is complete.

Testing all the disks in a disk group

To test all the disks in a disk group

1. Create a temporary disk group for testing the disks. For example, create a disk group called `blue_disks_dg` that includes all the disks in the disk array.
2. Import the disk group. Do not use the `-n` option.
3. Do one of the following:
   - To display the test results on the command, enter the following:
     /opt/VRTSvcs/vxfen/bin/vxfentsthdw -g blue_disk_dg
   - To redirect the test results to a text file, precede the command with "yes" to acknowledge that testing destroys data on the disks to be tested, as in this example:
     echo yes | /opt/VRTSvcs/vxfen/bin/vxfentsthdw -g blue_disks_dg > blue_test.txt
4. After completing the test, you can destroy the temporary disk group and put the disks into disk groups as needed.

Setting up Policy Master I/O fencing

The procedures in this section apply to production environments, where the Policy Master database is on shared storage.

Setting up and testing the coordinator disks

This section assumes that your Policy Master cluster includes coordinator disks that support SCSI-3 persistent reservations and I/O fencing.

See "Adding storage devices" on page 98, and "Testing disks for SCSI-3 compliance" on page 99.

Follow the procedures in this section to set up a disk group for your coordinator disks, and test the coordinator disk group.

Setting up a disk group for coordinator disks

Create the disk group starting with a single disk, and add other disks to the group.

To set up a disk group for coordinator disks

1. Create a disk group with a single disk. For example, enter the following:
   ```
   vxdg init vxfencoorddg sdA
   ```
   Where ***vxfencoorddg*** is the name of the disk group, and ***sdA*** is the name of the disk.
2. Add the other disks to the disk group. For example, enter the following:
   ```
   vxdg -g vxfencoorddg adddisk sdB
   vxdg -g vxfencoorddg adddisk sdC
   ```
   Where ***sdB*** and ***sdC*** are the names of the disks.

Testing the coordinator disk group

Use vxfentsthdw to test the coordinator disk group.

To test the coordinator disk group

1. Make sure the two systems are connected to the same storage devices you are testing.
2. Start vxfentsthdw. Enter the following. If you are not using ssh, omit the -n option:
   ```
   vxfentsthdw -n -c vxfencoorddg
   ```
3. Provide the system information at the prompts. The utility reports its progress on each disk in the disk group.

When each test succeeds, the display indicates the disk is ready to be configured for I/O fencing as a COORDINATOR DISK.

Creating I/O fencing configuration files and starting I/O fencing

After setting up and testing the coordinator disk group, follow the instructions in this section to configure it for use. When you are finished, shut down and restart the systems

Create the I/O fencing configuration file, `/etc/vxfendg`. The rc script uses that configuration file to generate the I/O fencing configuration file, `/etc/vxfentab`, that is required by the I/O fencing driver. Create the I/O fencing configuration file, `/etc/vxfenmode`, that configures the vxfen module to use either DMP devices or underlying raw character devices.

To create the /etc/vxfendg and /etc/vxfenmode files

1. Deport the disk group. Enter the following:
   `vxdg deport vxfencoorddg`
2. Import the disk group to prevent it from being imported automatically when the system reboots. Enter the following:
   `vxdg -t import vxfencoorddg`
3. Deport the disk group again, so it is prevented from being used for other purposes. Enter the following:
   `vxdg deport vxfencoorddg`
4. On each system, create the `/etc/vxfendg` file. Enter the following:
   `echo "vxfencoorddg" > /etc/vxfendg`
   Make sure there are no spaces between the quotation marks.
5. Create `/etc/vxfenmode`. On each system in the VCS One cluster, enter the command that corresponds to the SCSI-3 mode you have chosen. Do one of the following:
   - For DMP configuration, enter the following:
     `cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode`
   - For raw device configuration, enter the following:
     `cp /etc/vxfen.d/vxfenmode_scsi3_raw /etc/vxfenmode`

Setting the UseFence attribute to specify SCSI3 as its value

To set the UseFence attribute to specify SCSI3 as its value

- On each system on which you want to configure I/O fencing, enter the following:

  `haclus -modify UseFence SCSI3`

About VCS One client I/O fencing

If a system in the VCS One cluster loses connectivity with Policy Master cluster, I/O fencing prevents shared storage from being corrupted. The I/O fencing mechanism for client systems is based on SCSI-3 persistent reservations.

Consider the following scenario. Multiple systems in the VCS One cluster use a common shared storage. Due to a network fault, one of these systems loses its connectivity with the Policy Master cluster.

In the meantime, the Policy Master does not receive heartbeat signals from the disconnected system and instructs another system on the service group's SystemList to force import the shared disk group. The other SystemList system invalidates the disconnected system's registration keys on the shared storage and replaces them with its own. The service group that includes the storage resource then fails over to the other system.

Chapter 9

Adding a new or replacement system to the Policy Master cluster

This chapter includes the following topics:

Prerequisites for the new or replacement system

The system you are adding as a new or replacement Policy Master cluster system must meet the following requirements:

- Run the same supported operating system software and version, and have the same patch level as the existing systems.
- Install and configure a storage architecture, such as Storage Foundation. Storage Foundation adds Veritas Volume Manager, Veritas File System, and Veritas Cluster Server software to the new system.
  See "Installing the VCS One Policy Master" on page 36.
- If you are replacing a system, use the same identity as the system it is replacing, including the same:
  - Hostname
  - IP address
  - NIC device names
  - Shared storage

About adding or replacing a system

You may include up to four systems in the Policy Master cluster. The procedures vary depending on whether you are expanding the Policy Master cluster or you are replacing a faulted Policy Master cluster system.

Adding or replacing a system involves the following tasks:

- Connecting the new or replacement system to the Policy Master cluster
- Installing the VCS One Policy Master cluster software on the new or replacement system
- Adding the new or replacement system to the Policy Master cluster

Adding a system to the Policy Master cluster

Before you add the VCS One software to the new system, physically add the system to the Policy Master cluster.

Setting up the hardware

Connect the new system to the Policy Master cluster and shared storage.

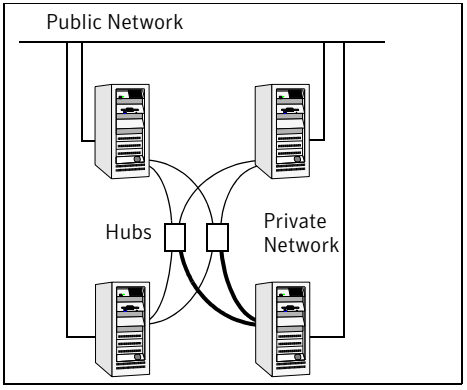
To set up the hardware

1 Connect the VCS One private Ethernet controllers. Do one of the following:

- If you are expanding from a Policy Master cluster with two systems, use independent hubs for private network connections, replacing crossover cables if used.
- If you already use independent hubs, connect the two Ethernet controllers on the new system to the independent hubs.

Figure 9-1 illustrates a new system being added to a three-system Policy Master cluster using two independent hubs.

Figure 9-1 Adding a system to a three-node Policy Master cluster using two independent hubs



2 Connect the system to the shared device storing the Policy Master configuration database.

3 Configure the new system to use the Policy Master systems' ssh key.
See "Setting up the Policy Master cluster hardware" on page 20.

Adding a system to the VCS One Policy Master cluster

This section provides instructions for adding a new system to your VCS One Policy Master cluster.

For information on replacing a faulted system, see “Replacing a system in the VCS One Policy Master cluster” on page 112.

The steps for adding a system may vary, depending on your configuration.

Verifying that the VCS One Policy Master service group is online

In the following steps, you are adding system1 to a Policy Master cluster that includes system2.

To verify that the VCS One Policy Master service group is online

1 Verify that the VCS One Policy Master system is online. Enter the following:

```
# /opt/VRTSvcsone/bin/haadmin -state
```

2 Check that the Policy Master packages are installed on the system that you are adding to the Policy Master cluster. Enter the following:

```
# rpm -qa |grep vcsone
```

Starting the process of adding a system

To start the process of adding a system

1 Navigate to the directory that contains the upgrade script. For example, enter the following:

```
# cd /opt/VRTS/install
```

2 Add the VCS One Policy Master to the Policy Master cluster. Enter the following:

```
# ./installvcsonepm -addnode
```

Specifying the target systems

You must specify the name of the system that you want to add to the Policy Master cluster, and the system in the Policy Master cluster to which you want to add the system.

1 At the prompt, enter the name of the Policy Master system that you want to add to the Policy Master cluster. For example, enter the following:

```
system1
```

2 At the prompt, enter the name of the system to which you want to add the Policy Master system. For example, enter the following: **system2**

You see a list of information that you need to prepare so that you can add the system.

3 Press **Enter**.

Configuring the Policy Master cluster

You must specify an ID for the Policy Master cluster, and configure the heartbeat settings.

For instructions, see the following topics:

- "Creating an ID for the Policy Master cluster" on page 45.
- "Configuring the heartbeat settings" on page 45.

Entering the NIC for the Policy Master virtual IP address

To enter the NIC for the Policy Master virtual IP address

1 Enter the NIC for the Policy Master Virtual IP address to use on your system. From the list of NIC devices discovered on your systems, select any NIC that is up and running on a public network. For example, enter the following:

- (On Linux) **`eth0`**
- (On Solaris x64) **`bge0`**

2 At the Policy Master virtual IP address configuration verification prompt, confirm that the virtual IP address is correct. Enter **`y`**.

Entering the NICs for disaster recovery

To enter the NICs for disaster recovery

1 For each unique virtual IP address, enter the public NIC. For example, enter the following:

- (On Linux) **`eth0`**
- (On Solaris x64) **`bge0`**

2 At the disaster recovery configuration verification prompt, verify that the virtual IP address and NIC information is correct. Enter the following: **`y`**.

Verify the VCS One operations on the new system

To verify the VCS One operations on the new system

1 Check the status of your Policy Master cluster. Enter the following:

```
# /opt/VRTSvcsone/bin/haadmin -state
```

2 Check to see that the new system is up and running. Enter the following:

```
# /opt/VRTSvcsone/bin/haadmin -switch PMSG -to system1
```

Replacing a system in the VCS One Policy Master cluster

If you are replacing a faulted Policy Master cluster system, you may restore the existing authentication service configuration and use it to configure authentication service on the new system.

The instructions in this section assume the following:

- You have a Policy Master cluster with two nodes, system1 and system2.
- Your system1 is faulted.
- You are replacing system1 with another node (named system1).

The steps for adding a system may vary, depending on your configuration.

To replace a system on the VCS One Policy Master cluster

1 Edit the VCS configuration file, main.cf. Enter the following:

```
# /opt/VRTSvcs/bin/haconf -makerw
```

2 Remove the faulted system, system1. Enter the following:

```
# /opt/VRTSvcs/bin/hagrp -modify PMSG SystemList -delete
sys1
# /opt/VRTSvcs/bin/hagrp -modify VCShmg SystemList
-delete sys1
# /opt/VRTSvcs/bin/hasys -delete sys1
```

3 Add the replacement system, system1. Enter the following:

```
# /opt/VRTS/install/installvcsonepm -addnode
```

4 Write the changes to the configuration file, main.cf. Enter the following:

```
# /opt/VRTSvcs/bin/haconf -dump -makero
```

5 Check the status of your Policy Master cluster. Enter the following:

```
# /opt/VRTSvcsone/bin/haadmin -state
```

6 Check to see that the new system is up and running. Enter the following:

```
# /opt/VRTSvcsone/bin/haadmin -switch PMSG -to system1
```

Chapter 10

Upgrading from VCS One 2.0.1 to 5.0

This chapter includes the following topics:

Overview

This chapter provides information on upgrading Policy Master and client systems from VCS One 2.0.1 to VCS One 5.0.

See Appendix B, "Sample Policy Master upgrade scenarios" for sample upgrade scenarios.

What the upgrade supports

The VCS One upgrade feature supports the following:

- Running the VCS One 5.0 Policy Master in parallel with the VCS One 2.0.1 Policy Master to minimize down time
- Migrating all the AT configuration files and configuration database files from VCS One 2.0.1 to VCS One 5.0

Operating system prerequisite

Before you upgrade, check that you are running an operating system that VCS One 5.0 supports. If necessary, install or upgrade to a supported operating system.

For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.

Not supported

The upgrade does not support the following:

- Policy Master upgrades with no shutdown time.
- Upgrades for versions earlier than VCS One 2.0.1.
- Upgrades for incorrectly configured Policy Master systems.
- Upgrading the root broker system before the other systems. (The root broker should be upgraded last).
- Upgrading from a Policy Master cluster that uses an external root broker.
- VCS One 2.0.1 Windows clients connected to the VCS One 5.0 Policy Master.

Configuration changes

When you upgrade from VCS One 2.0.1 to 5.0, the installer changes your 2.0.1 configuration to make it compatible with VCS One 5.0. This section provides details about those changes.

VAL-related objects

When you upgrade from VCS One 2.0.1 to 5.0, the installer removes all 2.0.1 VAL-related objects, roles, user privileges.

Deprecated attributes

When you upgrade from VCS One 2.0.1 to 5.0, the installer removes the following deprecated attributes:

- ClusterName and ClusterDomainName Policy Master cluster attributes
- LinkedFrame system attribute
- GTQDisplayName group attribute
- NumCPU LDom resource attribute

ManualMode restart for the VCS One cluster

VCS One 5.0 does not support ManualMode restarting of the VCS One cluster. If the RestartMode is set to `ManualMode` in VCS One 2.0.1, the installer changes it to `Normal` for VCS One 5.0.

User-modified attribute properties

If you changed any VCS One 2.0.1 attribute properties using `haattr -setproperty`, those changes will be lost when you upgrade to VCS One 5.0. Similarly, if you added custom attributes using `hattr - add`, the properties for those attributes will take on the default VCS One 5.0 values.

Upgrading the Policy Master

This section provides instructions on upgrading the Policy Master, including:

This subsection provides instructions on creating a cluster ID and specifying the Policy Master virtual IP address:

Adding a system to a VCS One 5.0 Policy Master cluster

See Chapter 9, "Adding a new or replacement system to the Policy Master cluster" for instructions on adding a system to your Policy Master cluster.

Exporting your VCS One 2.0.1 configurations

Follow the steps in this section to export your VCS One 2.0.1 configurations to a local drive, or to a remote location. This process exports the Symantec Product Authentication Service (AT) and database configurations.

Verifying VCS One operations on the new system

To verify VCS One operations on the new system

- Check that the Policy Master service group is online. Enter the following:
  # **/opt/VRTSvcsone/bin/hagrp -state**

Exporting your configurations

To export your configurations

1. Navigate to the directory that contains the export script. For example, enter the following:
   # **cd /mnt/rhel5_x86_64/cluster_server_one/**
2. Run the export utility. Enter the following:
   # **./installvcsonepm -export**

3 At the prompt, enter the name of the Policy Master system from which to export your configurations. For example, enter the following:

```
# my_machine1
```

The export script gives you the option of saving the exported data to a remote location.

4 Do one of the following:

To save the exported data locally	Enter the absolute path to the directory. For example, enter the following: **/tmp/backup**
To save the exported data to a remote location	Enter the hostname or IP address followed by a colon ":" and the path to the directory. For example, enter the following: **192.168.1.100:/tmp/backup**

Verifying that the exported configurations are saved to the specified location

To verify that the exported configurations are saved to the specified location

- Enter the following:

```
# ls -l /tmp/backup
```

Deleting a system from your VCS One 2.0.1 Policy Master cluster

Follow the steps in this section to delete a system from your VCS One 2.0.1 Policy Master cluster.

To delete a system from your VCS One 2.0.1 Policy Master cluster

1 Navigate to the VCS One directory on your root broker system. For example, navigate to the following location:

```
[root@my_machine2 cluster_server_one]#
```

2 Delete the system. Enter the following:

```
# ./installvcsonepm -deletenode
```

3 At the prompt, enter the name of the system that you want to delete from the Policy Master cluster. For example, enter the following:

my_machine1

4 At the removal confirmation prompt, confirm the deletion. Enter the following: **y**.

You see a status message with information about the deletion.

5 Check that your system is running. Enter the following:
hasys -state

6 Check that your Policy Master service group is online. Enter the following:
hagrp -state

7 Check the VCS One 2.0.1 Policy Master cluster status. Enter the following:
ps -ef | grep VRTS
All VCS One 5.0 processes are stopped.

Importing your 2.0.1 configurations to VCS One 5.0

After you export your VCS One 2.0.1 configurations, you can import those configurations to the 5.0 Policy Master. This process imports the Symantec Product Authentication Service (AT) and database configurations.

Verifying that the 5.0 Policy Master packages are installed on each system

To verify that the 5.0 Policy Master packages are installed on each system

- After you install the 5.0 Policy Master packages on each system in the Policy Master cluster, you must verify that the packages are installed. For each system, enter the following:
rpm -qa |grep VRTS

Starting the import process

To start the import process

1 Navigate to the directory that contains the import script. For example, enter the following:
cd /mnt/rhel5_x86_64/cluster_server_one/

2 Navigate to the VCS One directory on your root broker system. For example, go to the following location:
[root@my_machine2 cluster_server_one]#

3 Import the configurations. Enter the following:
./installvcsonepm -import
You see some information on what you need to prepare to perform the import.

4 Read each page and press **Enter**.

Specifying the target systems

You must specify the names of the systems on which you want to import the VCS One 2.0.1 configurations.

To specify the target systems

1. At the system names prompt, enter the names of the systems on which you want to import the VCS One 2.0.1 configurations. Separate each name with a space. Do not enter fully-qualified domain names or IP addresses. For example, enter the following: **`sys1 sys2`**
2. Do one of the following:

If you are not prompted about installing VCS One on a single system	Go to the next section, "Deciding about Storage Foundation."
If you are prompted about installing VCS One on a single system	Enter **`y`** to continue importing your configurations on a single Policy Master system.

Deciding about Storage Foundation

Symantec recommends that you use a Storage Foundation as your shared storage architecture. If Storage Foundation is not installed on all Policy Master systems, you must confirm that you want to continue without installing Storage Foundation.

To decide about Storage Foundation

- Do one of the following:

If you are not prompted about continuing without Storage Foundation	Go to the next section, "Specifying the location of the exported configurations."
If you are prompted about continuing without Storage Foundation	Enter **`y`** to continue importing your configuration without Storage Foundation.

Specifying the location of the exported configurations

You must specify the location of the exported authentication and database configurations.

To specify the location of the exported configurations

- At the saved Policy Master configurations prompt, do one of the following:

If your configurations are backed up to a remote location	Enter the hostname or IP address followed by a colon ":" and the path to the directory. For example, enter the following: **`192.168.1.100:/tmp/backup`**
If your configurations are backed up locally	Enter the absolute path to the directory containing the exported authentication and database data. For example, enter the following: **`/tmp/backup`**

Completing the import process

For the rest of the import process, complete the same steps you would complete during a regular Policy Master installation.

See the following sections:

- "Configuring the Policy Master cluster" on page 44
- "Specifying the authentication services port number" on page 46
- "Configuring virtual IP addresses for the Policy Master" on page 46
- "Choosing a storage architecture to configure" on page 48
- "Configuring your storage architecture" on page 51
- "Configuring disaster recovery" on page 48
- "Starting the Policy Master" on page 54

Verifying that the configurations are imported to the specified location

To verify that the configurations are imported to the specified location

- Enter the following:

  # **`/opt/VRTSvcsone/bin/hagrp -state`**

Migrating your 2.0.1 configurations to VCS One 5.0

Follow the steps in this section to migrate your 2.0.1 authentication and database configurations to VCS One 5.0. This process migrates the Symantec Product Authentication Service (AT) and database configurations.

Starting the migration

To start the migration

1 Navigate to the directory that contains the migration script. For example, enter the following:

```
# cd /mnt/rhel5_x86_64/cluster_server_one/
```

2 Start the migration. Enter the following:

```
# ./installvcsonepm -migrate
```

You see some information about the migration process.

3 Press **Enter**.

Specifying the target systems

You must specify the names of the 2.0.1 systems that contain your configurations, and the target VCS One 5.0 systems to which you want to migrate your 2.0.1 configurations.

To specify the target systems

1 Enter the names of the 2.0.1 systems. For example, enter the following:

```
my_machine1 my_machine2
```

2 At the system names prompt, enter the names of the target VCS One 5.0 systems to which you want to migrate the 2.0.1 configurations. Separate each name with a space. Do not enter fully-qualified domain names or IP addresses. For example, enter the following: **sys1 sys2**

3 Do one of the following:

If you are migrating the configuration to more than one system	Go to step 4.
If you are migrating the configuration to a single system	At the prompt asking you to confirm the migration to a single system, enter the following: **y**. Then, go to step 4.

4 At the prompt for confirming that you want to migrate your configurations to VCS One 5.0, enter **y**.

Completing the migration process

For the rest of the migration process, complete the same steps you would complete during a regular Policy Master installation.

For the remaining migration steps, see the following sections:

- "Configuring the Policy Master cluster" on page 44
- "Specifying the authentication services port number" on page 46
- "Configuring virtual IP addresses for the Policy Master" on page 46
- "Choosing a storage architecture to configure" on page 48
- "Configuring your storage architecture" on page 51
- "Configuring disaster recovery" on page 48
- "Starting the Policy Master" on page 54

(Optional) Creating an ID for the VCS One 5.0 Policy Master cluster and specifying the virtual IP addresses

Follow the steps in this section to create an ID for your VCS One 5.0 Policy Master cluster, and specify the Policy Master virtual IP addresses.

Verifying that the VCS One 5.0 Policy Master service group is online

To verify that the VCS One 5.0 Policy Master service group is online

- Enter the following:
  # **/opt/VRTSvcsone/bin/hagrp -state**

Creating an ID for the 5.0 Policy Master cluster and specifying the virtual IP address

To create an ID for the 5.0 Policy Master cluster and specify the virtual IP address

1. Navigate to the directory that contains the upgrade script. For example, enter the following:
   # **cd /mnt/rhel5_x86_64/cluster_server_one/**
2. Run the command for creating an ID for the Policy Master cluster and specifying the virtual IP address. Enter the following:
   ./installvcsonepm -cidvip
3. Enter the name of the system for which you want to create an ID for the 5.0 Policy Master cluster and specify a virtual IP address. For example, enter the following:
   my_machine2

4 Enter a unique ID between 0-65535. For example, enter the following:
`Cluster ID Number:` **`4333`**
You see a list of information that is required to configure the Policy Master.

5 Enter the NIC for the Policy Master virtual IP address. For example:
- (On Linux) **`eth0`**
- (On Solaris x64) **`bge0`**

6 At the prompt, specify whether or not you want to use the same NIC on all of the Policy Master systems.
Type **`y`** to use the same NIC on all of the Policy Master systems. Type **`n`** to use different NICs for different Policy Master systems.
If more than one base IP address is detected, select a base IP address.

7 Do one of the following:

If you are not prompted the select a base IP address	Go to step 8.
If you are prompted the select a base IP address	Select a base IP address. Then go to step 8.

8 Enter one or more virtual IP addresses for the Policy Master. For example, enter the following:
`192.168.1.102`

9 Enter the netmask for the Policy Master virtual IP address. For example, enter the following:
`255.255.252.0`

10 Verify that the virtual IP address and NIC information is correct. Enter the following: **`y`**.

11 At the prompt, allow the Policy Master to restart. Enter the following: **`y`**.
You see a message stating whether the ID and virtual IP address were updated successfully.

Verify that the ID and virtual IP addresses were updated successfully

To verify that the ID and virtual IP addresses were updated successfully

1 Enter the following:
`#` **`/opt/VRTSvcsone/bin/hagrp -state`**

2 Verify that the new virtual IP address is enabled. Enter the following:
`#` **`ifconfig -a`**

Upgrading the client

This section provides instructions for upgrading the VCS One client from 2.0.1 to 5.0, including the following subsections:

Backing up your 2.0.1 configurations

Before you upgrade your 2.0.1 client systems to VCS One 5.0, you should back up the configurations on each of your client systems.

To back up your 2.0.1 configurations

1. Create a backup directory on each client system. Enter the following:
   # **mkdir /backup**
2. Copy the vcsone.conf file into the backup directory for each system. Enter the following:
   # **cp /etc/VRTSvcsone/vcsone.conf /backup/**
3. Check that the service groups on each client system are up and running. Enter the following:
   # **/opt/VRTSvcsone/bin/hagrp -state**

Uninstalling the 2.0.1 client on one system

Follow the instructions in this section to uninstall one of your client systems.

You will uninstall the rest of the systems in a later section, "Upgrading the 2.0.1 client to 5.0 on additional systems" on page 125.

To uninstall the 2.0.1 client system

1. Log in as root on the client system.
2. Navigate to the directory containing the VCS One installer. Enter the following:
   # **cd /opt/VRTS/install/**
3. Start the uninstallation script. Enter the following:
   # **./uninstallvcsonecd my_machine3**

4 Follow the instructions for uninstalling the client software, with one exception: At the service group evacuation prompt, enter **n** to leave the service groups in their current state.
See Chapter 11, "Uninstalling VCS One software" for uninstallation instructions.

Installing and configuring the 5.0 client

After you uninstall the 2.0.1 client, follow the instructions in this section to install and configure that system as a VCS One 5.0 client system.

To install and configure the 5.0 client

1 Log in as root on the client system.

2 Start the installation script. Enter the following:
```
# ./rhel5_x86_64/installer my_machine3
```

3 From the Task menu, select the following task:
```
Install/Upgrade a Product
```

4 From the list of products, select:
```
Veritas Cluster Server One by Symantec - Client Daemon
(VCS One Client)
```

5 Follow the instructions for installing the client software.
See Chapter 4, "Installing and configuring the VCS One client" for installation instructions.

Upgrading the 2.0.1 client to 5.0 on additional systems

After you have upgraded one of your client systems, follow the instructions in this section to upgrade additional systems.

To upgrade the 2.0.1 client to 5.0 on additional systems

1 Follow the instructions to uninstall a 2.0.1 system.
See Appendix 10, "" on page 124.

2 Follow the instructions to install and configure the 5.0 client.
See "Installing and configuring the 5.0 client" on page 125.

3 Make sure the client system is in the RUNNING state. Enter the following:
```
# /opt/VRTSvcsone/bin/hasys -state
```

4 Check that the service groups are up and running on the client system. Enter the following:
```
# /opt/VRTSvcsone/bin/hagrp -state
```

Chapter 11

Uninstalling VCS One software

This chapter includes the following topics:

Uninstalling the VCS One software

To uninstall Veritas Cluster Server One (VCS One) software, use the uninstallation programs provided. On systems where the software has been installed, you can find the uninstallation programs in the directory `/opt/VRTS/`install.

The uninstallation programs are also provided on the VCS One software discs.

Uninstalling high availability agent software

In addition to the agents bundled with the product, VCS One provides agents for the management of key enterprise applications. See the following documentation available on the Agent Pack disc:

- For an overview of the supported high availability agents, read the *Veritas High Availability Agent Pack Getting Started Guide*.
- For uninstallation instructions, read the agent installation and configuration guides.

Uninstalling Policy Master server software

The uninstallation script uninstalls the Policy Master, which configures and manages the VCS One environment. The uninstallation script can also optionally uninstall Veritas Storage Foundation. Veritas Storage Foundation combines Veritas Volume Manager (VxVM) and Veritas File System (VxFS) to provide online storage management.

To uninstall the software from remote systems at this time, make sure ssh or rsh is configured between the system where you plan to run the uninstall program and the other systems where you are uninstalling the software.

See “Setting up the Policy Master cluster hardware” on page 20.

To uninstall the VCS One Policy Master server software

1. On the system where the VCS One Policy Master is installed, go to the directory containing the uninstallvcsonepm program. Enter the following:

   `cd /opt/VRTS/install`

   If you plan to use the uninstallation program in on the software disc, mount the appropriate disc by platform. Enter the following:

   `cd platform`

   where *`platform`* is the platform-specific directory, such as *`sles10_x86_64`* or *`sol_sparc`*.

   Go to the directory `cluster_server_one`.

2 Start the Policy Master uninstallation script. Enter the following:
`./uninstallvcsonepm`

3 At the system name prompt, enter the name of each system where you want to uninstall the VCS One Policy Master. Separate the names with a space. (Fully-qualified domain names and IP addresses are acceptable.) For example, enter the following: **`sys1 sys2`**
You are prompted to uninstall storage if you installed Storage Foundation when you installed the VCS One Policy Master.

4 At the Storage Foundation uninstallation prompt, do one of the following:
- If installed Storage Foundation when you installed the Policy Master, and you want to uninstall Storage Foundation, enter **`y`**.
- If did not install Storage Foundation when you installed the Policy Master, or if you do not want to uninstall Storage Foundation, enter **`n`**.

5 At the uninstallation confirmation prompt, confirm that you are sure about uninstalling the VCS One Policy Master. Enter the following: **`y`**. (Entering **`n`** aborts the uninstallation.)
The program stops the Policy Master.
If you are installing on Solaris, you must close any open volumes on your system. Open volumes are volumes that are mounted and used by another application. If you try to uninstall the VCS One Policy Master while there are open volumes on the system, the uninstallation may fail.

6 If you are installing on Solaris, close any open volumes and confirm that there are no open volumes on your system. At the open volumes prompt, enter **`n`**.

7 At the residual VCS One program removal prompt, decide if you want to delete the `/opt/VRTSvcsone`, `/etc/VRTSvcsone`, and `/var/VRTSvcsone` directories. Do one of the following:
- To remove the directories, enter **`y`**.
- To keep the directories, enter **`n`**.

Note: If the VCS One Policy Master is installed on the node where you are running the uninstall program, be careful not to remove residual program directories that the Policy Master is using.

The program uninstalls the software and indicates where the uninstallation logs are placed.

Uninstalling the VCS One client software

The uninstallation script uninstalls the VCS One client, which communicates securely with the Policy Master, and starts and stops the agents on the local system.

To uninstall the software from remote systems at this time, make sure ssh or rsh is configured between the system where you plan to run the uninstall program and the other systems where you are uninstalling the software.

When `uninstallvcsonecd` removes software on a system where VCS is installed, any file system soft links in the directory `/opt/VRTS/bin` are removed on the system. Running VCS and VCS One on the same system is not a supported configuration. To work around this issue, uninstall VCS and reinstall VCS One. For testing purposes only, if you need both products installed, replace the removed soft links.

See "Setting up the Policy Master cluster hardware" on page 20.

Launching the installer

Launching the installer

1. On the system where the VCS One client is installed, go to the directory containing the uninstallvcsonecd program. Enter the following:

   `cd /opt/VRTS/install`

   If you plan to use the uninstallation program on the software disc, mount the appropriate disc by platform. Enter the following:

   `cd` ***`platform`***

   where *`platform`* is the platform-specific directory, such as *`sles10_x86_64`* or *`sol_sparc`*.

   Go to the directory `cluster_server_one`.

2. Start the client uninstallation script. Enter the following:

   `./uninstallvcsonecd`

Specifying the system to uninstall

To specify the system to uninstall

1. At the system name prompt, enter the name of each system where you want to uninstall the VCS One client daemon software. If you have more that one system, separate the names by a space. (Fully-qualified domain names and IP addresses are acceptable.)
2. At the uninstallation confirmation prompt, enter the following: **`y`**.

Deciding about evacuating service groups

If there are any service groups that are online or intended to go online on the system, you can choose to evacuate them from this system or leave them in the current state. If you evacuate the service groups, they are brought offline and fail over to another system, if possible. If you do not evacuate the service groups, the installer leaves them in their current state.

To decide about evacuating service groups

- At the service group evacuation prompt, specify if you want to evacuate the service groups that are currently online. Enter one of the following: **y** or **n**.

Removing residual directories

Symantec recommends that you remove the following residual VCS One program directories: `/opt/VRTSvcsone`, `/etc/VRTSvcsone`, and `/var/VRTSvcsone`.

To remove residual directories

- Remove the recommended residual VCS One program directories. Enter **y**.

The program uninstalls the software and indicates where uninstallation logs are placed.

Removing directories from a local zone on Solaris

When you uninstall the VCS One client a global zone, the following directories are not deleted from your local zones:

- `/.vcsoneprofile`
- `/var/VRTSvcsone/data`

You must manually remove these directories from your local zones manually.

To manually remove directories from your local zones

- Run the removal command for each directory. Enter the following:

```
$> /usr/bin/rm -f /.vcsoneprofile
$> /usr/bin/rm -fr /var/VRTSvcsone
```

Uninstalling the Simulator

The following section describes how to uninstall the Simulator.

To uninstall the Simulator

1. Make sure that all Simulator instances are stopped. If a Simulator instance is running, stop it using the following command at the Windows command prompt:

   installation_location*\VCSOne\hamultisim -stopsim *instance_name

   where *installation_location* is the directory location where you installed the Simulator and *instance_name* is the name of the running Simulator instance. If multiple Simulator instances are running, enter this command for each Simulator instance.
   You can stop the Simulator by running a script or entering a command.

   To stop the default Simulator instance, do one of the following:

   - At the Windows command prompt, run the following batch file script:
     ***installation_location*\VCSOne\stopsim.bat**
   - At the Windows command prompt, enter the following command:
     ***installation_location*\VCSOne\hamultisim -stopsim default**

2. If you used the `-hosts` option with `hamultisim -addsim` when you created the Simulator instance, do one of the following:

   - At the Windows command prompt, run the following command to remove the Simulator instance and delete its entry from the hosts file:
     installation_location*\VCSOne\hamultisim -removesim \ *instance_name
   - Manually edit the hosts file to remove the unwanted entries. The hosts file is located here:
     `C:\WINDOWS\system32\drivers\etc\hosts`

3. Go to the directory where you installed the Simulator.

4. Select the `VCSOne` subdirectory.

5. Delete the `VCSOne` subdirectory and its contents.
   Deleting the `VCSOne` subdirectory removes the Simulator from the system.

Appendix A

Reinstalling the Policy Master

This appendix includes the following topic:

Reattaching existing clients to the Policy Master

If you reinstall the Policy Master, you need to reattach existing VCS One clients to the Policy Master.

To reattach existing clients to the Policy Master

1. Back up the VCS One database configuration:
   /opt/VRTSvcsone/bin/haconf -dbtoxml *backup_dir*
2. Back up the VxSS configuration on all Policy Master systems:
   /opt/VRTSvcsone/bin/haadmin -backup -vss *backup_dir*
3. To uninstall the Policy Master, see "Uninstalling Policy Master server software" on page 128.
4. To re-install the Policy Master, follow the procedure in "Installing the VCS One Policy Master" on page 36.
5. Freeze the Policy Master service group (PMSG):
   /opt/VRTSvcsone/bin/haadmin -freeze
6. Kill the process vcsoneatd.
   /opt/VRTSvcsone/bin/pkill -9 vcsoneatd.bin
7. Restore the VxSS configuration on all Policy Master systems:
   /opt/VRTSvcsone/bin/haadmin -restore -vss *backup_dir*
8. Restart the vcsoneatd process on all Policy Master systems:
   /opt/VRTSvcsone/bin/vcsoneatd
9. Unfreeze the PMSG:
   /opt/VRTSvcsone/bin/haadmin -unfreeze
10. Stop the Policy Master:
    /opt/VRTSvcsone/hastop -pm
11. Restore the VCS One configuration:
    /opt/VRTSvcsone/bin/haconf -loaddb -force *backup_dir*
12. Start the Policy Master:
    /opt/VRTSvcsone/bin/hastart -pm
13. Execute haat setuptrust on each Policy Master system.
    /opt/VRTSvcsone/bin/haat setuptrust -b *virtual IP address for the broker port* -s low -j client
14. Stop the web server:
    /opt/VRTSvcsone/bin/hastop -web
15. Restart the web server:
    /opt/VRTSvcsone/bin/hastart -web

Appendix B

Sample Policy Master upgrade scenarios

This chapter includes the following topics:

Upgrade scenario overview

Table B-1 provides a summary of the Policy Master upgrade scenarios, and points you to more information about each scenario. All of the upgrade scenarios assume your VCS One 2.0.1 configuration has two policy master systems.

Table B-1 Upgrade scenarios

Upgrade scenario	Description
Simplified upgrade (two systems imported)	Use this upgrade scenario for a test environment or production environment. After you upgrade to VCS One 5.0 using this scenario, you can roll your configuration back to VCS One 2.0.1. This scenario has no verification phase, and requires you to import two new systems. This upgrade scenario has the shortest down time, and the fewest steps. See "Performing a simplified upgrade and importing two new systems" on page 137.
Simplified upgrade (no systems imported)	Use this upgrade scenario for a test environment only. After you upgrade to VCS One 5.0 using this scenario, you cannot roll your configuration back to VCS One 2.0.1. This scenario has no verification phase, and does not require you to import any new systems. See "Performing a simplified upgrade without importing systems" on page 139.
Verified upgrade (two systems imported)	Use this upgrade scenario for a test environment or production environment. After you upgrade to VCS One 5.0 using this scenario, you can roll your configuration back to VCS One 2.0.1. This scenario has a verification phase, and requires you to import two new systems. See "Performing a verified upgrade and importing two new systems" on page 141.
Verified upgrade (no systems imported)	Use this upgrade scenario for a test environment or production environment. After you upgrade to VCS One 5.0 using this scenario, you must reload packages to roll your configuration back to VCS One 2.0.1. This scenario has a verification phase, and does not require you to import any new systems. "Performing a verified upgrade without importing systems" on page 144.

Upgrade scenario details

This section provides instructions for each of the upgrade scenarios.

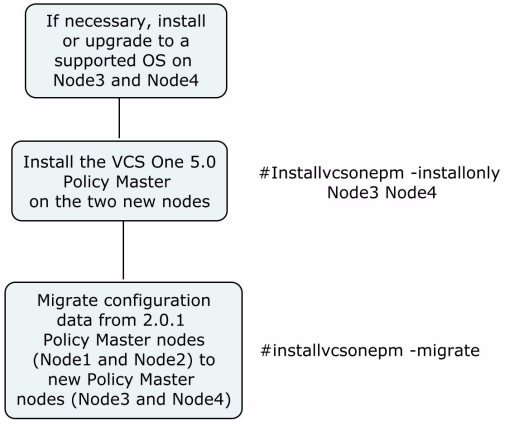
For information about the different scenarios, see: “Upgrade scenario overview” on page 136.

Performing a simplified upgrade and importing two new systems

Use this upgrade scenario for a test environment or production environment. If the VCS One 5.0 Policy Master upgrade fails, you can roll your configuration back to VCS One 2.0.1.

This scenario has no verification phase, and requires you to import two new systems. This upgrade scenario has the shortest down time, and the fewest steps.

Figure B-1 Performing a simplified upgrade and importing two new systems



Installing the VCS One 5.0 Policy Master on two new systems

Follow the instructions in this section to install the Policy Master on two new systems in the Policy Master cluster. When the installation is complete, the new VCS One 5.0 systems (Node3 and Node4) replace the previous 2.0.1 systems (Node1 and Node2).

To install the VCS One 5.0 Policy Master on two new systems

1 Check that Node3 and Node4 are running an operating system that VCS One 5.0 supports. Do one of the following:

- If Node3 and Node4 are running a supported operating system, skip to step 2.
- If Node3 and Node4 are not running a supported operating system, install or upgrade to a supported operating system. Then, go to step 2.

For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.

2 Install two new VCS One 5.0 systems (Node3 and Node4). You do not need to configure the systems. Use the -installonly option to install the VCS One packages over the systems. Enter the following:

```
# ./installvcsonepm -installonly
```

For more information about installing Policy Master systems, see Chapter 2, "Installing and configuring the VCS One Policy Master" on page 35.

Migrating configuration and database data to a new system

Migrate the VCS One 2.0.1 Symantec Product Authentication Service and database data. Migrate the data from Node1 and Node2 (in the 2.0.1 Policy Master cluster) to Node3 and Node4 (in the 5.0 Policy Master cluster).

To migrate the configuration data and database data to the new systems

◆ Enter the following:

```
# ./installvcsonepm -migrate
```

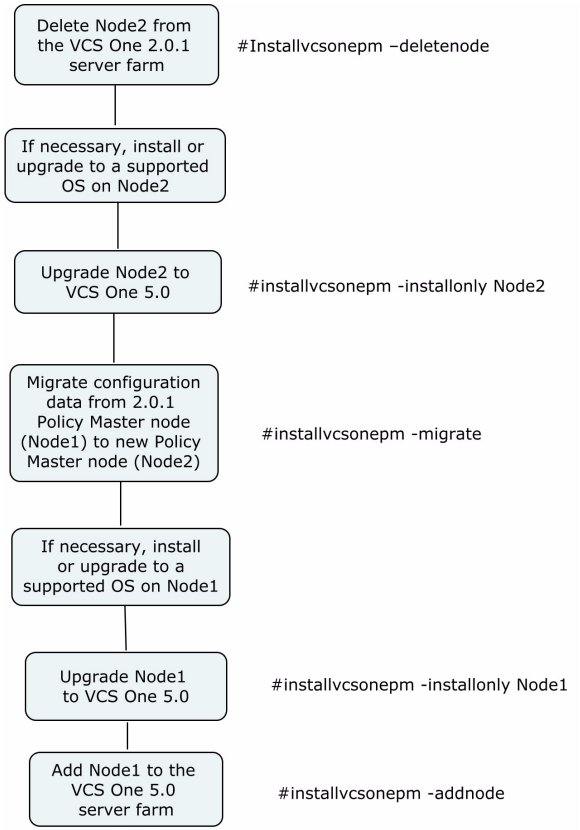
For more information on migrating configuration and database data, see "Migrating your 2.0.1 configurations to VCS One 5.0" on page 120.

Performing a simplified upgrade without importing systems

Use this upgrade scenario for a test environment only. After you upgrade to VCS One 5.0 using this scenario, you cannot roll your configuration back to VCS One 2.0.1.

This scenario has no verification phase, and does not require you to import any new systems.

Figure B-2 Performing a simplified upgrade without importing systems



Deleting a VCS One 2.0.1 system and upgrading it to 5.0

Follow the instructions in this section to delete a VCS One 2.0.1 system, and upgrade that system to VCS One 5.0.

To delete a VCS One 2.0.1 system and upgrade it to 5.0

1 Delete Node2 from your 2.0.1 Policy Master cluster. Enter the following:

```
# ./installvcsonepm -deletenode
```

See: "Deleting a system from your VCS One 2.0.1 Policy Master cluster" on page 117.

2 Check that Node2 is running an operating system that VCS One 5.0 supports. Do one of the following

- If Node2 is running a supported operating system, skip to step 3.
- If Node2 is not running a supported operating system, install or upgrade to a supported operating system. Then, go to step 3.

For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.

3 Upgrade Node2 to VCS One 5.0. Enter the following:

```
# ./installvcsonepm -installonly
```

See: "Installing the VCS One 5.0 Policy Master on two new systems" on page 137.

Migrating configuration and database data to a new system

Migrate the VCS One 2.0.1 Symantec Product Authentication Service and database data. Migrate the data from Node1 to Node2.

To migrate the configuration data and database data to the new system

- Enter the following:

```
# ./installvcsonepm -migrate
```

For more information on the migration process, see "Migrating your 2.0.1 configurations to VCS One 5.0" on page 120.

Upgrading a 2.0.1 system and adding it to the 5.0 Policy Master cluster

Follow the instructions in this section to upgrade Node1 to VCS One 5.0, and then add it to the VCS One 5.0 Policy Master cluster.

To upgrade a 2.0.1 system and add it to the VCS One 5.0 Policy Master cluster

1 Check that Node1 is running an operating system that VCS One 5.0 supports. Do one of the following

- If Node1 is running a supported operating system, skip to step 2.
- If Node1 is not running a supported operating system, install or upgrade to a supported operating system. Then, go to step 2.

For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.

2 Use the Policy Master installer to upgrade Node1 to VCS One 5.0. You don't need to configure the system. Use the -installonly option to install the VCS One packages over the systems. Enter the following:

```
# ./installvcsonepm -installonly
```

For more information about installing Policy Master systems, see Chapter 2, "Installing and configuring the VCS One Policy Master" on page 35.

3 Add Node1 to the 5.0 Policy Master cluster. Enter the following:

```
# ./installvcsonepm -addnode
```

See: Chapter 9, "Adding a new or replacement system to the Policy Master cluster".

Performing a verified upgrade and importing two new systems

Use this upgrade scenario for a test environment or production environment. If the VCS One 5.0 Policy Master upgrade fails, you can roll your configuration back to VCS One 2.0.1.

This scenario requires a verification phase. During the verification phase, both the VCS One 2.0.1 and the 5.0 Policy Master clusters are running. The VCS One 2.0.1 clients should use the 2.0.1 Policy Master cluster.

Installing the VCS One 5.0 Policy Master on two new systems

Follow the instructions in this section to install two new systems in the Policy Master cluster. When the installation is complete, the new VCS One 5.0 systems (Node3 and Node4) replace the previous 2.0.1 systems (Node1 and Node2).

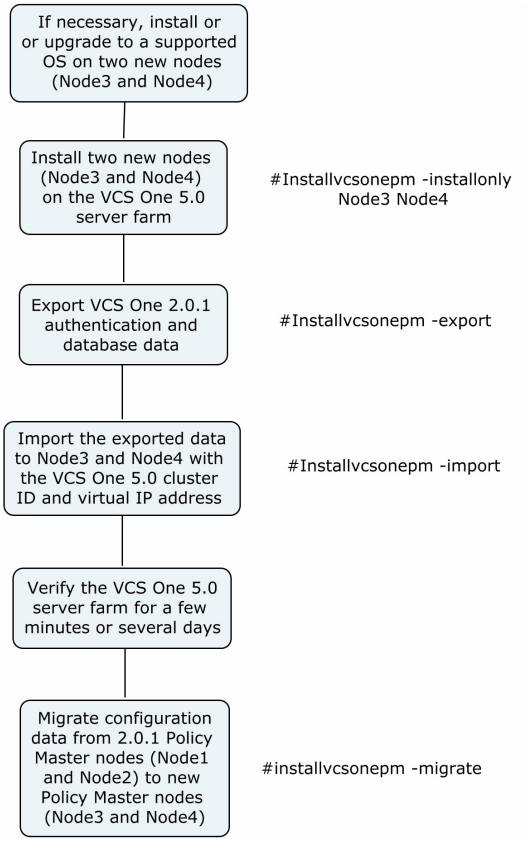
To install the VCS One 5.0 Policy Master on two new systems

1 Check that Node3 and Node4 are running an operating system that VCS One 5.0 supports. Do one of the following

- If Node3 and Node4 are running a supported operating system, skip to step 2.
- If Node3 and Node4 are not running a supported operating system, install or upgrade to a supported operating system. Then, go to step 2.

For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.

Figure B-3 Performing a verified upgrade and importing two new systems



2 Install two new VCS One 5.0 systems (Node3 and Node4). You don't need to configure the systems. Use the -installonly option to install the VCS One packages over the systems. Enter the following:

```
# ./installvcsonepm -installonly
```

For more information about installing Policy Master systems, see Chapter 2, "Installing and configuring the VCS One Policy Master" on page 35.

Importing configuration and database data to the new systems

Export configuration and database data from Node1 and Node2 to a directory on the system running the installer script, and import it into Node3 and Node4.

To import configuration and database data to the new systems

1 Export the Symantec Product Authentication Service and database data on the 2.0.1 Policy Master cluster Node1 and Node2. Enter the following:

```
# ./installvcsonepm -export
```

See: "Exporting your VCS One 2.0.1 configurations" on page 116.

2 Import the exported data to Node3 and Node4. Enter the following:

```
# ./installvcsonepm -import
```

See: "Importing your 2.0.1 configurations to VCS One 5.0" on page 118.

Verifying VCS One operations on the new systems

Verify the VCS One operations on Node3 and Node4 for as long as you choose. The verification period can last from several minutes to days.

To verify VCS One operations on the new system

- Monitor the Policy Master service group to ensure that it is continuously online. Enter the following:

```
# /opt/VRTSvcsone/bin/hagrp -state
```

Migrating configuration and database data to the new systems

Migrate the VCS One 2.0.1 Symantec Product Authentication Service and database data. Migrate the data from Node1 and Node2 (on the VCS One 2.0.1 Policy Master cluster) to Node3 and Node4 (on the VCS One 5.0 Policy Master cluster).

To migrate configuration and database data to the new systems

- Enter the following:

```
# ./installvcsonepm -migrate
```

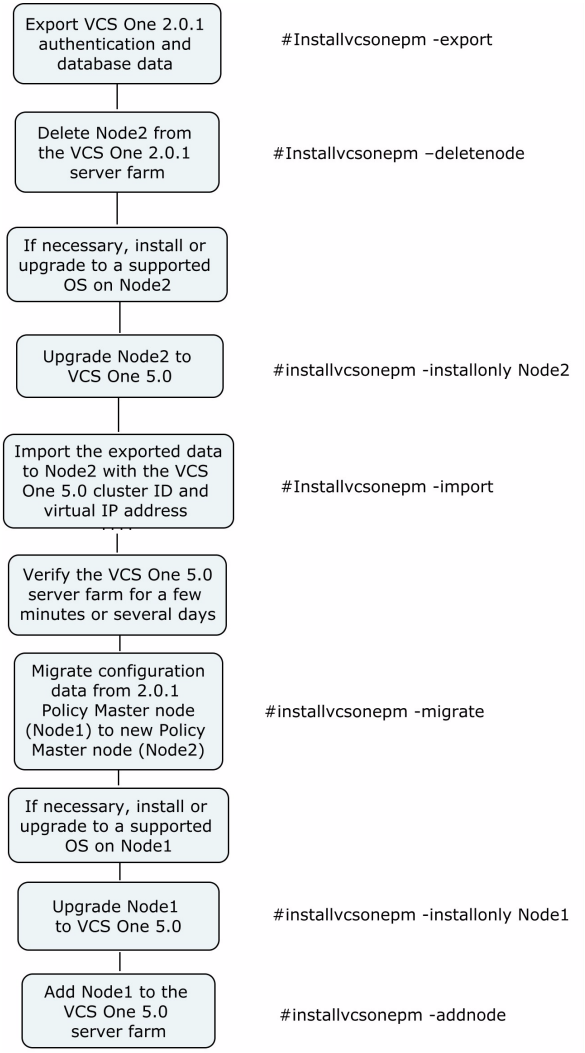
For more information on migrating configuration and database data to the new systems, see "Migrating your 2.0.1 configurations to VCS One 5.0" on page 120.

Performing a verified upgrade without importing systems

This scenario assumes that you have a 2.0.1 Policy Master cluster with two systems.

This scenario requires a verification phase. During the verification phase, both the VCS One 2.0.1 and the 5.0 Policy Master clusters are running. The VCS One 2.0.1 clients should use the 2.0.1 Policy Master cluster.

Performing a verified upgrade without importing systems



Deleting a VCS One 2.0.1 system and upgrading it to 5.0

Follow the instructions in this section to delete a system from your 2.0.1 Policy Master cluster, and upgrade it to VCS One 5.0.

To delete a VCS One 2.0.1 system and upgrade it to 5.0

1. Export the Symantec Product Authentication Service and database data on the VCS One 2.0.1 Policy Master Node2. Enter the following:

   # **./installvcsonepm -export**

   See: "Exporting your VCS One 2.0.1 configurations" on page 116.

2. Delete Node2 from your VCS One 2.0.1 Policy Master cluster. Enter the following:

   # **./installvcsonepm -deletenode**

   See: "Deleting a system from your VCS One 2.0.1 Policy Master cluster" on page 117.

3. Check that Node2 is running an operating system that VCS One 5.0 supports. Do one of the following

   - If Node2 is running a supported operating system, skip to step 4.
   - If Node2 is not running a supported operating system, install or upgrade to a supported operating system. Then, go to step 4.

   For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.

4. Use the Policy Master installer to upgrade Node2 to VCS One 5.0. You don't need to configure the system. Use the -installonly option to install the VCS One packages over the systems. Enter the following:

   # **./installvcsonepm -installonly**

   For more information about installing Policy Master systems, see Chapter 2, "Installing and configuring the VCS One Policy Master" on page 35.

Importing configuration and database data to a new system

Follow the instructions in this section to import the configuration data and database data to a new system.

To import configuration and database data to a new system

- Import the exported data to Node2. Enter the following:

  # **./installvcsonepm -import**

  See: "Importing your 2.0.1 configurations to VCS One 5.0" on page 118.

Verifying VCS One operations on the new system

Verify the VCS One operations on Node2 for as long as you choose. The verification period can last from several minutes to days.

To verify VCS One operations on the new system

- Monitor the Policy Master service group to ensure that it is continuously online. Enter the following:

  # **/opt/VRTSvcsone/bin/hagrp -state**

Migrating configuration and database data to a new system

Migrate the VCS One 2.0.1 Symantec Product Authentication Service and database data. Migrate the data from Node1 to Node2

To migrate configuration and database data to a new system

- Enter the following:

  # **./installvcsonepm -migrate**

  For more information on migrating configuration and database data to a new system, see "Migrating your 2.0.1 configurations to VCS One 5.0" on page 120.

Upgrading a 2.0.1 system and adding it to the VCS One 5.0 Policy Master cluster

Follow the instructions in this section to upgrade Node1 to VCS One 5.0, and then add it to the VCS One 5.0 Policy Master cluster.

To upgrade a 2.0.1 system and add it to the VCS One 5.0 Policy Master cluster

1. Check that Node1 is running an operating system that VCS One 5.0 supports. Do one of the following
   - If Node1 is running a supported operating system, skip to step 2.
   - If Node1 is not running a supported operating system, install or upgrade to a supported operating system. Then, go to step 2.

   For information on supported operating systems, see *Veritas Cluster Server One Release Notes*.
2. Use the Policy Master installer to upgrade Node1 to VCS One 5.0. You don't need to configure the system. Use the -installonly option to install the VCS One packages over the systems. Enter the following:

   # **./installvcsonepm -installonly**

For more information about installing Policy Master systems, see Chapter 2, “Installing and configuring the VCS One Policy Master” on page 35.

3 Add Node1 to the 5.0 Policy Master cluster. Enter the following:

```
# ./installvcsonepm -addnode
```

See: Chapter 9, “Adding a new or replacement system to the Policy Master cluster” on page 107.

Appendix C

Troubleshooting

This appendix includes the following topics:

Re-authenticating the client

If authentication fails, the VCS One client does not start. If the client fails to start, check the client log for details about the failure, and follow the instructions in this section to reauthenticate the client.

How to recognize if authentication has failed

This section provides a sample client log message for an authentication failure. The following error message is shown in the client log file at: `%vcsone_home%\log` (typically, `C:\Program Files\Veritas\Cluster Server One\log`):

```
2008-08-25 15:26:31 VCS One ERROR V-97-19-12358 Failed to obtain
the credential from Local cache, please ensure that the System
credential is deployed on the node and the System does not lag
behind the PM node
```

If authentication fails, the product installer does not display an error message during installation, but the installer log contains the following message:

```
haat execpkg ERROR V-18-7135 Failed to execute package
```

The installer log file is at `%allusersprofile%\application data\Veritas\VPI\log`.

Reasons authentication might fail

When you install the VCS One client, authentication can fail for the following reasons:

- Incorrectly set firewall ports that cause communication issues.
- The client system time lags behind the Policy Master server time by more than 30 minutes.
- The installer did not add a principle for the client.

If you upgrade the client, the credential may no longer be valid for one of the following reasons:

- The credentials were not backed up
- The client credential cache is deleted
- You did not re-deploy the client
- Credentials are not valid with the current broker

Re-authenticating the client

If the client log file indicates that authentication failed, follow the steps in this section to re-authenticate the client.

To re-authenticate the client

1. From the Policy Master, create a new credential.
   For instructions on creating a deployment credential, see: "Installing the client using a permanent credential" on page 68.
2. Change directories to the `/bin` directory:
   `cd /opt/VRTSvcsone/bin`
3. From the `/bin` directory, re-authenticate the client. Enter the following:
   `haat execpkg -i full_path_to_deployment_package -o`
   The full path to the deployment package should include the file name.
4. Restart the VCS One client.

Installing Storage Foundation after installing the client on Linux

If, after installing the VCS One client on Linux, you later install Storage Foundation 5.0 using the Storage Foundation installer, the following warning message appears:

```
CPI WARNING V-9-1-1267 SF version 5.0 includes VRTSperl version
5.0.2.1. A more recent version of VRTSperl, 5.8.8.0, is already
installed on system1.
CPI WARNING V-9-1-1271 In this situation VRTSperl version
5.8.8.0 will not be installed or downgraded on system1.
SF version 5.0 may not operate correctly with this more recent
rpm.
The VRTSperl rpm must be removed manually before version 5.0.2.1
can be installed.
Do you want to continue? [y,n,q,?] (n)
```

If you encounter this warning message, answer "yes" (or "y") to continue and do not downgrade the Perl version.

Troubleshooting I/O fencing

This section provides solutions to the following I/O fencing issues:

vxfentsthdw fails when the SCSI TEST UNIT READY command fails

If you see a message resembling:

```
Issuing SCSI TEST UNIT READY to disk reserved by other node
FAILED.
Contact the storage provider to have the hardware configuration
fixed.
```

The disk array does not support returning success for a SCSI TEST UNIT READY command when another host has the disk reserved using SCSI-3 persistent reservations.

vxfentsthdw fails when prior registration key exists on disk

Although the situation is unlikely, you may try to use the `vxfentsthdw` utility to test a disk that has a registration key already set. If you suspect a key exists on the disk you plan to test, use the `vxfenadm -g` command to display the key.

```
vxfenadm -g diskname
```

- If the disk is not SCSI-3 compliant, the following error is returned:
  `Inappropriate ioctl for device.`
- If you have a SCSI-3 compliant disk and no key exists, the output resembles the following:

  ```
  Reading SCSI Registration Keys...
  Device Name: diskname
  Total Number Of Keys: 0
  No keys ...
  ```

  Next, test the disk using the `vxfentsthdw` utility.
  See "Setting up and testing data disks" on page 79.
- If keys exist, you must remove them before you test the disk.
  See "System panics to prevent potential data corruption" on page 153.

System panics to prevent potential data corruption

When a system has a split brain condition and is ejected from the VCS One cluster, it panics and displays the following console message:

```
VXFEN:vxfen_plat_panic: Local cluster node ejected from cluster
to prevent potential data corruption.
```

How vxfen driver checks for a pre-existing split brain condition

The `vxfen` driver prevents an ejected system from rejoining the VCS One cluster after the private network links fail and before they are repaired.

For example, suppose that system 1 and system 2 are part of a VCS One cluster that functions normally when the private network links are broken. Also suppose system 1 is the ejected system. When system 1 reboots before the private network links are restored, its membership configuration does not show system 2; however, when it tries to register with the coordinator disks, it discovers system 2 is registered with them. Given this conflicting information about system 2, system 1 does not join the VCS One cluster and returns an error from `vxfenconfig`. The message is similar to the following:

```
vxfenconfig: ERROR: There exists the potential for a preexisting
split-brain. The coordinator disks list no nodes which are in the
current membership. However, they also list nodes which are not in
the current membership.

I/O Fencing Disabled!
```

The following information also appears:

```
<date> <system name> vxfen: WARNING: Potentially a preexisting
<date> <system name> split-brain.
<date> <system name> Dropping out of cluster.
<date> <system name> Refer to user documentation for steps
<date> <system name> required to clear preexisting split-brain.
<date> <system name>
<date> <system name> I/O Fencing DISABLED!
<date> <system name>
<date> <system name> gab: GAB:20032: Port b closed
```

However, the same error can occur when the private network links are working and both systems go down, system 1 reboots, and system 2 fails to come back up. From the view of the VCS One cluster from system 1, system 2 may still be registered on the coordinator disks.

Resolving an actual potential split brain condition

An actual split brain condition is where two systems are up, but there is no heartbeat between them. In the following example, system 1 and system 2 are both up, but there is no heartbeat between them. Then, system 2 is up and system 1 is ejected.

To resolve an actual potential split brain condition

1. Determine if system 1 is up.
2. If it is up and running, shut it down and repair the private network links to remove the split brain condition.
3. Reboot system 1.

Resolving an apparent potential split brain condition

An apparent split brain condition is where one system is up and one system is down, and there is no heartbeat between them. In the following example, system 2 is down, and system 1 is ejected and there is no heartbeat between the two systems.

To resolve an apparent potential split brain condition

1. Physically verify that system 2 is down.
2. Log in to system 1 and check to see that I/O fencing is not configured. Enter the following:
   ```
   vxfenadm -d
   ```
   The command output shows that I/O fencing is not configured on system 1.
3. Verify that the systems are registered with the coordinator disks. Enter the following:
   ```
   vxfenadm -g all -f /etc/vxfentab
   ```
   The command output identifies the keys registered with the coordinator disks.
4. Clear the keys on the coordinator disks as well as the data disks using the command `/opt/VRTSvcs/vxfen/bin/vxfenclearpre`.
   See "Using the vxfenclearpre command to clear keys after split brain" on page 155.
5. Make any necessary repairs to system 2 and reboot.

Using the vxfenclearpre command to clear keys after split brain

If you encounter a split brain condition, use the `vxfenclearpre` command to remove SCSI-3 registrations and reservations on the coordinator disks and the data disks in all shared disk groups.

To remove SCSI-3 registrations and reservations on the coordinator disks

1. Shut down all other systems in the Policy Master cluster that access shared storage. This prevents data corruption.
2. Start the script:

```
cd /opt/VRTSvcs/vxfen/bin
./vxfenclearpre
```

3. Read the script's introduction and warning, and then run it. The output is similar to the following:

```
Do you still want to continue: [y/n] (default : n)
y
Cleaning up the coordinator disks...

Cleaning up the data disks for all shared disk groups...

Successfully removed SCSI-3 persistent registration and
reservations from the coordinator disks as well as the
shared data disks.

Reboot the server to proceed with normal cluster startup...
#
```

4. Reboot all systems in the Policy Master cluster.

Adding or removing coordinator disks

This section describes how to destroy or replace a coordinator disk in the coordinator disk group.

Adding or removing coordinator disks requires all services be shut down.

In the following procedure:

- A coordinator disk group requires an odd number (three minimum) of disks or LUNs.
- When you add a disk, add it to the coordinator disk group (`vxfencoorddg`, for example) and retest the group for SCSI-3 persistent reservation support.
- You can destroy the coordinator disk group so that no registration keys remain on the disks. The disks can then be used elsewhere.

To remove and replace a disk in the coordinator disk group

1. Log in as root user on one of the systems in the Policy Master cluster.
2. If VCS is running, shut it down:
   ```
   hastop -all
   ```
3. Stop I/O fencing on all systems. Do one of the following:
   On Solaris:
   ```
   # /etc/init.d/vxfen stop
   ```
   On Linux:
   ```
   # service vxfen stop
   ```
   On AIX:
   ```
   # /etc/rc.d/rc2.d/S97vxfen stop
   ```
   On HP-UX:
   ```
   # /sbin/init.d/vxfen stop
   ```
   This removes any registration keys on the disks.
4. Import the coordinator disk group. The file `/etc/vxfendg` includes the disk group (for example, `vxfencoorddg`) that contains the coordinator disks. Enter the following:
   ```
   vxdg -tfC import `cat /etc/vxfendg`
   ```
   where:

   `-t` Specifies that the disk group is imported only until the system restarts.

   `-f` Specifies that the import is to be done forcibly, which is necessary if one or more disks is not accessible.

   `-c` Specifies that any import blocks are removed.
5. To remove disks from the disk group, use the VxVM disk administrator utility, vxdiskadm.

You can also destroy the existing coordinator disk group. For example, use:
`vxdg destroy vxfencoorddg`

6 Add the new disk to the system, initialize it as a VxVM disk, and add it to the coordinator disk group.
See "Setting up and testing coordinator disks" on page 83

7 Test the recreated disk group to see if it complies with SCSI-3 persistent reservations.
See "Setting up and testing coordinator disks" on page 83.

8 Deport the disk group. Enter the following:
```
vxdg deport 'cat /etc/vxfendg'
```

9 On each system in the VCS One cluster, start the I/O fencing driver. Do one of the following:

- On Solaris, enter the following:

```
# /etc/init.d/vxfen start
```

- On Linux, enter the following:

```
# service vxfen start
```

- On AIX, enter the following:

```
# /etc/rc.d/rc2.d/S97vxfen start
```

- On HP-UX, enter the following:

```
# /sbin/init.d/vxfen start
```

10 Restart VCS on each system. Enter the following:
```
hastart
```

How I/O fencing works in different situations

Table C-1 describes how I/O fencing works to prevent data corruption in different situations. The table also includes actions the operator can take in each situation.

Table C-1 I/O fencing scenarios

Event	Node A activity	Node B activity	Operator action
Both private networks fail.	Races for majority of coordinator disks. If it wins race for coordinator disks, Node A ejects Node B from the shared disks and continues.	Races for majority of coordinator disks. If it loses the race for the coordinator disks, Node B removes itself from the Policy Master cluster.	When Node B is ejected from the VCS One cluster, repair the private networks, then try to bring Node B back.
Both private networks function again after event above.	Continues to work.	Crashes. It cannot start the database because it cannot write to the data disks.	Restore the private networks and reboot Node B.
One private network fails.	Prints message about an IOFENCE on the console but continues.	Prints message about an IOFENCE on the console but continues.	Repair the private network. After network is repaired, both systems use it automatically.
Node A hangs.	Extremely busy for some reason or is in the kernel debugger. When Node A is no longer hung or in the kernel debugger, any queued writes to the data disks fail because Node A is ejected. When Node A receives message from GAB about being ejected, it removes itself from the Policy Master cluster.	Loses heartbeats with Node A, and races for a majority of coordinator disks. Wins race for coordinator disks and ejects Node A from shared data disks.	Verify that the private networks function and reboot Node A.

Table C-1 I/O fencing scenarios

Event	Node A activity	Node B activity	Operator action
Nodes A and B and private networks lose power. Coordinator and data disks retain power. Power returns to systems and they reboot, but private networks still have no power.	Reboots and I/O fencing driver (vxfen) detects Node B is registered with coordinator disks. Because the private networks are down, the driver does not see Node B listed as member of the VCS One cluster. This causes the I/O fencing device driver to prevent Node A from joining the VCS One cluster. Node A console displays the following: `Potentially a preexisting split brain. Dropping out of the cluster. Refer to the user documentation for steps required to clear preexisting split brain.`	Reboots and I/O fencing driver (vxfen) detects Node A is registered with coordinator disks. Because the private networks are down, the driver does not see Node A listed as member of the VCS One cluster. This causes the I/O fencing device driver to prevent Node B from joining the VCS One cluster. Node B console displays the following: `Potentially a preexisting split brain. Dropping out of the cluster. Refer to the user documentation for steps required to clear preexisting split brain.`	For instructions on resolving preexisting split brain condition, see "Troubleshooting I/O fencing" on page 152.
Node A crashes while Node B is down. Node B comes up and Node A is still down.	Crashes.	Reboots and detects Node A is registered with the coordinator disks. The driver does not see Node A listed as member of the VCS One cluster. The I/O fencing device driver prints the following message on console: `Potentially a preexisting split brain. Dropping out of the cluster. Refer to the user documentation for steps required to clear preexisting split brain.`	See "Installing Storage Foundation after installing the client on Linux" on page 151 for instructions on resolving preexisting split brain condition.

Table C-1 I/O fencing scenarios

Event	Node A activity	Node B activity	Operator action
The disk array containing two of the three coordinator disks is powered off.	Operates as long as all systems stay in the VCS One cluster.	Operates as long as all systems stay in the VCS One cluster.	Power on the failed disk array and restart the I/O fencing driver. This lets Node A register with all coordinator disks.
Node B leaves the VCS One cluster and the disk array is still powered off.	Races for a majority of coordinator disks. It fails because only one of three coordinator disks is available. Removes itself from the VCS One cluster.	Leaves the VCS One cluster.	

Appendix D

Sample installation output

This appendix includes the following topics:

Installing the VCS One Policy Master with Storage Foundation

This section provides sample output of the output from a VCS One Policy Master installation with Storage Foundation on Linux. Use this example for reference only. The output for each operating system version and installation environment differs slightly.

Starting the installer

This section provides a brief overview of the installation procedure.

See Chapter 2, "Installing and configuring the VCS One Policy Master" for detailed instructions.

To start the installer

1. Mount the product disc.
2. Invoke the installer. Enter the following:

```
# ./installer -rsh
```

Reading the copyright information

```
                    Installation Program

Copyright (c) 2009 Symantec Corporation. All rights reserved.
Symantec, the Symantec Logo are trademarks or registered trademarks
of Symantec Corporation or its affiliates in the U.S. and other
countries. Other names may be trademarks of their respective owners.
The Licensed Software and Documentation are deemed to be "commercial
computer software" and "commercial computer software
documentation" as defined in FAR Sections 12.212 and DFARS Section
227.7202.

Logs for installer are being created in /var/tmp/installer-eKiPxL
```

Selecting a task

```
            Veritas Cluster Server One 5.0.0 by Symantec

Symantec Product          Version Installed   Licensed
=============================================================================

Symantec Licensing Utilities (VRTSvlic package) are not installed
due to which products and licenses are not discovered
Please use the menu below to continue.
```

```
Task Menu:

I) Install/Upgrade a Product C) Configure an Installed Product
L) License a Product P) Perform a Pre-Installation Check
U) Uninstall a Product D) View a Product Description
Q) Quit ?) Help

Enter a Task: [I,C,L,P,U,D,Q,?] i
```

Selecting a Policy Master installation

```
                Veritas Cluster Server One 5.0.0 by Symantec

1) Veritas Cluster Server One by Symantec - Policy Master (VCS One
PM)
2) Veritas Cluster Server One by Symantec - Client Daemon (VCS One
Client)
b) Back to previous menu

Select a product to install: [1-2,b,q] 1
```

Accepting the End User License Agreement

```
Do you agree with End User License Agreement (EULA) specified in
EULA.pdf file present on media? [y,n,q,?] (n) y
```

Reviewing the installation and configuration requirements

```
                Veritas Cluster Server One 5.0.0 by Symantec

VCS One Policy Master installation and configuration documentation
You can install the VCS One Policy Master on one or more nodes.
Ensure that passwordless communication is established between the
system that runs the installation script and the target installation
systems. You can use rsh or ssh as the access method. If you are
using rsh, specify the -rsh option when you invoke the installation
script.

If you want the Policy Master to be highly available, install it on
two or more systems.

Press [Enter] to continue:

To install and configure, the following is required:
1. For installation on two or more systems
-- A unique cluster ID between 0 and 65535
-- Two or more NIC cards per system for heartbeat links
2. Virtual IP address
-- Each system in the cluster must have a public NIC
```

```
-- You must specify a virtual IP address and netmask. The Policy
Master listens on this virtual IP address.
Press [Enter] to continue:

           Veritas Cluster Server One 5.0.0 by Symantec

3. Shared Storage configuration
3a. (Recommended) Storage Foundation configuration
-- Mount point
-- Disk(s) and diskgroup names
-- Volume name and size
3b. (Optional) configuration on NetApp filer
-- Mount point
-- IP address or hostname of the NetApp filer
-- Type of access to the NetApp filer (rsh, ssh or API that use the
NetApp SDK)
-- Username and password for accessing NetApp filer
-- IP address or hostname for the NIC connected to the NetApp filer
-- File system path on the NetApp filer
3c. (Optional) Configuration on external shared storage
-- Mount point for external shared storage
4. (Optional) disaster recovery configuration
-- One or more virtual IP addresses
-- Netmasks for each of the virtual IP addresses
-- Public NICs to be used on each system for the virtual IP
addresses
Press [Enter] to continue:
```

Entering the target systems

```
           Veritas Cluster Server One 5.0.0 by Symantec

Enter the system names separated by spaces on which to install
Veritas Cluster Server One by Symantec - Policy Master (VCS One PM):
redhat95243 pilotvmred9

Initial system check:
Checking ssh communication with pilotvmred9 .... Linux 2.6.18-92.el5
Checking network speed with pilotvmred9 ..................... OK
Checking VCS One PM installation on redhat95243 ..... Not installed
Checking VxFS installation on redhat95243 ............ Not installed
Checking VxVM installation on redhat95243 ........... Not installed
Checking VCS One PM installation on pilotvmred9 ...... Not installed
Checking VxFS installation on pilotvmred9 ............ Not installed
Checking VxVM installation on pilotvmred9 ........... Not installed
```

Deciding about Storage Foundation installation

```
           Veritas Cluster Server One 5.0.0 by Symantec

Storage Foundation installation
```

```
While installing the VCS One PM, you can install Storage Foundation,
and create the diskgroup and volume during the installation.
Enter 'n', if you do not want to install and use Storage Foundation
for storing the VCS One configuration.
Enter 'y', if you want to install Storage Foundation packages.
Do you want to install Storage Foundation? [y,n,q] (y)
```

Selecting a license type

```
Checking system licensing

           Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-eKiPxL

Installing licensing rpms: 100%
/
You must install one of the following license types on the Policy
Master:

1) Demo License
2) NFR License
3) Permanent License

Select a License flavor to install: [1-3,q] 1
License key successfully registered on redhat95243
License key successfully registered on pilotvmred9
```

Reviewing the package list

```
           Veritas Cluster Server One 5.0.0 by Symantec

Checking installed rpms on redhat95243
Checking installed rpms on pilotvmred9

The following VCS One PM rpms will be installed:

VRTSperl               Veritas Perl 5.10 Redistribution
VRTSvlic               Veritas Licensing
VRTSat               Client Symantec Product Authentication Service
Client
VRTSvxvmcommon         Veritas Volume Manager Common Package
VRTSvxvmplatform       Veritas Volume Manager Platform Specific
Package
VRTSvdid Veritas       Device Identification API
VRTSicsco Symantec     Infrastructure Core Services Common
VRTSpbx Symantec       Private Branch Exchange
VRTSobc33 Veritas      Enterprise Administrator Core Service
VRTSob Veritas         Enterprise Administrator Service
VRTSdsa Veritas        Datacenter Storage Agent
```

```
VRTSfspro Veritas      File System Management Services Provider
VRTSvmman Veritas      Volume Manager Manual Pages
VRTSlvmconv Veritas    Linux LVM to VxVM Converter
VRTSddlpr Veritas      Device Discovery Layer Services Provider
VRTSvmpro               Veritas Volume Manager Management Services
                        Provider
VRTSdcli               Veritas Distributed Command Line Interface
VRTSalloc               Veritas Volume Manager Intelligent Storage
                        Provisioning
VRTSvxfscommon         Veritas File System Common package
VRTSvxfsplatform       Veritas File System Platform Specific Package
VRTSfsman              Veritas File System Manual Pages
VRTSfssdk              Veritas File System Software Developer Kit
VRTSfsmnd               Veritas File System Software Developer Kit
                        Manual Pages
VRTSvcsoneut            Veritas Cluster Server One by Symantec -
                        Utilities
VRTSllt                Veritas Low Latency Transport
VRTSgab                Veritas Group Membership and Atomic Broadcast
VRTSvxfen              Veritas I/O Fencing
VRTSvcsonedb            Veritas Cluster Server One by Symantec -
                        Configuration Database
VRTSvcsonemg            Veritas Cluster Server One by Symantec -
                        Message Catalogs
VRTSvcs                Veritas Cluster Server
VRTSvcsag              Veritas Cluster Server Bundled Agents
VRTSvcsmg              Veritas Cluster Server Message Catalogs
VRTSvcsonemn            Veritas Cluster Server One by Symantec -
                        Man Pages
VRTSpmmag              Veritas Cluster Server PMM Agents
VRTSvcsonec             Veritas Cluster Server One by Symantec -
                        Command Line Utilities
VRTSvcsonepm            Veritas Cluster Server One by Symantec -
                        Policy Master
VRTSvcsonew             Veritas Cluster Server One by Symantec -
                        Web Console
VRTSspt                Veritas Software Support Tools

Press [Enter] to continue:
```

Choosing when to configure the Policy Master

```
                Veritas Cluster Server One 5.0.0 by Symantec

It is possible to install VCS One PM rpms without performing
configuration.
It is optional to configure VCS One PM now. If you choose to
configure VCS One PM later, you can either do so manually, or run
the installvcsonepm -configure command. The product installation
scripts can be found in /opt/VRTS/install directory
Are you ready to configure VCS One PM? [y,n,q] (y)
```

```
                Veritas Cluster Server One 5.0.0 by Symantec

You can enter 'b' to go back to the first question.
You can enter '?' for additional information about the question.
Following each set of questions, you are asked to confirm the
information you have entered. To repeat the questions and correct
any previous errors, enter 'n' at the confirmation prompt. No
configuration changes are made to the systems until you answer and
confirm all configuration questions and VCS One PM is installed
successfully.
Press [Enter] to continue:
```

Configuring the VCS One Policy Master cluster

```
                Veritas Cluster Server One 5.0.0 by Symantec

All nodes are configured to run the Policy Master from the Policy
Master cluster. The VCS One Policy Master cluster provides high
availability to the Policy Master. To configure the Policy Master
cluster, the following information is required:

     A cluster name
     A unique cluster ID between 0-65535
     Two or more NIC cards per system used for heartbeat links
     One or more heartbeat links are configured as private links
     One heartbeat link may be configured as a low priority link

Configuring all systems to create one cluster

Enter the unique cluster name: [?] vcsonepm_cluster
Enter the unique Cluster ID between 0-65535: [b,q,?] 12312
Discovering NICs on redhat95243 ......................... Discovered

          NIC : IP Address
          ------------------------
          eth0 : 10.198.95.243
          eth1 : none
          eth2 : none

Discovering NICs on pilotvmred9 ......................... Discovered

          NIC : IP Address
          ------------------------
          eth0 : 10.198.92.157
          eth1 : 192.168.100.101
          eth2 : 192.168.100.102

Enter the NIC for the first private heartbeat link on redhat95243:
[b,q,?] eth1
```

```
Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)
Enter the NIC for the second heartbeat link on redhat95243: [b] eth2
Do you want to configure an additional low priority heartbeat link?
[y,n,q,b,?] (n)
Are you using the same NICs for private heartbeat links on all
systems? [y,n,q,b,?] (y)
Would you like to use the default port number 14159 for
Authentication Services? [y,n,q,b] (y)
```

Confirming the VCS One Policy Master cluster configuration

```
            Veritas Cluster Server One 5.0.0 by Symantec

Policy Master cluster configuration information verification:

Cluster Name : vcsonepm_cluster
Cluster ID : 12312
Broker Port : 14159

Private Heartbeat NICs for redhat95243:link1=eth1 link2=eth2
Private Heartbeat NICs for pilotvmred9:link1=eth1 link2=eth2
```

Configuring the Policy Master virtual IP addresses

```
            Veritas Cluster Server One 5.0.0 by Symantec

The following information is required to configure the Policy
Master:

     Public NICs used by each system in the Policy Master cluster
     Policy Master virtual IP addresses and netmasks

Active NIC devices discovered on redhat95243:

          NIC : IP Address : Netmask
          ---------------------------------------
          eth0 : 10.198.95.243 : 255.255.248.0

          Active NIC devices discovered on pilotvmred9:

          NIC : IP Address : Netmask
          ---------------------------------------
          eth0 : 10.198.92.157 : 255.255.248.0
          eth1 : 192.168.100.101 : 255.255.248.0
          eth2 : 192.168.100.102 : 255.255.248.0

Enter the NIC for Policy Master Virtual IP address on redhat95243:
[?] (eth0)
Would you like to use the same NIC (eth0) on all PM nodes? [y,n,q]
(y)
```

```
Only one IP address 10.198.95.243 is detected for NIC eth0 under
system redhat95243. This IP address will be set as the base IP.

Only one IP address 10.198.92.157 is detected for NIC eth0 under
system pilotvmred9. This IP address will be set as the base IP.

Enter one or more Virtual IPs separated by space for the Policy
Master: [b,q,?] 10.198.92.127 10.198.94.158

Checking the 10.198.92.127 virtual IP address ..... Not in use
Checking the 10.198.94.158 virtual IP address ..... Not in use

Enter the netmask for IP 10.198.92.127: [b,q,?] (255.255.248.0)
Enter the netmask for IP 10.198.94.158: [b,q,?] (255.255.248.0)
```

Confirming the Policy Master virtual IP address configuration

```
            Veritas Cluster Server One 5.0.0 by Symantec

Policy Master configuration verification:

Virtual IP 1:
     Virtual IP: 10.198.92.127
     Netmask: 255.255.248.0

Virtual IP 2:
     Virtual IP: 10.198.94.158
     Netmask: 255.255.248.0

NIC(s) under redhat95243:
     1: NIC - eth0; IP - 10.198.95.243

NIC(s) under pilotvmred9:
     1: NIC - eth0; IP - 10.198.92.157

Is this information correct? [y,n,q] (y)
```

Choosing a storage architecture

```
            Veritas Cluster Server One 5.0.0 by Symantec

VCS One PM should use shared storage for storing Configuration
Database
The following storage architectures are supported for storing VCS
One PM Configuration Database:
1. Storage Foundation -- One or more shared disks controlled by
Storage Foundation
2. NetApp filer -- Shared storage exported by a specified NetApp
filer server
```

```
3. Other -- Local storage or shared storage exported by an NFS
server and accessible by all the systems

Symantec recommends to use different shared storages for different
VCS One Policy Master server farms.
Note: Storage Foundation is not installed on all the Policy Master
nodes. If you install and configure Storage Foundation for storing
the VCS One PM Configuration Database, you must defer Storage
Foundation configuration until all packages are successfully
installed.

Storage architecture:

     1) Storage Foundation
     2) NetApp filer
     3) Other

Please select a kind of Storage Architecture for the Configuration
Database with the index number: [1-3,q] 1
```

Deciding whether to configure disaster recovery

```
                Veritas Cluster Server One 5.0.0 by Symantec

A VCS One global cluster links the individual VCS One clusters at
separate sites, and enables wide-area failover and disaster
recovery (DR) for the applications you configured. A VCS One global
cluster configuration can have a maximum of two clusters.
Clustering on a global level also requires an infrastructure to
replicate the application data between these clusters.
The following information is required to configure VCS One PM
disaster recovery:

     One or more virtual IP addresses and netmasks
     Public NICs used by each system for the virtual IP addresses

Do you want to configure VCS One PM disaster recovery? [y,n,q] (y)
```

Configuring disaster recovery

```
Active NIC devices discovered on redhat95243:

          NIC : IP Address : Netmask
          ---------------------------------------
          eth0 : 10.198.95.243 : 255.255.248.0


Active NIC devices discovered on pilotvmred9:

          NIC : IP Address : Netmask
          ---------------------------------------
```

```
          eth0 : 10.198.92.157 : 255.255.248.0
          eth1 : 192.168.100.101 : 255.255.248.0
          eth2 : 192.168.100.102 : 255.255.248.0

Enter one or more Virtual IPs for VCS One PM disaster recovery:
[b,q,?] 10.200.58.209 10.200.58.210

Checking virtual IP address 10.200.58.209 ..... Not in use
Checking virtual IP address 10.200.58.210 ..... Not in use

Enter a nic for IP 10.200.58.209 on redhat95243: [b,q,?] eth0
Would you like to use the same NIC (eth0) on all PM nodes for IP
10.200.58.209? [y,n,q] (y)
Enter the netmask for IP 10.200.58.209: [b,q,?] (255.255.248.0)
Enter a nic for IP 10.200.58.210 on redhat95243: [b,q,?] eth0
Would you like to use the same NIC (eth0) on all PM nodes for IP
10.200.58.210? [y,n,q] (y)
Enter the netmask for IP 10.200.58.210: [b,q,?] (255.255.248.0)
```

Confirming the disaster recovery configuration

```
            Veritas Cluster Server One 5.0.0 by Symantec

VCS One PM Disaster Recovery Configuration Verification:

Virtual IP 1:
     IP Address : 10.200.58.209
     Netmask : 255.255.248.0

NICs for Virtual IP 1:
     redhat95243 : eth0
     pilotvmred9 : eth0

Virtual IP 2:
     IP Address : 10.200.58.210
     Netmask : 255.255.248.0

NICs for Virtual IP 2:
     redhat95243 : eth0
     pilotvmred9 : eth0

Is this information correct? [y,n,q] (y)
```

Installing packages

```
                Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-eKiPxL

Installing VCS One PM: 100%

Installation completed successfully on all systems
```

Starting Storage Foundation processes

```
                Veritas Cluster Server One 5.0.0 by Symantec

Starting Storage Foundation Processes

Starting the vxconfigd process on redhat95243 .................. Done
Starting the vxrelocd process on redhat95243 .................. Done
Starting the vxconfigbackupd process on redhat95243 .......... Done
Starting the vxconfigd process on pilotvmred9 ................. Done
Starting the vxrelocd process on pilotvmred9 ............... Done
Starting the vxconfigbackupd process on pilotvmred9 ........ Done
```

Configuring Storage Foundation

```
                Veritas Cluster Server One 5.0.0 by Symantec

VCS One PM can use Storage Foundation for storing configuration
information

The following information is required to configure Storage
Foundation:

-- Name of the existing diskgroup or the diskgroup you are creating
-- Disk(s) need(s) to be part of the diskgroup to be created
-- Name of the volume that already exists or is being created in the
diskgroup
-- Size of the volume to be created
-- Mount point where the volume to be mounted

Note: Storage Foundation configuration will be performed on the
first system redhat95243

Storage Foundation information:
System : redhat95243
Free disks : sda sdb sdc
No diskgroups found on redhat95243
```

```
System : pilotvmred9
Free disks : sda sdb
No diskgroups found on pilotvmred9

Enter a diskgroup for the Configuration Database: [?] pmdg
Checking diskgroup pmdg on redhat95243 ..... Does not exist

Enter disks separated by space for pmdg on redhat95243: [b,q,?] sdb
Checking disk sdb on redhat95243 ..... Not in use
Checking type of sdb on redhat95243 ..... Uninitialized

Do you wish to initialize the disk sdb? [y,n,q] (y)
Initializing disk sdb on redhat..... Done with format cdsdisk
Checking disk sdb is shared between all the systems..... Shared
Checking status of sdb on redhat95243 ..... Online
Creating diskgroup pmdg on redhat95243 ..... Done
No volumes in pmdg on redhat95243

Enter a volume for the Configuration Database: [b,q,?] pmvol
Checking volume pmvol in pmdg on redhat95243 ..... Does not exist

Enter a size for the volume pmvol in pmdg on redhat95243: [b,q,?]
200M
Creating volume pmvol in pmdg on redhat95243 ..... Done
Creating vxfs on pmvol in pmdg on redhat95243 ..... Done

Enter a mount point for the Configuration Database: [b,q,?] /PM
Checking the mount point /PM on redhat95243 ..... Exist
Checking the mount point /PM on pilotvmred9 ..... Exist
Mounting pmvol on /PM on redhat95243 ..... Done
```

Confirming the Storage Foundation configuration

```
        Veritas Cluster Server One 5.0.0 by Symantec

Storage Foundation configuration for the configuration database:

     Diskgroup : pmdg
     Disks : sdb
     Volume : pmvol
     Volume Size : 200M
     File System : vxfs
     Mount Point : /PM

Is this information correct and not in use by other VCS One Policy
Master server farms? [y,n,q] (y)
```

```
                Veritas Cluster Server One 5.0.0 by Symantec

Configure llthosts on redhat95243 ............................. Done
Configure llthosts on pilotvmred9 ........................... Done
Configure llttab on redhat95243 ............................... Done
Configure llttab on pilotvmred9 ............................. Done
Configure gabtab on redhat95243 ............................. Done
Configure gabtab on pilotvmred9 ............................. Done
Configure sysname on redhat95243 ............................ Done
Configure sysname on pilotvmred9 ............................ Done
Configure main.xml on redhat95243 ........................... Done
Configure main.xml on pilotvmred9 ........................... Done
Change some type attributes on redhat95243 .................. Done
Change some type attributes on pilotvmred9 .................. Done
Configure main.cf on redhat95243 ............................ Done
Configure main.cf on pilotvmred9 ............................ Done
Configure vcsone.ini on redhat95243 ......................... Done
Configure vcsone.ini on pilotvmred9 ......................... Done
Configure vcsone.conf on redhat95243 ........................ Done
Configure vcsone.conf on pilotvmred9 ........................ Done
Configure ATD on redhat95243 ................................ Done
Configure ATD on pilotvmred9 ................................ Done
Configure vcs run mode file on redhat95243 ................... Done
Configure vcs run mode file on pilotvmred9 ................... Done
Configure vcsone db on redhat95243 ........................... Done
Configure vcsone db on pilotvmred9 ............................ Done
```

Starting the Policy Master processes

```
Do you want to start Veritas Cluster Server One by Symantec - Policy
Master processes now? [y,n,q] (y)

                Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-eKiPxL

Starting VCS One PM: 100%

Startup completed successfully on all systems

Installation log files, summary file, and response file are saved
at: /var/VRTS/install/logs/installer-eKiPxL

Installation - Success
Configuration - Success
Startup - Success

The VCS One PM installation operation successful.
Please access https://10.198.92.127:14171 for VCS One Web Console.
```

Installing the VCS One Policy Master with NetApp

This section provides sample output of the output from a VCS One Policy Master installation with NetApp on Linux. Use this example for reference only. The output for each operating system version and installation environment differs slightly.

Starting the installer

This section provides a brief overview of the installation procedure.

See Chapter 2, "Installing and configuring the VCS One Policy Master" for detailed instructions.

To install the VCS One Policy Master with NetApp

1. Mount the product disc.
2. Invoke the installer. Enter the following:
   ./installer

Reading the copyright information

```
                    Installation Program

Copyright (c) 2009 Symantec Corporation. All rights reserved.
Symantec, the Symantec Logo are trademarks or registered trademarks
of Symantec Corporation or its affiliates in the U.S. and other
countries. Other names may be trademarks of their respective owners.

The Licensed Software and Documentation are deemed to be "commercial
computer software" and "commercial computer software documentation"
as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Logs for installer are being created in /var/tmp/installer-UUfIaK
```

Selecting a task

```
          Veritas Cluster Server One 5.0.0 by Symantec

Symantec Product          Version Installed   Licensed
=============================================================================

Symantec Licensing Utilities (VRTSvlic package) are not installed
due to which products and licenses are not discovered. Please use
the menu below to continue.

Task Menu:
I) Install/Upgrade a Product  C) Configure an Installed Product
L) License a Product          P) Perform a Pre-Installation Check
```

```
U) Uninstall a Product          D) View a Product Description
Q) Quit                         ?) Help
Enter a Task: [I,C,L,P,U,D,Q,?] i
```

Selecting a Policy Master installation

```
            Veritas Cluster Server One 5.0.0 by Symantec
1)  Veritas Cluster Server One by Symantec - Policy Master (VCS One
PM)
2)  Veritas Cluster Server One by Symantec - Client Daemon (VCS One
Client)
b)  Back to previous menu

Select a product to install: [1-2,b,q] 1
```

Accepting the End User License Agreement

```
Do you agree with End User License Agreement (EULA) specified in
EULA.pdf file present on media? [y,n,q,?] (n) y
```

Reviewing the installation and configuration requirements

```
            Veritas Cluster Server One 5.0.0 by Symantec

VCS One Policy Master installation and configuration documentation

You can install the VCS One Policy Master on one or more nodes.
Ensure that passwordless communication is established between the
system that runs the installation script and the target installation
systems. You can use rsh or ssh as the access method. If you are
using rsh, specify the -rsh option when you invoke the installation
script.

If you want the Policy Master to be highly available, install it on
two or more systems.


Press [Enter] to continue:

            Veritas Cluster Server One 5.0.0 by Symantec


To install and configure, the following is required:

1. For installation on two or more systems
-- A unique Cluster ID between 0 and 65535
-- Two or more NIC cards per system for heartbeat links

2. Virtual IP address
```

```
-- Each system in the cluster must have a public NIC
-- You must specify a virtual IP address and netmask. The Policy
Master listens on this virtual IP address.
Press [Enter] to continue:

           Veritas Cluster Server One 5.0.0 by Symantec

3. Shared Storage configuration
3a. (Recommended) Storage Foundation configuration
-- Name of the existing diskgroup or the diskgroup you are creating
-- Disk(s) that are be part of the diskgroup you are creating
-- Name of the existing volume or the volume to be created in the
diskgroup
-- Size of the volume to be created
-- Type of file system being created on the volume
-- Mount point where the volume is mounted

3b. (Optional) configuration on NetApp filer
-- Mount point
-- IP address or hostname of the NetApp filer
-- Type of access to the NetApp filer
-- rsh (requires passwordless communication between the Policy
Master node and NetApp filer)
-- ssh (requires passwordless communication between the Policy
Master node and NetApp filer)
-- API (uses the NetApp SDK)
-- Username for accessing NetApp filer
-- Password for accessing NetApp filer for API access mode
-- IP address or hostname for the NIC that is connected to the
NetApp filer for each Policy Master system
-- File system path on the NetApp filer where the Configuration
Database will be stored

3c. (Optional) Configuration on external shared storage
-- Mount point where the external shared storage is mounted for
storing the VCS One PM configuration

Press [Enter] to continue:

4. (Optional) disaster recovery configuration
-- One or more virtual IP addresses
-- Netmasks for each of the virtual IP addresses
-- Public NICs to be used on each system for the virtual IP
addresses

Press [Enter] to continue:
```

Entering the target systems

```
            Veritas Cluster Server One 5.0.0 by Symantec
Enter the system names separated by spaces on which to install
Veritas Cluster Server One by Symantec - Policy Master (VCS One PM):
thoropt158 thoropt159

Initial system check:
Checking ssh communication with thoropt159 .... Linux 2.6.18-128.el5
Checking network speed with thoropt159..... OK
Checking VCS One PM installation on thoropt158........ Not installed
Checking VxFS installation on thoropt158 .......... Not installed
Checking VxVM installation on thoropt158 ........... Not installed
Checking VCS One PM installation on thoropt159 ....... Not installed
Checking VxFS installation on thoropt159 .......... Not installed
Checking VxVM installation on thoropt159 ............ Not installed
```

Deciding about Storage Foundation installation

```
            Veritas Cluster Server One 5.0.0 by Symantec

Storage Foundation installation
While installing the VCS One PM, you can install Storage Foundation,
and create the diskgroup and volume during the installation.
Enter 'n', if you do not want to install and use Storage Foundation
for storing the VCS One configuration.
Enter 'y', if you want to install Storage Foundation packages.
Do you want to install Storage Foundation? [y,n,q] (y) n
```

Checking the licensing

```
Checking system licensing


            Veritas Cluster Server One 5.0.0 by Symantec


Logs for installer are temporarily being created in /var/tmp/
installer-UUfIaK

Installing licensing rpms: 100%

Permanent license is already installed on thoropt158
Permanent license is already installed on thoropt159
            Veritas Cluster Server One 5.0.0 by Symantec


Checking installed rpms on thoropt158
Checking installed rpms on thoropt159
```

Reviewing the package list

```
                Veritas Cluster Server One 5.0.0 by Symantec

The following VCS One PM rpms will be installed:
VRTSperl          Veritas Perl 5.10 Redistribution
VRTSvlic          Veritas Licensing
VRTSatClient      Symantec Product Authentication Service Client
VRTSsfmh         Veritas Storage Foundation Managed Host by Symantec
VRTSvcsoneut      Veritas Cluster Server One by Symantec - Utilities
VRTSllt           Veritas Low Latency Transport
VRTSgab           Veritas Group Membership and Atomic Broadcast
VRTSvxfen         Veritas I/O Fencing
VRTSvcsonedb      Veritas Cluster Server One by Symantec -
Configuration Database
VRTSvcsonemg      Veritas Cluster Server One by Symantec - Message
Catalogs
VRTSvcs           Veritas Cluster Server
VRTSvcsag         Veritas Cluster Server Bundled Agents
VRTSvcsmg         Veritas Cluster Server Message Catalogs
VRTSvcsonemn      Veritas Cluster Server One by Symantec - Man Pages
VRTSpmmag         Veritas Cluster Server PMM Agents
VRTSvcsonec       Veritas Cluster Server One by Symantec - Command
Line Utilities
VRTSvcsonepm      Veritas Cluster Server One by Symantec - Policy
Master
VRTSvcsonew       Veritas Cluster Server One by Symantec - Web
Console
VRTSspt           Veritas Software Support Tools

Press [Enter] to continue:
```

Choosing when to configure the Policy Master

```
                Veritas Cluster Server One 5.0.0 by Symantec


It is possible to install VCS One PM rpms without performing
configuration.

It is optional to configure VCS One PM now. If you choose to
configure VCS One PM later, you can either do so manually, or
run the installvcsonepm -configure command. The product installation
scripts can be found in /opt/VRTS/install directory

Are you ready to configure VCS One PM? [y,n,q] (y) y


                Veritas Cluster Server One 5.0.0 by Symantec


To configure VCS One PM, answer the following sets of questions
```

```
You can enter 'b' to go back to the first question.
You can enter '?' for additional information about the question.

Following each set of questions, you are asked to confirm the
information you have entered. To repeat the questions and correct
any previous errors, enter 'n' at the confirmation prompt.

No configuration changes are made to the systems until you answer
and confirm all configuration questions and VCS One PM is installed
successfully.

Press [Enter] to continue:
```

Configuring the VCS One Policy Master cluster

```
                Veritas Cluster Server One 5.0.0 by Symantec

All nodes are configured to run the Policy Master from the Policy
Master cluster. The VCS One Policy Master cluster  provides high
availability to the Policy Master. To configure the Policy Master
cluster, the following information is required:

        A cluster name
        A unique cluster ID between 0-65535
        Two or more NIC cards per system used for heartbeat links

        One or more heartbeat links are configured as private links
        One heartbeat link may be configured as a low priority link

Configuring all systems to create one cluster

Enter the unique cluster name: [?] my_cluster
Enter the unique Cluster ID between 0-65535: [b,q,?] 65530
    Discovering NICs on thoropt158 ..................... Discovered
          NIC    : IP Address
        ------------------------
          eth0   : none
          eth1   : none
          eth2   : 10.182.7.218
          eth3   : none
    Discovering NICs on thoropt159 ..................... Discovered
          NIC    : IP Address
        ------------------------
          eth0   : none
          eth1   : none
          eth2   : 10.182.7.219
          eth3   : none
Enter the NIC for the first private heartbeat link on thoropt158:
[b,q,?] eth0
```

```
Would you like to configure a second private heartbeat link?
[y,n,q,b,?] (y)
Enter the NIC for the second heartbeat link on thoropt158: [b] eth1
Do you want to configure an additional low priority heartbeat link?
[y,n,q,b,?] (n)
Are you using the same NICs for private heartbeat links on all
systems? [y,n,q,b,?] (y)
Would you like to use the default port number 14159 for
Authentication Services? [y,n,q,b] (y)
```

Confirming the VCS One Policy Master cluster configuration

```
            Veritas Cluster Server One 5.0.0 by Symantec

Policy Master cluster configuration information verification:

Cluster Name : vcsonepm_cluster
Cluster ID : 65530
Broker Port : 14159

Private Heartbeat NICs for thoropt158:link1=eth0 link2=eth1
Private Heartbeat NICs for thoropt159:link1=eth0 link2=eth1

Is this information correct? [y,n,q] (y)
```

Configuring the Policy Master virtual IP addresses

```
            Veritas Cluster Server One 5.0.0 by Symantec


The following information is required to configure the Policy
Master:

        Public NICs used by each system in the Policy Master cluster
        Policy Master virtual IP addresses and netmasks

Active NIC devices discovered on thoropt158:
          NIC    : IP Address      : Netmask
        ----------------------------------------
          eth2   : 10.182.7.218    : 255.255.240.0


Active NIC devices discovered on thoropt159:
          NIC    : IP Address      : Netmask
        ----------------------------------------
          eth2   : 10.182.7.219    : 255.255.240.0

Enter the NIC for Policy Master Virtual IP address to use on
thoropt158: [b,q,?] (eth2)
Would you like to use the same NIC (eth2) on all PM nodes? [y,n,q,b]
(y)
```

```
Only one IP address 10.182.7.218 is detected for NIC eth2 under
system thoropt158. This IP address will be set as the base IP.

Only one IP address 10.182.7.219 is detected for NIC eth2 under
system thoropt159. This IP address will be set as the base IP.

Enter one or more Virtual IPs separated by space for the Policy
Master: [b,q,?] 10.182.14.6

Checking the 10.182.14.6 virtual IP address ..... Not in use

Enter the netmask for IP 10.182.14.6: [b,q,?] (255.255.240.0)
```

Confirming the Policy Master virtual IP address configuration

```
            Veritas Cluster Server One 5.0.0 by Symantec

Policy Master configuration verification:

Virtual IP 1:
        Virtual IP: 10.182.14.6
        Netmask: 255.255.240.0
NIC(s) under thoropt158:
        1: NIC - eth2; IP - 10.182.7.218
NIC(s) under thoropt159:
        1: NIC - eth2; IP - 10.182.7.219

Is this information correct? [y,n,q] (y)
```

Choosing a storage architecture

```
            Veritas Cluster Server One 5.0.0 by Symantec

VCS One PM should use shared storage for storing Configuration
Database
The following storage architectures are supported for storing VCS
One PM Configuration Database:

1. NetApp filer -- Shared storage exported by a specified NetApp
filer server
2. Other -- A local storage or a shared storage exported by an NFS
server and accessible by all the systems

Symantec recommends to use different shared storages for different
VCS One Policy Master server farms.

Storage architecture:
     1)  NetApp filer
     2)  Other
Please select a kind of Storage Architecture for the Configuration
Database with the index number: [1-2,q] 1
```

Configuring NetApp

```
                Veritas Cluster Server One 5.0.0 by Symantec

VCS One can use NFS for storing configuration information. Only
NetApp filers are supported as NFS servers. During installation, the
configuration must be mounted on the first node.
The following information is required to configure the database on
NetApp filers:

-- Mount point
-- IP address / hostname for NetApp filer
Note: The entries for the Policy Master nodes should exist in the
/etc/hosts directory on the NetApp filer.
-- NetApp filer access method
-- rsh (requires passwordless access between the Policy Master node
and the NetApp filer)
-- ssh (requires passwordless access between the Policy Master node
and the NetApp filer)
-- API (uses the NetApp SDK)
-- Username for accessing filer
-- Password for accessing filer in case of API access mode
-- IP address / hostname for the NIC connected to the filer for each
Policy Master system
-- File System Path on NetApp filer used to store the VCS One
configuration
Enter the mount point for the Configuration Database: [b,q,?]
/software/vcsone
Enter the fully qualified hostname or IP Address of the NetApp
filer: [b,q,?]
netapp3.veritas.com

NetApp filer access method
     1)  Use rsh
     2)  Use ssh
     3)  Use api
     b)  Back to previous menu
Select the access method to access the NetApp filer: [1-3,b,q,?] (1)
3
Enter the username to be used to access the NetApp filer: [b,q,?]
(root)
Enter the password for root:
Enter again:
Enter the hostname or IP Address for NIC on thoropt158: [b,q,?]
(thoropt158)
Enter the hostname or IP Address for NIC on thoropt159: [b,q,?]
(thoropt159)
Enter the exported path on the NetApp filer where VCS One
configuration would be stored: [b,q,?]
/vol/rgriffit_vol/vcsone
Do you wish to use API over SSL? [y,n,q,b,?] (n) y
Enter the SSL library path (version 0.9.8 or greater): [b] /lib
```

Confirming the NetApp configuration

```
            Veritas Cluster Server One 5.0.0 by Symantec
NetApp filer configuration:

        Mount Point: /software/vcsone
        NetApp filer: netapp3.veritas.com
        Access Mode: UseAPI
        Username: root
        Password not shown for security reasons
        Hostname / IP Address for NIC connected to NetApp filer:
                thoropt158: thoropt158
                thoropt159: thoropt159
        Path on NetApp filer: /vol/rgriffit_vol/vcsone
                SSL Path: /lib
Is this information correct and not in use by other VCS One Policy
Master server farms? [y,n,q] (y)

            Veritas Cluster Server One 5.0.0 by Symantec

Cleanup of directories on shared storage
The shared storage might contain directories from a previous
installation.
WARNING: If you do not clean up these directories, VCS One may be
improperly configured and fail to start up. The installer will quit
if the shared storage directories are not clean.

Do you wish to perform cleanup? [y,n,q] (y)
            Veritas Cluster Server One 5.0.0 by Symantec
```

Deciding whether to configure disaster recovery

```
VCS One PM Disaster Recovery Configuration

A VCS One global cluster links the individual VCS One clusters at
separate sites, and enables wide-area failover and disaster recovery
(DR) for the applications you configured. A VCS One global cluster
configuration can have a maximum of two clusters.
Clustering on a global level also requires an infrastructure to
replicate the application data between these clusters.

The following information is required to configure VCS One PM
disaster recovery:

        One or more virtual IP addresses and netmasks
        Public NICs used by each system for the virtual IP addresses

Do you want to configure VCS One PM disaster recovery? [y,n,q] (y) n
```

Showing configuration details

```
                Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-UUfIaK

Installing VCS One PM: 100%

Installation completed successfully on all systems


                Veritas Cluster Server One 5.0.0 by Symantec


Exporting the NetApp volume for thoropt158 ................. Done
Mounting the NetApp volume on thoropt158 ..................... Done
Cleaning up the previous configuration ....................... Done
Configure llthosts on thoropt158 ............................. Done
Configure llthosts on thoropt159 ............................. Done
Configure llttab on thoropt158 ............................... Done
Configure llttab on thoropt159 ............................... Done
Configure gabtab on thoropt158 ............................... Done
Configure gabtab on thoropt159 ............................... Done
Configure sysname on thoropt158 .............................. Done
Configure sysname on thoropt159 .............................. Done
Configure main.xml on thoropt158 ............................. Done
Configure main.xml on thoropt159 ............................. Done
Change some type attributes on thoropt158 .................... Done
Change some type attributes on thoropt159 .................. Done
Configure main.cf on thoropt158 ............................. Done
Configure main.cf on thoropt159 ............................. Done
Configure vcsone.ini on thoropt158 ........................... Done
Configure vcsone.ini on thoropt159 ........................... Done
Configure vcsone.conf on thoropt158 .......................... Done
Configure vcsone.conf on thoropt159 .......................... Done
Configure ATD on thoropt158 .................................. Done
Configure ATD on thoropt159 ................................ Done
Configure vcs run mode file on thoropt158 ..................... Done
Configure vcs run mode file on thoropt159 .................. Done
Configure vcsone db on thoropt158 ............................ Done
Configure vcsone db on thoropt159 ............................ Done
```

Starting the Policy Master processes

```
Do you want to start Veritas Cluster Server One by Symantec - Policy
Master processes now? [y,n,q] (y)


                Veritas Cluster Server One 5.0.0 by Symantec
```

```
Logs for installer are temporarily being created in /var/tmp/
installer-UUfIaK

  Starting VCS One PM: 100%
Startup completed successfully on all systems


           Veritas Cluster Server One 5.0.0 by Symantec

A string of five or more characters is required to encrypt passwords
in the responsefile
Enter five or more characters to be used as an encryption key:
123456
This key must be retained in a secure file and referenced using the
-enckeyfile option if the generated responsefile is to be used
again.

Press [Enter] to continue:
Installation log files, summary file, and response file are saved
at:

        /var/VRTS/install/logs/installer-UUfIaK

Installation - Success
Configuration - Success

The VCS One PM installation operation successful.
[root@thoropt158 rhel5_x86_64]#
```

Installing the VCS One client

This section provides sample output of the output from a VCS One client installation. Use this example for reference only. The output for each operating system version and installation environment differs slightly.

Starting the installer

This section provides a brief overview of the installation procedure.

See Chapter 4, "Installing and configuring the VCS One client" for detailed instructions.

To install the VCS One client

1. Mount the product disc.
2. Invoke the installer. Enter the following:
   ./installer

Reading the copyright information

```
                    Installation Program

Copyright (c) 2009 Symantec Corporation. All rights reserved.
Symantec, the Symantec Logo are trademarks or registered trademarks
of Symantec Corporation or its affiliates in the U.S. and other
countries. Other names may be trademarks of their respective owners.
The Licensed Software and Documentation are deemed to be "commercial
computer software" and "commercial computer software documentation"
as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Logs for installer are being created in /var/tmp/installer-hXl2SJ
```

Selecting a task

```
          Veritas Cluster Server One 5.0.0 by Symantec

Symantec Product          Version Installed   Licensed
================================================================

Symantec Licensing Utilities (VRTSvlic package) are not installed
due to which products and licenses are not discovered
Please use the menu below to continue.
Task Menu:

I) Install/Upgrade a Product C) Configure an Installed Product
L) License a Product P) Perform a Pre-Installation Check
U) Uninstall a Product D) View a Product Description
Q) Quit ?) Help
```

```
Enter a Task: [I,C,L,P,U,D,Q,?] i
```

Selecting a client installation

```
                Veritas Cluster Server One 5.0.0 by Symantec

1) Veritas Cluster Server One by Symantec - Policy Master (VCS One
PM)
2) Veritas Cluster Server One by Symantec - Client Daemon (VCS One
Client)
b) Back to previous menu

Select a product to install: [1-2,b,q] 2
```

Accepting the End User License Agreement

```
Do you agree with End User License Agreement (EULA) specified in
EULA.pdf file present on media? [y,n,q,?] (n) y
```

Reviewing the installation and configuration requirements

```
                Veritas Cluster Server One 5.0.0 by Symantec

VCS One client installation and configuration documentation

Be sure to establish passwordless communication between the system
that runs the installation script and the target installation
systems. You can use rsh or ssh as the access method. If you are
using rsh, specify the -rsh option while invoking the installation
script.

Before installing the VCS One client, meet the prerequisites and
prepare the following information:

1. Target installation system names.
2. Virtual address on which the Policy Master is listening. You must
enable communication between the system that runs the installation
script and the Policy Master system currently using the virtual IP
address.
3. Fully qualified names of the ESXi servers and control nodes. The
control node is the machine that is used to manage an ESXi server.

Press [Enter] to continue:
```

Entering the target systems

```
            Veritas Cluster Server One 5.0.0 by Symantec

Enter the system names separated by spaces on which to install
Veritas Cluster Server One by Symantec - Client Daemon (VCS One
Client): redhat95241 redhat95244

Initial system check:

Checking ssh communication with redhat95244 ... Linux 2.6.18-128.el5
Checking network speed with redhat95244 ..... OK
Checking VCS One Client installation on redhat95241 .. Not installed
Checking VCS One Client installation on redhat95244 .. Not installed

            Veritas Cluster Server One 5.0.0 by Symantec

Checking installed rpms on redhat95241
Checking installed rpms on redhat95244
```

Reviewing the package list

```
            Veritas Cluster Server One 5.0.0 by Symantec

The following VCS One Client rpms will be installed:

VRTSperl     Veritas Perl 5.10 Redistribution
VRTSvcsoneut Veritas Cluster Server One by Symantec - Utilities
VRTSvcsonemg Veritas Cluster Server One by Symantec - Message
             Catalogs
VRTSvcsonemn Veritas Cluster Server One by Symantec - Man Pages
VRTSvcsonec  Veritas Cluster Server One by Symantec - Command Line
             Utilities
VRTSvcsonecd Veritas Cluster Server One by Symantec - Client Daemon
VRTSvcsoneag Veritas Cluster Server One by Symantec - Bundled Agents
VRTSspt      Veritas Software Support Tools

Press [Enter] to continue:

            Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-VZkdbX
Check & Stop VCS One Client: 100%
```

Choosing when to configure the client

```
                Veritas Cluster Server One 5.0.0 by Symantec

It is possible to install VCS One Client rpms without performing
configuration. It is optional to configure VCS One Client now. If
you choose to configure VCS One Client later, you can either do so
manually, or run the installvcsonecd -configure command. The product
installation scripts can be found in /opt/VRTS/install directory
Are you ready to configure VCS One Client? [y,n,q] (y)

                Veritas Cluster Server One 5.0.0 by Symantec

You have chosen to configure VCS One Client. Answer the following
questions:

Enter 'b', to move back to the first question in the configuration
set.
Enter '?', to display additional information about the question.

After you complete each set of questions, you see a summary of the
information that you entered. Enter 'n', to repeat a question set
and modify your entries. Changes are implemented after you provide
and confirm all the configuration information, and the VCS One
Client installation process completes successfully.

Press [Enter] to continue:
```

Configuring the client

```
                Veritas Cluster Server One 5.0.0 by Symantec

To configure the VCS One client, the following is required:

  The Policy Master virtual IP addresses
  Client base IP addresses for available subnets on which Policy
  Master and client nodes can communicate.
  The location of SSL libraries (version 0.9.8 or greater)

Enter one or more Virtual IPs of the Policy Master separated by
space: [?] 10.198.92.127

Enter the local IP on redhat95241 to use for communication with the
virtual IP address 10.198.92.127 on the Policy Master. (press enter
to use default) [?] (None)

Enter the local IP on redhat95244 to use for communication with the
virtual IP address 10.198.92.127 on the Policy Master. (press enter
to use default) [?] (None)

IP addresses configured on redhat95241: 10.198.95.241 1.2.3.4
```

```
Enter a valid list of space separated IP addresses for redhat95241:
[?] (10.198.95.241 1.2.3.4) 10.198.95.241

IP addresses configured on redhat95244: 10.198.95.244

Enter a valid list of space separated IP addresses for redhat95244:
[?] (10.198.95.244) 10.198.95.244

Do you have permanent credential packages for the systems? [y,n,q,?]
(n)
Do you have deployment credential package for the systems? [y,n,q,?]
(n)
Would you like to configure the SSL library path? [y,n,q,?] (n) n

installer requires that ssh commands used between systems execute
without prompting for passwords or confirmations. If installer
hangs or asks for a login password, stop installer and run it again
with ssh configured for passwordless logins, or configure and use
the -rsh option.

Checking ssh communication with 10.198.92.127 .. Linux 2.6.18-53.el5
Checking network speed with 10.198.92.127 ..................... OK
Checking vcsoneatd process ............................... Running
Checking vcsoneatd version ............................. 6.0.17.0

Detected 1049 seconds time skew between 10.198.92.127 and
redhat95241!
Detected 2246 seconds time skew between 10.198.92.127 and
redhat95244!

WARNING: This will result in the client being unable to communicate
with the Policy Master. Proceed anyway?
Do you wish to continue? [y,n,q] (n) y

Virtual IPs of the Policy Master node: 10.198.92.127

Base IP addresses for redhat95241: 10.198.95.241

Base IP addresses for redhat95244: 10.198.95.244

Root Broker Hash: 10113e149b6fe8657ac84f2500af2623c0401936

Is this information correct? [y,n,q] (y)

     Virtual IPs of the Policy Master node: 10.198.92.127

     Base IP addresses for redhat95241: 10.198.95.241

     Base IP addresses for redhat95244: 10.198.95.244

     Root Broker Hash: 10113e149b6fe8657ac84f2500af2623c0401936
```

```
            Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-hXl2SJ

Installing VCS One Client: 100%

Installation completed successfully on all systems

            Veritas Cluster Server One 5.0.0 by Symantec

Configuring ATD on redhat95241
Creating an ATD principal for redhat95241 ................... Done
Retrieve broker port from 10.198.92.127 ..................... Done
Authenticating redhat95241
Checking communication between 10.198.92.127 and redhat95241
.......................................................... Done
Creating a ATD credential package ........................... Done
Executing the ATD credential package ........................ Done
Creating configuration files for the VCS One client ........ Done
Copying the configuration files to redhat95241 .............. Done
Adding redhat95241 to the Policy Master configuration ...... Done
Configuring ATD on redhat95244
Creating an ATD principal for redhat95244 ................... Done
Retrieve broker port from 10.198.92.127 ..................... Done
Authenticating redhat95244
Checking communication between 10.198.92.127 and redhat95244
.......................................................... Done
Creating a ATD credential package ........................... Done
Executing the ATD credential package ........................ Done
Creating configuration files for the VCS One client ........ Done
Copying the configuration files to redhat95244 .............. Done
Adding redhat95244 to the Policy Master configuration ...... Done
```

Starting the client

```
Do you want to start Veritas Cluster Server One by Symantec - Client
Daemon processes now? [y,n,q] (y)

            Veritas Cluster Server One 5.0.0 by Symantec

Logs for installer are temporarily being created in /var/tmp/
installer-hXl2SJ

Starting VCS One Client: 100%

Startup completed successfully on all systems

Installation log files, summary file, and response file are saved
at: /var/VRTS/install/logs/installer-hXl2SJ
```

```
Installation - Success
Configuration - Success
Startup - Success
VCS One Client installation operation successful.
```

Appendix E

Response file variables

The variable's type and dimension indicate how the values are defined. A semi-colon indicates the end of the definition. Typical formats include the following:

- A one-dimensional list is a simple list.
  $CPI::CFG{SYSTEMS}=[qw(sys30 sys31)];
- A two-dimensional list has the two dimensions on the left of the equal sign.
  $CPI::CFG{VCSONEPM_NETMASK}{<DUMMY>}= [qw (255.255.254.0) 255.555.254.00];
- A one-dimensional scalar is a variable with a single value.
  $CPI::CFG{UPI}= "VCSONECD";
- A two-dimension scalar is a variable with a single value and the variable to the left of the equal sign has two dimensions.
  $CPI::CFG{OPT}{CONFIGURE}=1;

Table E-1 describes response file variables. The response file variables depend on the product being installed. For example, the variables in the `installvcsoncd` response file differ from those in `installagpack`.

Table E-1 Response file variable definitions

Variable	Dimension/ Type	Definition
$CPI::CFG{AT_ROOTDOMAIN}	1 dimen. list	Optional. Defines the name of the system where the root broker is installed.
$CPI::CFG{DONOTINSTALL}	1 dimen. list	Optional. Defines a list of optional RPMs not to be installed on the systems.

Table E-1 Response file variable definitions (continued)

Variable	Dimension/ Type	Definition
$CPI::CFG{DONOTREMOVE}	1 dimen. list	Optional. Defines a list of RPMs not to be removed from the systems during uninstall.
$CPI::CFG{KEYS}{<SYSTEM>}	2 dimen. list	Optional. Defines a list of license keys to be registered on the systems during install.
$CPI::CFG{OPT_LOGPATH}	1 dimen. scalar	Optional. Defines where log files are copied following an install. The default location is /var/VRTS/install/logs.
$CPI::CFG{OPT}{CONFIGURE}	2 dimen. scalar	Optional. Performs configuration and startup of a product that has previously been installed using the -installonly option.
$CPI::CFG{OPT}{INSTALLCONFIG}	2 dimen. scalar	Optional. Designates a standard installation including licensing, install, configuration, and startup.
$CPI::CFG{OPT}{INSTALLONLY}	2 dimen. scalar	Optional. Installs RPMs but does not configure or start the product.
$CPI::CFG{OPT}{KEYFILE}	2 dimen. scalar	Optional. Defines the location of an ssh keyfile used to communicate with all remote systems.
$CPI::CFG{OPT}{LICENSE}	2 dimen. scalar	Optional. Licenses the product only.
$CPI::CFG{OPT}{NOLIC}	2 dimen. scalar	Optional. Installs the product without requiring entry of a license key.
$CPI::CFG{OPT}{PASSFILE}	2 dimen. scalar	Optional. Defines the location of a file containing a key to decrypt passwords stored in response files.
$CPI::CFG{OPT}{PATCHPATH}	2 dimen. scalar	Optional. Defines a location, typically a NetApp mount, from which remote systems can directly install product patches.
$CPI::CFG{OPT}{PKGPATH}	2 dimen. scalar	Optional. Defines a location, typically a NetApp mount, from which all remote systems can install product RPMs.

Table E-1 Response file variable definitions (continued)

Variable	Dimension/ Type	Definition
$CPI::CFG{OPT}{RSH}	2 dimen. scalar	Optional. Uses rsh instead of ssh as the communication method between systems.
$CPI::CFG{OPT}{TMPPATH}	2 dimen. scalar	Optional. Defines where a working directory is created to store temporary files and RPMs needed during the install. The default location is /var/tmp.
$CPI::CFG{OPT}{UNATTENDED}	2 dimen. scalar	Optional. Installs a product, with default configuration options, without manual intervention.
$CPI::CFG{OPT}{UNINSTALL}	2 dimen. scalar	Optional. Uninstalls a product.
$CPI::CFG{SYSTEMS}	1 dimen. list	Required. Lists systems on which the product is to be installed, uninstalled, or configured.
$CPI::CFG{SYSTEMSCFG}	1 dimen. list	Optional. Lists systems to be recognized for configuration when a secure environment prevents all systems from being installed at once.
$CPI::CFG{UPI}	1 dimen. scalar	Required. An abbreviation defining the product to be installed, uninstalled, or configured. Product abbreviations include: VCSONEPM, VCSONECD, VCSONESIM, HAAT, and AGPACK.
$CPI::CFG{OPT}{CREATE_DEPLOYMENT_CREDENTIAL}	2 dimen scalar	Optional. Designates that the create_deployment_credential option needs to be performed.
$CPI::CFG{VCSONECD_CLUSTERIP}	1 dimen scalar	Required. Lists the virtual IP addresses on which the Policy Master is listening.
$CPI::CFG{VCSONECD_EVACUATE_GROUPS}	1 dimen scalar	Optional. When set to Y, this variable tries to evacuate online service groups.
$CPI::CFG{OPT}{CREATECREDENTIAL}	2 dimen scalar	Optional. Designates that the createcredential option must be performed.

Table E-1 Response file variable definitions (continued)

Variable	Dimension/ Type	Definition
$CPI::CFG{VCSONECD_CREDPKG}	1 dimen scalar	Required. Determines if the product is installed using credential packages. The values are Y (yes) and N (no).
$CPI::CFG{VCSONECD_DEPLOYMENTCREDPKG}	1 dimen scalar	Optional. Determines if the product is installed using the deployment credential package. The values are Y (yes) and N (no).
$CPI::CFG{VCSONECD_CREDENTIAL}	2 dimen scalar	Required. Defines the location of the credential package. The path can be absolute or relative to the response file location. If you are using credential packages for the configuration, you must set this variable.
$CPI::CFG{VCSONECD_SSLLIBPATH}	1 dimen scalar	Optional. Defines the location of the SSL libraries. If agents will use SSL, you must set this variable.
$CPI::CFG{VCSONEPM}{VCSONEPM_PM_USESOLARISMPATH}	1 dimen scalar	Optional. Defines whether to use the multipathing functionality of the Solaris operating system daemon.
$CPI::CFG{VCSONEPM_CLEANUPSTORAGE}	1 dimen scalar	Required. Defines whether the storage needs to be cleaned up.
$CPI::CFG{VCSONEPM_CLUSTERID}	1 dimen scalar	Required. Must be an integer between 0 and 65535 that uniquely identifies the Policy Master cluster.
$CPI::CFG{VCSONEPM_PMDB_DG}	1 dimen scalar	Optional. Defines the disk group name.
$CPI::CFG{VCSONEPM_PMDB_FS}	1 dimen scalar	Required. Defines the file system type. If shared storage is not used, local-dir is used.
$CPI::CFG{VCSONEPM}{VCSONEPM_PM_MPATHCOMMAND}	1 dimen scalar	Optional. Defines the absolute path for in.mpathd in Solaris.
$CPI::CFG{VCSONEPM__PMDB_MOUNT}	1 dimen scalar	Required. Defines the mount point for the configuration data.
$CPI::CFG{VCSONEPM_PMDB_VOLUME}	1 dimen scalar	Optional. Defines the volume name.

Table E-1 Response file variable definitions (continued)

Variable	Dimension/ Type	Definition
$CPI::CFG{VCSONEPM_LLTLINK#} {*SYSTEM*}	2 dimen scalar	Required. Defines the NIC to be used for a private heartbeat link on each system. Two LLT links are required per system (LLTLINK1 and LLTLINK2). Up to four LLT link can be configured.
$CPI::CFG{VCSONEPM_LLTLINKLOWPRI} {*SYSTEM*}	2 dimen scalar	Optional. Defines a low priority heartbeat link. Typically, LLTLINKLOWPRI is used on a public network to provide an additional layer of communication.
$CPI::CFG{VCSONEPM_PMDB_NETAPP}	1 dimen scalar	Optional. Defines where to store the database on NetApp export.
$CPI::CFG{VCSONEPM_PM_NETMASK}	1 dimen list	Required. Defines the list of netmasks for each of the corresponding virtual IPs.
$CPI::CFG{VCSONEPM_VCSONEPMNIC MASK} {num} {*SYSTEM*}	2 dimen list	Required. Defines the NICs for each of the corresponding virtual IPs. If you use the same NIC on all systems, enter **ALL**.
$CPI::CFG{VCSONEPM_PMDB_SFCONFIG}	1 dimen scalar	Optional. Designates that the installer create the Storage Foundation configuration; that is, it starts processes, and creates and mounts the disk group and volume.
$CPI::CFG{VCSONEPM_PMDB_SFDSK}	1 dimen list	Optional. Defines the disks that are part of the disk group and volume.
$CPI::CFG{VCSONEPM_SFINSTALL}	1 dimen scalar	Required. Designates that the installation will install Storage Foundation packages.
$CPI::CFG{VCSONEPM_PMDB_SFVOLSIZE}	1 dimen scalar	Optional. Defines the volume size the installer will create for the disks defined by $CPI::CFG{VCSONEPM_SFDSK}.
$CPI::CFG{VCSONECD_SELINUX_PERMISSIVE}	1 dimen scalar	Optional. Specifies if SELinux changes from enforcing mode to permissive mode.

Table E-1 Response file variable definitions (continued)

Variable	Dimension/ Type	Definition
$CPI::CFG{VCSONECD_VALIDIP}{ SYSTEM}	2 dimen scalar	Optional. Defines all the base IP addresses that will be used for communication with the VCS One policy Master on the client systems.
$CPI::CFG{VCSIBECD_DC_PMCO MM}	1 dimen scalar	Required. Specifies if passwordless communication with the active Policy Master system is enabled.
$CPI::CFG{VCSONECD_CC_ATPO RT}	1 dimen scalar	Required. Defines the authentication service port used on the VCS One Policy Master.
$CPI::CFG{VCSONEPM_SINGLESY STEM}	1 dimen scalar	Optional. Defines if a single system installation is acceptable. Valid values are **Y** and **N**. This variable is checked only if the installation needs to be performed on a single system. If you specify **N**, the installation exits.
$CPI::CFG{VCSONEPM_PM_NIC}	1 dimen scalar	Required. Defines the NICs for each corresponding virtual IP address.
$CPI::CFG{VCSONEPM_PM_VIP}	1 dimen list	Required. Lists the virtual IP addresses on which the Policy Master is listening.
$CPI::CFG{VCSONEPM_CLUSTER NAME}	1 dimen scalar	Required. Defines the Policy Master cluster name.
$CPI::CFG{VCSONEPM_PMDB_NF ACCESS}	1 dimen scalar	Optional. Defines the method of accessing the NetApp filer.
$CPI::CFG{VCSONEPM_PMDB_NA USER}	1 dimen scalar	Optional. Defines the user name that is used to access the NetApp filer.
$CPI::CFG{VCSONEPM_PMDB_NA PASSWD}	1 dimen scalar	Optional. Defines the NetApp filer password.
$CPI::CFG{VCSONEPM_PMDB_NA FSPATH}	1 dimen scalar	Optional. Defines the path of the volume that is exported from the NetApp filer.
$CPI::CFG{VCSONEPM_PMDB_NA FILER}	1 dimen scalar	Optional. Defines the name of the NetApp filer used for shared storage.

Table E-1 Response file variable definitions (continued)

Variable	Dimension/ Type	Definition
$CPI::CFG{VCSONEPM_DR_NETMASK}	1 dimen list	Required. Defines the netmasks for all of the Virtual IP addresses for disaster recovery.
$CPI::CFG{VCSONEPM_DR_NIC}{num}{<SYSTEM>}	2 dimen list	Required. Defines the NICs for all of the corresponding Virtual IP addresses for Disaster Recovery.
$CPI::CFG{VCSONEPM_DR_VIP}	1 dimen list	Required. Defines the virtual IP addresses for Disaster Recovery.

Table E-2 lists the response file variable definitions for the `-create_deployment_credential` option.

Table E-2 Response file variable definitions for -create_deployment_credential

Variable	Dimen/ Type	Definition
$CPI::CFG{VCSONECD_DC_CLUSTERIP}	1 dimen scalar	Required. Lists virtual IP addresses on which the Policy Master is listening when you use the `-create_deployment_credential` option.
$CPI::CFG{VCSONECD_DC_DESTDIR}	1 dimen scalar	Required. Defines the target directory in which to copy the generated credential file when you use the `-create_deployment_credential` option.
$CPI::CFG{VCSONECD_DC_TIMEOUT}	1 dimen scalar	Required. Defines the timeout of the deployment credential that is being created. A client cannot connect to the Policy Master after the timeout period.

Table E-3 lists the response file variable definitions for the –createcredential option.

Table E-3 Response file variable definitions for -createcredential

Variable	Dimen/ Type	Definition
$CPI::CFG{VCSONECD_CC_SYSTEMS}	1 dimen scalar	Required. Lists the systems for which credentials are to be created.
$CPI::CFG{VCSONECD_CC_PLATFORM}	1 dimen scalar	Required. Lists the platforms for which credentials are to be created.
$CPI::CFG{VCSONECD_CC_CLUSTERIP}	1 dimen scalar	Required. Lists the virtual IP addresses on which the Policy Master is listening when you use the -createcredential option.
{VCSONECD_CC_DESTDIR}	1 dimen scalar	Required. Defines the target directory in which to copy the generated credential files when you use the -createcredential option.

Appendix F

Required packages

This appendix contains information about the VCS One Policy Master and client packages. Topics include:

- Mandatory package list for a Policy Master installation with Storage Foundation
- Mandatory client packages

Mandatory package list for a Policy Master installation with Storage Foundation

Table F-1 lists mandatory packages when the Policy Master is installed with Storage Foundation.

Table F-1 Mandatory Policy Master packages with Storage Foundation

Package	Description
VRTSperl	Veritas Perl 5.10 redistribution
VRTSvlic	Veritas licensing
VRTSatClient	Symantec Product Authentication Service (AT) client
VRTSvxvmcommon	Veritas Volume Manager by Symantec common package
VRTSvxvmplatform	Veritas Volume Manager by Symantec platform-specific package
VRTSvdid	Veritas Device Identification API
VRTSicsco	Symantec Infrastructure Core Services common
VRTSpbx	Symantec Private Branch Exchange

Table F-1 Mandatory Policy Master packages with Storage Foundation (continued)

Package	Description
VRTSobc33	Veritas Enterprise Administrator Core Service
VRTSob	Veritas Enterprise Administrator Service
VRTSdsa	Veritas Datacenter Storage Agent
VRTSfspro	Veritas File System Management Services Provider
VRTSvmman	Veritas Volume Manager manual pages
VRTSlvmconv	Veritas Linux LVM to VxVM converter
VRTSddlpr	Veritas Device Discovery Layer Services Provider
VRTSvmpro	Veritas Volume Manager Management Services Provider
VRTSdcli	Veritas distributed command line interface
VRTSalloc	Veritas Volume Manager Intelligent Storage Provisioning
VRTSvxfscommon	Veritas File System common package
VRTSvxfsplatform	Veritas File System platform-specific package
VRTSfsman	Veritas File System manual pages
VRTSfssdk	Veritas File System software developer kit
VRTSfsmnd	Veritas File System software developer kit manual pages
VRTSvcsoneut	Veritas Cluster Server One by Symantec - utilities
VRTSllt	Veritas low latency transport
VRTSgab	Veritas group membership and atomic broadcast
VRTSvxfen	Veritas I/O fencing
VRTSvcsonedb	Veritas Cluster Server One by Symantec - configuration database
VRTSvcsonemg	Veritas Cluster Server One by Symantec - message catalogs
VRTSvcs	Veritas Cluster Server
VRTSvcsag	Veritas Cluster Server bundled agents
VRTSvcsmg	Veritas Cluster Server message catalogs
VRTSvcsonemn	Veritas Cluster Server One by Symantec - man pages

Table F-1 Mandatory Policy Master packages with Storage Foundation (continued)

Package	Description
VRTSpmmag	Veritas Cluster Server PMM agents
VRTSvcsonec	Veritas Cluster Server One by Symantec - command line utilities
VRTSvcsonepm	Veritas Cluster Server One by Symantec - Policy Master
VRTSvcsonew	Veritas Cluster Server One by Symantec - web console
VRTSspt	Veritas software support tools

Mandatory package list for a Policy Master installation without Storage Foundation

Table F-2 lists mandatory packages when the Policy Master is installed without Storage Foundation.

Table F-2 Mandatory Policy Master packages without Storage Foundation

Package	Description
VRTSperl	Veritas Perl 5.10 redistribution
VRTSvlic	Veritas licensing
VRTSatClient	Symantec Product Authentication Service (AT) client
VRTSvcsoneut	Veritas Cluster Server One by Symantec - utilities
VRTSllt	Veritas low latency transport
VRTSgab	Veritas group membership and atomic broadcast
VRTSvxfen	Veritas I/O fencing
VRTSvcsonedb	Veritas Cluster Server One by Symantec - configuration database
VRTSvcsonemg	Veritas Cluster Server One by Symantec - message catalogs
VRTSvcs	Veritas Cluster Server
VRTSvcsag	Veritas Cluster Server bundled agents
VRTSvcsmg	Veritas Cluster Server message catalogs

Table F-2 Mandatory Policy Master packages without Storage Foundation (continued)

Package	Description
VRTSvcsonemn	Veritas Cluster Server One by Symantec - man pages
VRTSpmmag	Veritas Cluster Server PMM agents
VRTSvcsonec	Veritas Cluster Server One by Symantec - command line utilities
VRTSvcsonepm	Veritas Cluster Server One by Symantec - Policy Master
VRTSvcsonew	Veritas Cluster Server One by Symantec - web console
VRTSspt	Veritas software support tools

Mandatory client packages

Table F-3 lists the packages you must install.

Table F-3 Mandatory client packages

Package	Description
VRTSperl	Veritas Perl 5.10 redistribution
VRTSvcsoneut	Veritas Cluster Server One by Symantec - utilities
VRTSvcsonemg	Veritas Cluster Server One by Symantec - message catalogs
VRTSvcsonemn	Veritas Cluster Server One by Symantec - man pages
VRTSvcsonec	Veritas Cluster Server One by Symantec - command line utilities
VRTSvcsonecd	Veritas Cluster Server One by Symantec - client daemon
VRTSvcsoneag	Veritas Cluster Server One by Symantec - bundled agents

Index

I

L

N

P

R

S

T

U

V

W