Symantec High Availability Solution Guide for VMware

Linux

6.0.2

March 2013

Symantec

Symantec™ High Availability Solution Guide for VMware

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: 6.0.2

Document version: 6.0.2 Rev 2

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 support 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/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/contact_techsupp_static.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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support 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

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support 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

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

Introducing the Symantec High Availability solution for VMware

This chapter includes the following topics:

How the Symantec High Availability solution works in a VMware environment

The Symantec High Availability solution for VMware employs Veritas Cluster Server (VCS) and its agent framework to monitor the state of the applications and their dependent components running on the virtual machines that use non-shared storage. Specific agents are available to monitor the application, storage, and network components. Together, these agents monitor the overall health of the configured applications by running specific commands, tests, or scripts.

The storage configuration in the VMware virtual environment determines how VCS functions differently in a non-shared virtual environment. The non-shared storage configuration in the VMware virtual environment involves the VMware VMDK and RDM disks that reside on the shared datastore. This datastore is accessible to multiple virtual machines. However, the disks are attached to a single virtual machine at any given point of time. VCS provides a new storage agent “VMwareDisks” that communicates with the VMware ESX/ESXi hosts to perform

the disk detach and attach operations to move the storage disk between the virtual machines, in a VCS cluster.

In event of an application failure, the agents attempt to restart the application services and components for a configurable number of times. If the application fails to start, they initiate an application failover to the failover target system. During the failover, the VMwareDisks agent moves the storage disk to the failover target system, the network agents bring the network components online, and the application-specific agents then start the application services on the failover target system.

In case of a virtual machine fault, the VCS agents begin to fail over the application to the failover target system. The VMwareDisks agent sends a disk detach request to the ESX/ESXi host. After the detach operation is successful, the agent proceeds to attach the disks to the new failover target system.

In a scenario where the ESX/ESXi host itself faults, the VCS agents begin to fail over the application to the failover target system that resides on another host. The VMwareDisks agent communicates with the new ESX/ESXi host and initiates a disk detach operation on the faulted virtual machine. The agent then attaches the disk to the new failover target virtual machine.

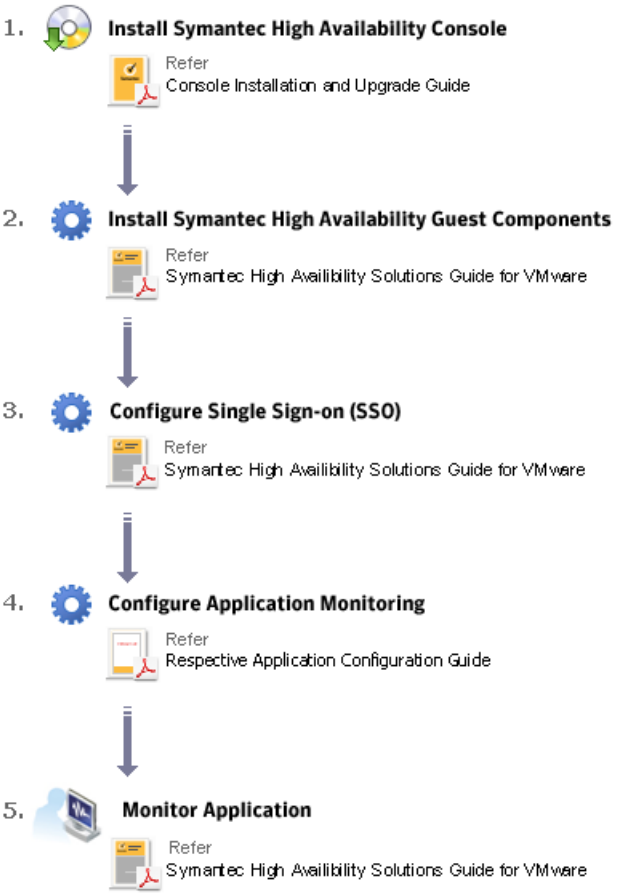
For details on the VCS configuration concepts and clustering topologies, refer to the *Veritas Cluster Server Administrator's Guide*.

For details on the application agents, refer to the application-specific agent guide. For details on the storage agents, refer to the *VCS Bundled Agents Reference Guide*.

Getting started with Symantec High Availability solution

The Symantec High Availability solution can be deployed by following five simple steps.

The following figure represents the workflow for getting started with the Symantec High Availability solution and the corresponding document you must refer for details.



Understanding Symantec High Availability terminology

Table 1-1 lists the technical terms, their abbreviated form, and synonyms used in this document. The table also provides the equivalent terms used in the Veritas Cluster Server and Symantec ApplicationHA documentation.

Based on context, the indicated synonyms have been used in the vCenter-integrated GUI, as well as in this document.

Table 1-1 Terminology disambiguation chart

Symantec High Availability Solutions documentation	Veritas Cluster Server documentation	Symantec ApplicationHA documentation
■ System (until it becomes a part of a VCS cluster) ■ VCS cluster system (once it joins a cluster) ■ Failover target system (once it is included in the list of failover targets for an application)	■ Node ■ VCS Cluster Node ■ Member	■ Guest ■ Guest virtual machine
■ Cluster ■ VCS Cluster	■ Cluster ■ VCS Cluster	Not applicable
■ ESX host	■ ESX host	■ ESX host
■ ESX cluster	■ ESX cluster	■ ESX cluster
■ Datacenter	■ Datacenter	■ Datacenter
■ Application ■ Application instance ■ Service Group	■ Service group	■ Component group
■ Application components	■ Resources	■ Application components
■ Symantec High Availability Guest Components ■ guest components ■ VCS	■ VCS	■ Guest components
■ Symantec High Availability Console ■ Console	■ Symantec High Availability Console ■ Console	■ Symantec High Availability Console ■ Console
■ Symantec High Availability tab ■ Symantec High Availability tab view ■ tab	■ Symantec High Availability tab	■ Symantec High Availability tab ■ Symantec High Availability tab view ■ tab

Table 1-1 Terminology disambiguation chart *(continued)*

Symantec High Availability Solutions documentation	Veritas Cluster Server documentation	Symantec ApplicationHA documentation
■ Symantec High Availability Dashboard ■ dashboard	■ Symantec High Availability Dashboard ■ dashboard	■ Symantec High Availability Dashboard ■ dashboard
■ Application dependency	■ Service group dependency	Not applicable
■ Component dependency	■ Resource dependency	■ Component dependency

Understanding operation names

Table 1-2 describes lists the names of VCS administrative operations/tasks that you can perform from the VMware vSphere Client GUI, as well as the equivalent operation names used in Veritas Cluster Server documentation:

Table 1-2 Task disambiguation chart

vSphere Client GUI-based operations	VCS operations
Start Application	Online Service Group
Stop Application	Offline Service Group
Switch	Switch To
Add Failover System	Add Node
Remove Failover System	Remove Node
Enter Maintenance Mode	Freeze Service Group
Exit Maintenance Mode	Unfreeze Service Group
Clear Fault State	Clear Fault
Resolve a Held-up Operation	Flush
Unconfigure Application Monitoring	Delete Service Group
Determine Application State	Probe
Stop/Start dependent components in order	Propagate (option for online/offline SGs)
Suspend application monitoring after reboot	Persistent (option for freeze)

About setting up the Symantec High Availability solution in a VMware environment

Table 1-3 describes the tasks for setting up the Symantec High Availability solution in a VMware virtualization environment.

Table 1-3 Tasks for setting up Symantec High Availability in a VMware virtualization environment

Task	Description
Install the Symantec High Availability Console	Install the Symantec High Availability Console on a system identified to serve as a Console server. This installation registers the Symantec High Availability plugin on the vCenter Server. For more details refer to the *Symantec High Availability Console Installation and Upgrade Guide*. After the installation is complete, the Symantec High Availability tab, Symantec High Availability dashboard, and the Symantec High Availability home page are added to the vSphere client. The Symantec High Availability tab is visible when you select a virtual machine from the VMware vCenter Server inventory. The Symantec High Availability dashboard is visible when you select a VMware cluster or a datacenter from the VMware vCenter Server inventory. The Symantec High Availability home page is added as an vSphere Client extension under its Solutions and Applications pane. Use the Symantec High Availability home page to perform any of the following tasks: ■ Install guest components ■ Manage licenses Use the Symantec High Availability tab to configure and control application monitoring on virtual machines that are managed from the VMware vCenter Server. You can perform these operations per virtual machine. Use the Symantec High Availability dashboard to administer the configured applications on virtual machines in a VMware cluster/datacenter. You can perform these operations at a VMware cluster or datacenter level. For details, refer to the *Symantec High Availability Console Installation and Upgrade Guide*.

Table 1-3 Tasks for setting up Symantec High Availability in a VMware virtualization environment *(continued)*

Task	Description
Install Symantec High Availability guest components	Install the Symantec High Availability guest components on all the systems where you wish to configure the application for high availability. This installs the infrastructure, application, and replication agents and the configuration wizards on the systems. **Note:** Before you install the guest components, you must install the Console.
Configure SSO	Configure single sign-on between the system where you installed the guest components and the Console host. **Note:** You need to manually configure SSO, if you have installed the guest components using the product installer or CLI. The Guest Components installer launched using the vSphere Client menu configures SSO after the guest components installation is complete. SSO provides secure communications between the system and the Console. It uses digital certificates for permanent authentication and uses SSL to encrypt communications. The single sign-on authentication is required for all VCS cluster operations on the system. It is also required so that the vCenter server does not prompt you for a user name and password each time you log on to the vSphere Client and click on a system to view the application status.
Manage storage	Configure the storage disks to save the application data. See "Managing storage" on page 19.
Configure application monitoring	Run the Symantec High Availability configuration wizard to configure application monitoring. For details refer to the respective application configuration guide.

Supported VMware versions

The Symantec High Availability solution 6.0.2 supports the following VMware servers and management clients:

VMware ESX Server	4.1, 4.1 Update 1, 4.1 Update 2
VMware ESXi Server	4.1, 5.0, 5.0 Update 1 and 5.1

VMware vCenter Server	4.1 U2, 5.0, 5.0 U1a/b and 5.1 **Note:** VMware Fault Tolerance is not supported.
VMware vSphere Client	4.1 U2, 5.0, 5.0 U1a/b and 5.1

Chapter 2

Deploying the Symantec High Availability solution

This chapter includes the following topics:

Managing storage

Configure the storage disks to save the application data.

VMware virtualization manages the application data by storing it on SAN LUNs (RDM file), or creating virtual disks on a local or networked storage attached to the ESX host using iSCSI, network, or Fibre Channel. The virtual disks reside on a datastore or a raw disk that exists on the storage disks used.

For more information, refer to the VMware documentation.

The application monitoring configuration in a VMware environment requires you to use the RDM or VMDK disk formats. During a failover, these disks can be deported from a system and imported to another system.

Consider the following to manage the storage disks:

- Use a networked storage and create virtual disks on the datastores that are accessible to all the ESX servers that hosts the VCS cluster systems.

- In case of virtual disks, create non-shared virtual disks (Thick Provision Lazy Zeroed).
- Add the virtual disks to the virtual machine on which you want to start the configured application.
- Create either LVM logical volumes or VxVM volumes.
- Mount the volumes on the mount point.

The following VCS storage agents are used to monitor the storage components involving non-shared storage:

- If the storage is managed using LVM, the LVMVolumeGroup and LVMLogicalVolume agents are used.
- If the storage is managed using VXVM, the DiskGroup and Volume agents are used.

Before configuring the storage, you can review the resource types and attribute definitions of these VCS storage agents. For details refer to the *Veritas Cluster Server Bundled Agents Reference Guide*.

Installing the Symantec High Availability guest components

To configure an application for high availability, you must install the Symantec High Availability guest components on the systems where you want to configure the application.

Note: Before you begin to install the guest components, ensure that you have installed the Symantec High Availability Console on a system that is dedicated to serve as a Console Server.

For more details refer to *Symantec High Availability Console Installation and Upgrade Guide*.

You can install the guest components in the following ways:

- Using the product installer
  Use this method to install the guest components in physical or virtual environments.
  For more details refer to the product installation and upgrade guide.
- Using the command line interface (CLI)
  Use this method to install the guest components in physical or virtual environment.

For more details refer to the product installation and upgrade guide.

- Using the VMware vSphere client integrated menu
  Use this method to install the guest components in a VMware environment.
  See "About installing Symantec High Availability guest components using the vSphere Client menu" on page 22.

Note: The systems where you plan to install the Symantec High Availability guest components must run one of the following operating systems:

- Win2008 x64 (including SP1 and SP2)

- Win2008 R2 x64 (including SP1)

Note: Ensure that the systems where you plan to install the Symantec High Availability guest components, run one of the supported Linux operating systems.

Supported guest operating systems

Table 2-1 shows the supported operating systems for this release.

Table 2-1 Supported guest operating systems

Operating systems	Levels
Oracle Enterprise Linux 5	Updates 6, 7, and 8
Oracle Enterprise Linux 6	Updates 1 and 2 **Note:** You cannot use the vSphere Client GUI menu to install VCS binaries on systems running OEL 6. You must install the binaries for OEL6 by using the common product installer (CPI). For more information, see the *VCS Installation Guide*.
Red Hat Enterprise Linux 5	Updates 5, 6, 7, 8, and 9
Red Hat Enterprise Linux 6	Updates 1, 2, and 3
SUSE Linux Enterprise 10	SP 4
SUSE Linux Enterprise 11	SP 1 and SP 2

Note: 64-bit operating systems are only supported.

If your system is running a lower level of either Red Hat Enterprise Linux, SUSE Linux Enterprise Server, or Oracle Enterprise Linux, than indicated above, you must upgrade it before attempting to install VCS. Consult the Red Hat, SUSE, or Oracle documentation for more information on upgrading or reinstalling your system.

Symantec supports only Oracle, Red Hat, and SUSE distributed kernel binaries.

Symantec products operate on subsequent kernel and patch releases, provided the operating systems maintain kernel ABI (application binary interface) compatibility.

About installing Symantec High Availability guest components using the vSphere Client menu

Installing the guest components using the vSphere Client menu involves the following tasks:

- To install the guest components on the systems running Linux operating system, copy the platform-specific guest installation package on to the Console host.
  See "Copying the platform-specific guest installation package" on page 22.
- Installing the guest components using the installation wizard.
  See "Installing Symantec High Availability guest components using the vSphere Client menu" on page 23.

Note: To use CPI installer-based methods, such as automated installation using response files, or manual installation using Linux commands and utilities, see the *VCS 6.0 Installation Guide*.

Copying the platform-specific guest installation package

To install the Symantec High Availability guest components on the virtual machines running Linux operating system, ensure that the platform-specific Symantec High Availability guest components installation package is available on the Console host.

Note: The VCS binaries for SLES and RHEL operating systems are stored on separate DVDs. If you want to install VCS on both RHEL and SLES guests using the vSphere Client GUI, then you must copy the RPMs for one of the Linux flavors onto the Console host. For example, if you install the Console using the Veritas Product Installer or VPI (which is a command-line based product installer for Veritas storage and high availability products from Symantec) the RHEL DVD, then the RHEL binaries are automatically copied to the Console host. You must later copy the SLES binaries by running the following command: `CopyInstaller.bat <Source>`. Where <Source> is the directory path where the SLES disc is mounted or copied.

Perform the following to copy the platform-specific guest installation package on the Console host

1. Insert the product software disc for Linux operating system into your system drive.
2. On the Console host, navigate to the following path:

   `cd <Installation Path>\Veritas\ApplicationHA\Console\installer`

   For example:

   `cd C:\Program Files\Veritas\ApplicationHA\Console\installer`

   Where C:\ is the system drive
3. Run the Copyinstaller.bat file.
4. Enter the parameters in the following format.

   `CopyInstaller.bat <Source>`

   Where, *<Source>* is the directory path where the installer disc is mounted or copied.

   For example:

   ```
   CopyInstaller.bat <D:>dvd1

   CopyInstaller.bat <D:>dvd2-linux\rhel5_x86_64

   CopyInstaller.bat <F:>dvd2-linux\sles11_x86_64

   CopyInstaller.bat \\shared\dvd2-linux\win2k8_x86_64
   ```

Installing Symantec High Availability guest components using the vSphere Client menu

Consider the following points before you proceed with the installation.

- You can use this option to install the following Symantec high availability products. You can use this option to install the products on multiple virtual machines across ESX clusters and data centers registered with a VMware vCenter Server.
  - Symantec ApplicationHA guest components
  - Veritas Cluster Server (VCS)
- Ensure that you have installed and enabled VMware Tools on the machine/s where you want to install the guest components. Ensure that the VMware Tools version is compatible with the ESX version in your environment.
- The installer prompts for the user account details of the system where you want to install the guest components. This user account must have the local administrator privileges.
- Installation of guest components using the vSphere Client GUI also configures single sign-on (SSO) between the virtual machine and the Console host. However, if the SSO configuration fails, you must manually configure it after the guest installation is complete. To manually configure SSO, in the Inventory view, click the virtual machine where you want to configure SSO, and then click the Symantec High Availability tab. Specify the user name and password of a user account with administrative or root privileges on the virtual machine. The single sign-on authentication is used for all operations on the virtual machine. This is also required so that the server does not prompt you for a user name and password each time you log on to the vSphere Client and click on a virtual machine to view its status.
- Installation of guest components using the vSphere Client GUI ensures that supported VCS agents for this release are also automatically installed.
- If the VOM Managed Host components of any version earlier to 5.0 are installed in your environment, then the guest components installer upgrades these components to its latest version.

Perform the following steps to install the Symantec High Availability guest components on the virtual machines, through the vSphere Client menu

---

Note: Execute only those steps that are applicable to the guest operating system.

---

1 Using the vSphere Client, connect to the vCenter Server and navigate to **Home > Solutions and Applications > Symantec High Availability**. On the Getting Started tab, click **Install Guest Components**

Alternatively,

Using the vSphere Client, connect to the vCenter Server and navigate to **Home > Hosts and Clusters**. From the vCenter inventory tree view, right-click on the datacenter, cluster or any of the virtual machines, and select **Symantec High Availability > Install Guest Components**.

This launches the Symantec High Availability Guest Components Installer.

2 On the Welcome panel, review the prerequisites and then click **Next**.

3 On the vCenter Server Details panel, specify the vCenter Server user credentials and then click **Next**.

The wizard discovers only those virtual machines where the user has the permissions.

The specified user must have the following privileges:

- Symantec High Availability administrator privileges to perform the installation on the virtual machines.
- vCenter privileges for "create tasks", "update tasks" and "acquire guest control ticket" on the virtual machines.

4 On the Product Selection panel, select the product that you want to install.

The **Packages included** table lists the installation packages that are included in the selected product.

Review the license agreement that is available against the corresponding package, select **I accept the terms of license agreement** and then click **Next**.

A package is installed based on the operating system that runs on selected systems.

Note: If a required package is not displayed, you must copy that package to the Console host and then run this wizard again.

See "Copying the platform-specific guest installation package" on page 22.

---

5 On the System Selection panel, perform the following tasks:

- Select the virtual machines on which you want to install the guest components.

  To select the virtual machines

- Skip this sub-step if you launched the installation wizard by right-clicking a system in the inventory view of the vSphere Client GUI.
  Click **Add**.
- On the Select Virtual Machines panel, select the desired virtual machines, specify the required details and click **OK**.
  The specified details apply to all the selected virtual machines. If they are different for one or more machines, you can edit them later.

- If required, edit the user credentials and the license key details.
  If the user credentials and license key is different for an individual virtual machine, you can edit the details inline.
  If the details to be edited are same for multiple virtual machines, select the desired machines and click **Edit**. On the **Edit Virtual Machine Details** panel, enter the details that apply to the selected virtual machines and click **OK**.
- Click **Install** to begin the installation.
  The installer performs the required validation checks on the selected virtual machines and moves to the Installation panel, if all the selected virtual machines pass the validation checks.
  If the validation checks fail on any of the virtual machines, the status is reflected as follows:
  For virtual machines that pass the validation checks: **Ready for install**.
  For virtual machines that do not pass the validation checks: **Verification failed**
  To view the cause of validation failure, select the virtual machine. The details are displayed in the Verification Details box.
  Rectify the issue and then click **Install**.
  The installer re-validates the failed virtual machines.

The installer does not proceed with the installation unless all the selected virtual machines have passed the validation checks.

6 On the Installation panel, review the progress of the tasks queued. After all the tasks are queued and the status is marked as **complete**, click **Finish**.

This indicates that the selected virtual machines are queued for installation.

You can now view the installation progress under the Recent Tasks on vSphere Client.

After the installation is complete single sign-on is configured for the virtual machines with the Symantec High Availability Console host. You can now proceed to configure application monitoring, using the Symantec High Availability tab.

For details, refer to the individual application configuration guide.

Note: If the SSO configuration has failed for a virtual machine and you select that virtual machine from vSphere Client to configure application monitoring for an application, then the Symantec High Availability tab first displays a panel to specify the virtual machine user credentials. This configures the single sign-on for the virtual machine with the Symantec High Availability Console host. After you configure the single sign-on you can configure application monitoring for an application running on the virtual machine.

Upgrading Symantec High Availability guest components

Upgrading Symantec High Availability guest components, involves upgrading Veritas Cluster Server (VCS) on the guests. If you have VCS already installed on the guests, you can upgrade to Release 6.0.2 using the vSphere Client GUI. The steps to upgrade and install are same. For more information about the steps to install:

See "Installing the Symantec High Availability guest components" on page 20.

Supported VCS upgrade paths

Table 2-2 provides the supported scenarios for upgrading to Veritas Cluster Server 6.0.2.

Table 2-2 VCS upgrade matrix

Upgrade from	Upgrade to
VCS 5.1	VCS 6.0.2
VCS 5.1SPx	VCS 6.0.2
VCS 5.1SP1RP1	VCS 6.0.2
VCS 5.1SP1RP2	VCS 6.0.2
VCS 5.1SP1RP3	VCS 6.0.2
VCS 6.0	VCS 6.0.2
VCS 6.0RP1	VCS 6.0.2
VCS 6.0.1	VCS 6.0.2

Configuring single sign-on between the virtual machine and the Symantec High Availability Console

SSO configuration involves specifying the virtual machine administrator account to set up a permanent authentication for the virtual machine.

You need to manually configure SSO, if you have installed the guest components using the product installer or CLI. The Guest Components installer launched using the vSphere Client menu configures SSO after the guest components installation is complete.

Use the Symantec High Availability tab to configure the single sign-on between the virtual machine and the Console host.

Note: Symantec High Availability solution uses platform-based authentication; it does not store user passwords.

The Symantec High Availability Console uses the Authentication service to provide secure communications between the virtual machine and the Console. It uses digital certificates for authentication and uses SSL to encrypt communications.

This single sign-on authentication is required for all operations on the virtual machine. This is also required so that the server does not prompt you for a user name and password each time you log on to the vSphere Client and click on a virtual machine to view its status.

Perform the following steps to configure the single sign-on for the virtual machines.

To configure single sign-on for the virtual machines

1. Launch the vSphere Client and connect to the vCenter Server used to manage your virtual machines.
2. On the Security Warning dialog that displays information about the Symantec High Availability Console certificate, do the following:
   - Check the option to install the certificate.
   - Click **Ignore**.

   If you do not install the Symantec High Availability Console certificate, this dialog pops up each time you log on to the vCenter Server using the vSphere Client.
3. Open the Hosts and Clusters view in the vSphere Client and then expand the Cluster to display the list of virtual machines.
4. From the left pane select the virtual machine to configure the SSO and then in the right pane select the **Symantec High Availability** tab.
5. Click **Yes** on the security certificate related dialog box, if displayed.
6. In the User Name and Password field, specify the credentials of a user that has administrative privileges on the virtual machine.
7. Click **Configure**.

   The Symantec High Availability Console uses the specified user account to set up a permanent authentication for the virtual machine.

   After the authentication is successful, the Symantec High Availability tab refreshes and displays the application configuration view.

   Note: If you experience an error, "Error occurred during deployment of the ApplicationHA guest credential", you must repair the Console installation and then try to configure the single sign-on again.

   ---

8. Repeat these steps for all virtual machines where you wish to configure application monitoring.

Managing the licenses for Symantec High Availability solution

You can update the licenses by adding or removing specific license keys on the systems where you have installed the Symantec High Availability guest components.

Use any of the following methods to manage the licenses:

- Connect to the vCenter Server and navigate to **Home** > **Solutions and Application** > **Symantec High Availability**.
  Use this method to manage licenses for local and remote virtual machines.
  See "Managing the licenses through vSphere Client menu" on page 30.
- From the command line, to remove a license key, navigate to the directory `/etc/vx/licenses/lic` and run the command **`# rm license key`**
  To add a license, run the command **`vxlicinst`**, and specify the license key.

For more details refer to the product installation and upgrade guide.

Managing the licenses through vSphere Client menu

Perform the following steps to manage the licenses through vSphere Client menu. You can manage the licenses on local and remote virtual machines.

To manage the licenses

1. Connect to the vCenter Server and navigate to **Home** > **Solutions and Applications** > **Symantec High Availability**
2. Click the **License Management** tab.
3. Select the desired virtual machines and click **Next**.

   Only the machines that are running can be selected.
4. Select a virtual machine and click **Add License**.

   Use the **CTRL** key to select multiple virtual machines.
5. On the Add License panel, enter the license key in the **New License Key** text box and click **Validate Key**.

   The installer validates the license key. For successful validation the status reflects **New license applied**. In case of validation failure, the status is reflects **Validation Failed. Enter a valid license key**. Click **Ok**.
6. Click **Apply**.

The specified license keys take effect immediately.

To view the details of the existing licenses, select the individual virtual machine. The details are displayed in the **Existing License Details** table.

Chapter 3

Administering application availability

This chapter includes the following topics:

Administering application monitoring using the Symantec High Availability tab

Veritas Cluster Server provides you with an interface, the Symantec High Availability tab, to configure and control application monitoring. The Symantec High Availability tab is integrated with the VMware vSphere Client.

Note: You can administer application monitoring in two ways. One, using the Symantec High Availability tab as described below, and two, using the Symantec High Availability dashboard. Using the Symantec High Availability dashboard, you can administer application monitoring for multiple applications on multiple systems in a data center. For more information on the latter:

See "Administering application availability using Symantec High Availability dashboard" on page 49.

Use the Symantec High Availability tab to perform the following tasks:

- To configure and unconfigure application monitoring

- To unconfigure the VCS cluster
- To start and stop configured applications
- To add and remove failover systems
- To enter and exit maintenance mode
- To switch an application
- To determine the state of an application (components)
- To resolve a held-up operation
- To modify application monitoring settings
- To view application dependency
- To view component dependency

To view the Symantec High Availability tab, launch the VMware vSphere Client, select a system from the inventory and then click the **Symantec High Availability** tab.

If you have not configured single sign-on for the system, specify the user credentials of a user that has administrative privileges on the system.

Note: You can also perform the application monitoring operations directly from a browser window using the following URL:
https://*<VMNameorIP>*:5634/vcs/admin/application_health.html?priv=ADMIN
where *<VMNameorIP>* is the virtual machine name or the IP address of the system from where you want to access the tab.

A prompt for user account details will be displayed. You must enter the system user account details.

Understanding the Symantec High Availability tab work area

The Symantec High Availability tab displays the consolidated health information for applications running in a Veritas Cluster Server (VCS) cluster. The cluster may include one or more systems.

When you click a system in the inventory view of the VMware vSphere client, the Symantec High Availability tab displays application information for the entire VCS cluster, not just the selected system.

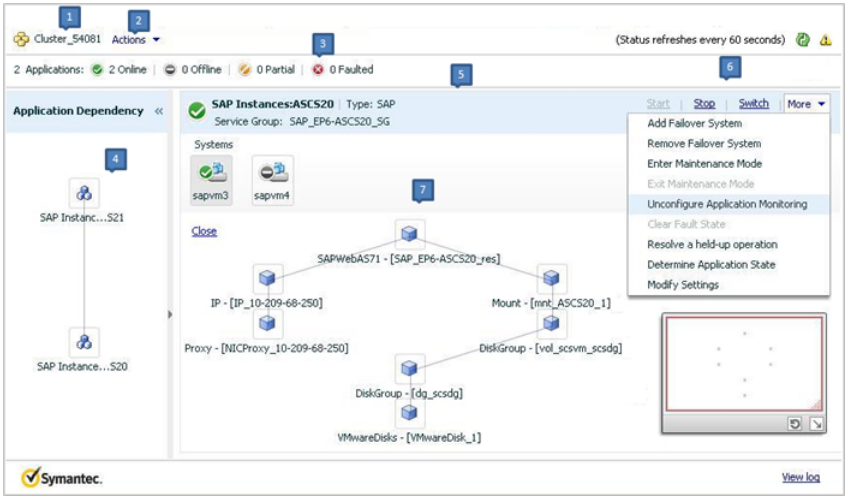
Note: If you do not configure any application for monitoring in the VCS cluster, then the Symantec Application High Availability tab displays only the following link: **Configure an application for high availability**.

The Symantec High Availability tab uses icons, color coding, dependency graphs, and tool tips to report the detailed status of an application.

The Symantec High Availability tab displays complex applications, for example SAP Netweaver, in terms of multiple interdependent instances of that application. These interdependent instances represent component groups of the application. The component groups are also known as "service groups" in VCS terminology.

Each service group in turn includes several critical components of the application. The components are known as "resources" in VCS terminology.

The following figure displays two instances of SAP running in the Symantec High Availability tab:



1. Title bar

2. Actions menu

3. Aggregate Status Bar

4. Application dependency graph

5.Application table

6. Application-specific task menu

7. Component dependency graph

The Symantec High Availability tab graphic user interface (GUI) includes the following components:

- Title bar: Displays the name of the VCS cluster, the Actions menu, the Refresh icon, the Alert icon. Note that the Alert icon appears only if the communication between Symantec High Availability Console and the system fails, and the Symantec High Availability tab fails to display the system, or displays stale data.

- Actions menu: Includes a drop-down list of operations that you can perform with effect across the cluster. These include: Configuring an application for high availability; Unconfigure all applications; and Unconfigure VCS cluster.
- Aggregate status bar: Displays a summary of applications running in the cluster. This includes the total number of applications, and the state-wise breakdown of the applications in terms of the Online, Offline, Partial, and Faulted states.
- Application dependency graph: Illustrates the order in which the applications or application instances, must start or stop.

  If an application must start first for another application to successfully start, the former application appears at a lower level. A line connects the two applications to indicate the dependency. If no such dependency exists, all applications appear in a single horizontal line.
- Application table: Displays a list of all applications configured in the VCS cluster that is associated with the system you selected in the inventory view of the vSphere Client GUI.

  Each application is listed in a separate row. Each row displays the systems where the application is configured for monitoring.

  The title bar of each row displays the following entities to identify the application or application instance (service group):
  - Display name of the application (for example, Payroll application)
  - Type of application (for example, Custom)
  - Service group name
- Application-specific task menu: Appears in each application-specific row of the application table. The menu includes application-specific tasks such as Start, Stop, Switch, and a dropdown list of more tasks. The More dropdown list includes tasks such as Add a failover system, and Remove a failover system.
- Component dependency graph: Illustrates the order in which application components (resources) must start or stop for the related application or application instance to respectively start or stop. The component dependency graph by default does not appear in the application table. To view the component dependency graph for an application, you must click a system on which the application is running.

  The track pad, at the right-bottom corner helps you navigate through complex component dependency graphs.

  If you do not want to view the component dependency graph, in the top left corner of the application row, click **Close**.

To view the status of configured applications

In the application dependency graph, click the application for which you want to view the status. If the appropriate row is not already visible, the application table automatically scrolls to the appropriate row. The row displays the state of the application for each configured failover system in the cluster for that application.

If you click any system in the row, a component dependency graph appears. The graph uses symbols, color code, and tool tips to display the health of each application component. Roll the mouse over a system or component to see its health details.

The health of each application/application component on the selected system is displayed in terms of the following states:

Table 3-1 Application states

State	Description
Online	Indicates that the configured application or application components are running on the virtual machine. If the application is offline on at least one other failover system, an alert appears next to the application name.
Offline	Indicates that the configured application or its components are not running on the virtual machine.
Partial	Indicates that either the application or its components are being started on the virtual machine or Veritas Cluster Server was unable to start one or more of the configured components If the application is offline on at least one other failover system, an alert appears next to the application name.
Faulted	Indicates that the configured application or its components have unexpectedly stopped running.

To configure or unconfigure application monitoring

Use the Symantec High Availability tab to configure or unconfigure an application for monitoring in a cluster under Veritas Cluster Server (VCS) control.

The tab provides you with specific links to perform the following configuration tasks:

- Configure the first application for monitoring in a VCS cluster:
  If you have not configured any application for monitoring in the cluster, the Symantec High Availability tab appears blank except for the link **Configure an application for high availability**.

Click the link to launch the Symantec High Availability Application Monitoring Configuration Wizard. Use the wizard to configure application monitoring.

- Add an application to the existing application monitoring configuration:
  Click **Actions** > **Configuration application for high availability** to launch the Symantec High Availability Application Monitoring Configuration Wizard. Use the wizard to configure application monitoring.
- Unconfigure monitoring of an application:
  In the appropriate row of the application table, click **More** > **Unconfigure Application Monitoring** to delete the application monitoring configuration from the VCS.
  Note that this step does not remove VCS from the system or the cluster, this step only removes the monitoring configuration for that application.
  Also, to unconfigure monitoring for an application, you can perform one of the following procedures: unconfigure monitoring of all applications, or unconfigure VCS cluster.
- Unconfigure monitoring of all applications:
  Click **Actions** > **Unconfigure all applications**. This step deletes the monitoring configuration for all applications configured in the cluster.
- Unconfigure VCS cluster:
  Click **Actions** > **Unconfigure VCS cluster**. This step stops the VCS cluster, removes VCS cluster configuration, and unconfigures application monitoring.

To start or stop applications

Use the following options on the Symantec High Availability tab to control the status of the configured application and the associated components or component groups (application instances).

Note that the **Start** and **Stop** links are dimmed in the following cases:

- If you have not configured any associated components or component groups (resources or service groups) for monitoring
- If the application is in maintenance mode
- If no system exists in the cluster, where the application is not already started or stopped as required.

To start an application

1 In the appropriate row of the application table, click **Start**.

2 If the application (service group) is of the failover type, on the Start Application panel, click **Any system**. VCS uses pre-defined policies to decide the system where to start the application.

If the application (service group) is of the parallel type, on the Start Application panel, click **All systems**. VCS starts the application on all required systems, where the service group is configured.

Note: Based on service group type, either the Any system or the All Systems link automatically appears.

To learn more about policies, and parallel and failover service groups, see the *VCS Administrator's Guide*.

If you want to specify the system where you want to start the application, click **User selected system**, and then click the appropriate system.

3 If the application that you want to start requires other applications or component groups (service groups) to start in a specific order, then check the **Start the dependent components in order** check box, and then click **OK**.

To stop an application

1 In the appropriate row of the application table, click **Stop**.

2 If the application (service group) is of the failover type, in the Stop Application Panel, click **Any system**. VCS selects the appropriate system to stop the application.

If the application (service group) is of the parallel type, in the Stop Application Panel click **All systems**. VCS stops the application on all configured systems.

Note: Based on service group type, either the Any system or the All Systems link automatically appears.

To learn more about parallel and failover service groups, see the *VCS Administrator's Guide*.

If you want to specify the system, where you want to stop the application, click **User selected system**, and then click the appropriate system.

3 If the application that you want to stop requires other applications or component groups (service groups) to stop in a specific order, then check the **Stop the dependent components in order** check box, and then click **OK**.

To switch an application to another system

If you want to gracefully stop an application on one system and start it on another system in the same cluster, you must use the Switch link. You can switch the application only to a system where it is not running.

Note that the Switch link is dimmed in the following cases:

- If you have not configured any application components for monitoring
- If you have not specified any failover system for the selected application
- If the application is in maintenance mode
- If no system exists in the cluster, where the application can be switched
- If the application is not in online/partial state on even a single system in the cluster

To switch an application

1. In the appropriate row of the application table, click **Switch**.
2. If you want VCS to decide to which system the application must switch, based on policies, then in the Switch Application panel, click **Any system**, and then click **OK**.

   To learn more about policies, see the *VCS Administrator's Guide*.

   If you want to specify the system where you want to switch the application, click **User selected system**, and then click the appropriate system, and then click **OK**.

   Veritas Cluster Server stops the application on the system where the application is running, and starts it on the system you specified.

To add or remove a failover system

Each row in the application table displays the status of an application on systems that are part of a VCS cluster in a VMware environment. The displayed system/s either form a single-system Veritas Cluster Server (VCS) cluster with application restart configured as a high-availability measure, or a multi-system VCS cluster with application failover configured. In the displayed cluster, you can add a new system as a failover system for the configured application.

The system must fulfill the following conditions:

- Veritas Cluster Server 6.0.2 is installed on the system.
- The system is not part of any other VCS cluster.
- The system has at least two network adapters.

- The host name of the system must be resolvable through the DNS server or, locally, using `/etc/hosts` file entries.
- The required ports are not blocked by a firewall.
- The application is installed identically on all the systems, including the proposed new system.

To add a failover system, perform the following steps:

Note: The following procedure describes generic steps to add a failover system. The wizard automatically populates values for initially configured systems in some fields. These values are not editable.

To add a failover system

1. In the appropriate row of the application table, click **More** > **Add Failover System**.
2. Review the instructions on the welcome page of the Symantec High Availability Configuration Wizard, and click **Next**.

3 If you want to add a system from the Cluster systems list to the Application failover targets list, on the Configuration Inputs panel, select the system in the Cluster systems list. Use the Edit icon to specify an administrative user account on the virtual machine. You can then move the required system from the Cluster system list to the Application failover targets list. Use the up and down arrow keys to set the order of systems in which VCS agent must failover applications.

If you want to specify a failover system that is not an existing cluster node, on the Configuration Inputs panel, click **Add System**, and in the Add System dialog box, specify the following details:

System Name or IP address	Specify the name or IP address of the system that you want to add to the VCS cluster.
User name	Specify the user name with administrative privileges on the system. If you want to specify the same user account on all systems that you want to add, check the **Use the specified user account on all systems** box.
Password	Specify the password for the account you specified.
Use the specified user account on all systems	Click this check box to use the specified user credentials on all the cluster systems.

The wizard validates the details, and the system then appears in the Application failover target list.

4 If you are adding a failover system from the existing VCS cluster, the Network Details panel does not appear.

If you are adding a new failover system to the existing cluster, on the Network Details panel, review the networking parameters used by existing failover systems. Appropriately modify the following parameters for the new failover system.

Note: The wizard automatically populates the networking protocol (UDP or Ethernet) used by the existing failover systems for Low Latency Transport communication. You cannot modify these settings.

- To configure links over ethernet, select the adapter for each network communication link. You must select a different network adapter for each communication link.

- To configure links over UDP, specify the required details for each communication link.

Network Adapter	Select a network adapter for the communication links. You must select a different network adapter for each communication link. Symantec recommends that one of the network adapters must be a public adapter and the VCS cluster communication link using this adapter is assigned a low priority. **Note:** Do not select the teamed network adapter or the independently listed adapters that are a part of teamed NIC.
IP Address	Select the IP address to be used for cluster communication over the specified UDP port.
Port	Specify a unique port number for each link. You can use ports in the range 49152 to 65535. The specified port for a link is used for all the cluster systems on that link.
Subnet mask	Displays the subnet mask to which the specified IP belongs.

5 If a virtual IP is not configured as part of your application monitoring configuration, the Virtual Network Details page is not displayed. Else, on the Virtual Network Details panel, review the following networking parameters that the failover system must use, and specify the NIC:

Virtual IP address	Specifies a unique virtual IP address.
Subnet mask	Specifies the subnet mask to which the IP address belongs.
NIC	For each newly added system, specify the network adaptor that must host the specified virtual IP.

6 If the newly added failover system is associated with a different ESX host as compared to other systems, then on Target ESX Details page, specify the ESX host of the newly added failover system. Also specify the administrative user account details associated with the ESX host.

Note: If the application for which you are adding a failover system does not use storage attached directly to the ESX host, the wizard does not display this page.

If the new failover system runs on a different ESX host, or is configured to failover to another ESX host, specify that ESX host. To specify the ESX host, click **Add ESX Host** and on the Add ESX Host dialogue box, specify the following details, and then click **Next**:

ESX hostname or IP address	Specify the target ESX hostname or IP address. The virtual machines can fail over to this ESX host during vMotion. Specify an ESX host that has the same mount points as those currently used by the application.
User name	Specify a user account for the ESX host. The user account must have administrator privileges on the specified ESX host.
Password	Specify the password associated with the user name you specified.

The wizard validates the user account and the storage details on the specified ESX host, and uses this account to move data disks during vMotion.

7 On the Configuration Summary panel, review the VCS cluster configuration summary, and then click **Next** to proceed with the configuration.

8 On the Implementation panel, the wizard adds the specified system to the VCS cluster, if it is not already a part. It then adds the system to the list of failover targets. The wizard displays a progress report of each task.

- If the wizard displays an error, click **View Logs** to review the error description, troubleshoot the error, and re-run the wizard from the Symantec High Availability tab.
- Click **Next**.

9 On the Finish panel, click **Finish**. This completes the procedure for adding a failover system. You can view the system in the appropriate row of the application table.

Similarly you can also remove a system from the list of application failover targets.

Note: You cannot remove a failover system if an application is online or partially online on the system.

To remove a failover system

1. In the appropriate row of the application table, click **More** > **Remove Failover System**.
2. On the Remove Failover System panel, click the system that you want to remove from the monitoring configuration, and then click **OK**.

Note: This procedure only removes the system from the list of failover target systems, not from the VCS cluster. To remove a system from the cluster, use VCS commands. For details, see the *Veritas Cluster Server Administrator's Guide*.

To suspend or resume application monitoring

After configuring application monitoring you may want to perform routine maintenance tasks on those applications. These tasks may or may not involve stopping the application but may temporarily affect the state of the applications and its dependent components. If there is any change to the application status, Veritas Cluster Server (VCS) may try to restore the application state. This may potentially affect the maintenance tasks that you intend to perform on those applications.

If stopping the application is not an option, you can suspend application monitoring and create a window for performing such maintenance tasks. When application monitoring is suspended, VCS freezes the application configuration.

The **Enter Maintenance Mode** link is automatically dimmed if the application is already in maintenance mode. Conversely, if the application is not in maintenance mode, the **Exit Maintenance Mode** link is dimmed.

The Symantec High Availability tab provides the following options:

To enter maintenance mode

1 In the appropriate row, click **More**> **Enter Maintenance Mode**.

During the time the monitoring is suspended, Symantec high availability solutions do not monitor the state of the application and its dependent components. The Symantec High Availability tab does not display the current status of the application. If there is any failure in the application or its components, VCS takes no action.

2 While in maintenance mode, if a virtual machine restarts, if you want application monitoring to remain in maintenance mode, then in the Enter Maintenance Mode panel, check the **Suspend the application availability even after reboot** check box, and then click **OK** to enter maintenance mode.

To exit the maintenance mode

1 In the appropriate row, click **More**> **Exit Maintenance Mode**, and then click **OK** to exit maintenance mode.

2 Click the Refresh icon in the top right corner of the Symantec High Availability tab, to confirm that the application is no longer in maintenance mode.

To clear Fault state

When you fix an application fault on a system, you must further clear the application Faulted state on that system. Unless you clear the Faulted state, VCS cannot failover the application on that system.

You can use the Symantec High Availability tab to clear this faulted state at the level of a configured application component (resource).

The Clear Fault link is automatically dimmed if there is no faulted system in the cluster.

To clear Fault state

1 In the appropriate row of the application table, click **More** > **Clear Fault state**.

2 In the Clear Fault State panel, click the system where you want to clear the Faulted status of a component, and then click **OK**.

To resolve a held-up operation

When you try to start or stop an application, in some cases, the start or stop operation may get held-up mid course. This may be due to VCS detecting an incorrect internal state of an application component. You can resolve this issue by using the resolve a held-up operation link. When you click the link, VCS appropriately resets the internal state of any held-up application component.

This process prepares the ground for you to retry the original start or stop operation, or initiate another operation.

To resolve a held-up operation

1. In the appropriate row of the application table, click **More** > **Resolve a held-up operation**.
2. In the Resolve a held-up operation panel, click the system where you want to resolve the held-up operation, and then click **OK**.

To determine application state

The Symantec High Availability tab displays the consolidated health information of all applications configured for monitoring in a VCS cluster. The tab automatically refreshes the application health information every 60 seconds.

If you do not want to wait for the automatic refresh, you can instantaneously determine the state of an application by performing the following steps:

To determine application state

1. In the appropriate row of the Application table, click **More** > **Determine Application State**.
2. In the Determine Application State panel, select a system and then click **OK**.

Note: You can also select multiple systems, and then click **OK**.

To remove all monitoring configurations

To discontinue all existing application monitoring in a VCS cluster, perform the following step:

- On the Symantec High Availability tab, in the Title bar, click **Actions** > **Unconfigure all applications**. When a confirmation message appears, click **OK**.

To remove VCS cluster configurations

If you want to create a different VCS cluster, say with new systems, a different LLT protocol, or secure communication mode, you may want to remove existing VCS cluster configurations. To remove VCS cluster configurations, perform the following steps:

Note: The following steps deletes all cluster configurations, (including networking and storage configurations), as well as application-monitoring configurations.

- On the Title bar of the Symantec High Availability tab, click **Actions >Unconfigure VCS cluster**.
- In the Unconfigure VCS Cluster panel, review the Cluster Name and Cluster ID, and specify the User name and Password of the Cluster administrator, and then click **OK**.

Administering application monitoring settings

The Symantec High Availability tab lets you define and modify settings that control application monitoring with Veritas Cluster Server (VCS). You can define the settings on a per application basis. The settings apply to all systems in a VCS cluster, where that particular application is configured for monitoring.

The following settings are available:

- **App.StartStopTimeout**: When you click the **Start Application** or **Stop Application**, or **Switch Application** links in the Symantec High Availability tab, VCS initiates an application start or stop, respectively. This option defines the number of seconds that VCS must wait for the application to start or stop, after initiating the operation. You can set a value between 0 and 300 seconds for this attribute; the default value is 30 seconds.

  If the application does not respond in the stipulated time, the tab displays an alert. The alert states that the operation may take some more time to complete and that you must check the status after some time. A delay in the application response does not indicate that the application or its dependent component has faulted. Parameters such as workload, system performance, and network bandwidth may affect the application response. VCS continues to wait for the application response even after the timeout interval elapses.

  If the application fails to start or stop, VCS takes the necessary action depending on the other configured remedial actions.
- **App.RestartAttempts**: This setting defines the number of times that VCS must try to restart a failed application. The value of App.RestartAttempts may vary between 0 and 5; the default value is 0. If an application fails to start within the specified number of attempts, VCS fails over the application to a configured failover system.
- **App.DisplayName**: This setting lets you specify an easy-to-use display name for a configured application. For example, Payroll Application. VCS may internally use a different application name to uniquely identify the application.

However, the internal string, for example OraSG2, may not be intuitive to understand, or easy to recognize while navigating the application table. Moreover, once configured, you cannot edit the application name, while you can modify the application display name as required. Note that the Symantec High Availability tab displays both the application display name and the application name.

Administering application availability using Symantec High Availability dashboard

The Symantec High Availability Dashboard is a consolidated graphic user interface that lets you administer application monitoring on systems in a VMware vCenter-administered data center.

The dashboard is fully integrated with the VMware vSphere Client GUI. The dashboard appears in the Symantec High Availability tab of the VMware vSphere Client GUI. To view the dashboard, select a data center or an ESX cluster in the inventory, and then click the Symantec High Availability tab.

Note: To administer application availability using the dashboard, single sign-on between the system and Symantec High Availability Console must be configured. Also, the application-specific agent must be appropriately configured.

For more information, see the *Symantec High Availability Solution Guide for VMware*.

On the dashboard, you can view the aggregate health statistics for monitored applications across a data center. You can also drill down to an ESX cluster and view monitored applications running in that cluster.

To understand how to navigate across the dashboard:

See "Understanding the dashboard work area" on page 50.

You can drill down to an individual application and perform the following administrative actions:

- Start application
- Stop application
- Enter maintenance mode
- Exit maintenance mode
- Switch application (to another system)

Apart from applications on systems running Veritas Cluster Server, the Symantec High Availability Dashboard also displays applications running on Symantec ApplicationHA guests (versions 6.0 and 5.1 SP2).

For more information on monitoring applications running on Symantec ApplicationHA guests:

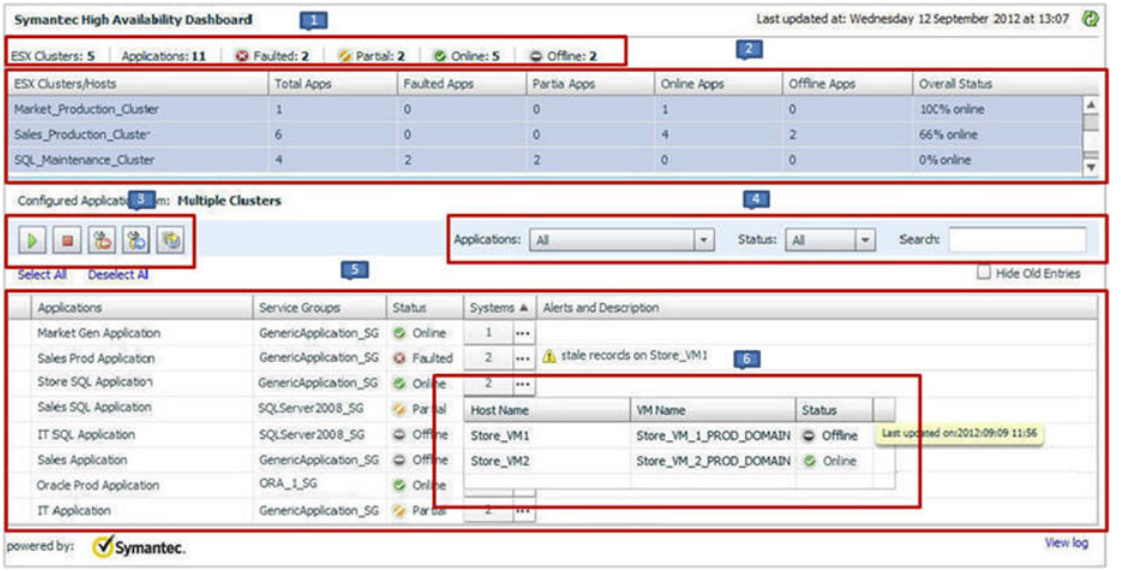
See "Monitoring applications running on Symantec ApplicationHA guests" on page 55.

Understanding the dashboard work area

The Symantec High Availability dashboard displays the aggregate application health status information for a datacenter or an ESX cluster.

Depending on whether you click a datacenter or a VMware cluster in the inventory view (left pane) of the VMware vSphere Client GUI, the dashboard displays the aggregate application status information. Apart from the application table described in detail below, the dashboard uses color code and tool tips to indicate the status of an application.

The following figure illustrates the dashboard work area. Note that the red boxes highlight the key GUI elements:



In the above figure, the labels stand for the following elements of the dashboard

1	Aggregate status bar	**2**	ESX cluster/host table	**3**	Taskbar
4	Filters menu	**5**	Application table	**6**	Systems table (dropdown)

Aggregate status bar

The aggregate status bar of the dashboard displays the following details:

- Number of ESX clusters that have applications configured for monitoring with VCS
- Number of configured applications in the selected data center
- Number of faulted applications
- Number of applications in partial state
- Number of online applications
- Number of offline applications

ESX cluster/host table

The Symantec High Availability dashboard displays this table only if you click a datacenter in the inventory view of the vSphere Client, and then click the Symantec High Availability tab.

The cluster table lists the following statistics per ESX cluster (or independent ESX host) in the data center:

- Number of configured applications
- Number of faulted applications
- Number of applications in partial state
- Number of online applications
- Number of offline applications
- Overall status (percentage of healthy applications)

If you click a row in the ESX cluster/host table, the application table of the dashboard displays monitored applications running on systems hosted by the selected ESX cluster or ESX host (an ESX server that is not part of an ESX cluster).

Note: This is the only method to navigate to applications running on systems hosted by standalone ESX hosts, by using the Symantec High Availability dashboard.

Taskbar

The taskbar displays icons for various administrative tasks. A tool tip highlights the task that each icon represents.

The dashboard supports the following tasks:

- Start Application: Starts a configured application
- Stop Application: Stops a configured application
- Enter Maintenance Mode: Suspends application monitoring of the configured application. In maintenance mode, VCS does not monitor the state of the application, and its dependent components.
- Exit Maintenance Mode: Resumes application monitoring for a configured application.
- Switch Application: Switches and an application gracefully from one system to another.

Filters menu

The filters menu lets you dynamically filter the applications that are displayed in the applications table. You can filter the applications by the following parameters:

- Application name
- Application status
- Search (by a string)

Application table

If you click an ESX cluster in the ESX cluster/host table, or in the inventory view of the VMware vSphere Client, then the list of applications running in that ESX cluster appears in the application table of the dashboard.

If you click an ESX host (an ESX server that is not part of an ESX cluster) in the ESX cluster/host table, then the list of applications that are configured on systems hosted by that ESX server appears. Note that this is the only route to navigate to such applications through the dashboard

The following table lists each column in the application table and its description:

Column	Description
Applications	Indicates the application name.

Column	Description
Service Groups	Indicates the group of critical application components that VCS uses to determine the health of a monitored application. Service group is a VCS term. The equivalent term in Symantec ApplicationHA terminology is “component group”. VCS may use more than one service group to monitor a complex application. The dashboard displays each service group of such an application as a separate instance of that application.
Status	This column indicates the effective status of an application in a VCS cluster. It does not indicate the state of the application on per member system. For example, in a two-system cluster, if the application has faulted on one system but has failed over to another system, then this column states the state of the application as Online. Indicates one of the following states of an application: ■ Online ■ Offline ■ Faulted ■ Partial **Note:** After you perform an administrative task such as starting or stopping an application, or entering or exiting maintenance mode, it takes a few seconds for the dashboard to reflect the revised status of the configured application.
Systems	Indicates the number of systems where the application is configured for monitoring. To view more information about all such systems, click the **(...)** icon. The System table (dropdown) appears, listing the ESX host name of each configured system, the VM name (system name), and the status of the application on each system.
Alerts and description	Displays a triangular alert icon **(!)** and describes the reason for the alert. This column displays alerts in two cases: a) If the application status record is stale; b) If the application has faulted on a system. For stale records, the column includes the timestamp of the last received health record. In case of application fault, the column provides details of the system where the fault occurred.

Accessing the dashboard

You can use the Symantec High Availability dashboard to perform one of the following actions:

- Identify all instances and failover systems of one or more applications running in a data center
- Drill down to a specific application, and perform an administrative action on the application
- View alerts for faulted applications and stale application health reports

Prerequisites for accessing the dashboard

Before you access the Symantec High Availability dashboard to administer an application, ensure:

- Single sign-on is configured between the Symantec High Availability Console and the systems hosting the monitored applications
- Symantec High Availability Console is able to communicate with Symantec High Availability guest components on designated port (port 5634).
- The application that you want to administer is configured for application monitoring with Symantec High Availability

How to access the dashboard

When you install Symantec High Availability guest components, the product installation script or wizard automatically installs the required dashboard components. As a result, the Symantec High Availability Dashboard appears in the **Symantec High Availability** tab of the vSphere Client.

You must, however, ensure that Symantec High Availability is successfully installed and that you have adequate user privileges to access the dashboard.

To access dashboard

Perform the following step:

- In the inventory view (left pane) of the vSphere Client, click a datacenter or a VMware cluster. In the right pane, to view the Symantec High Availability dashboard, click the Symantec High Availability tab.

Who can access the dashboard

To access High Availability dashboard, the VMware vCenter administrator must assign one the following roles to you:

- Guest: View application state
- Operator: View application state and perform administrative actions

- Admin: View application state and perform administrative actions. You can also configure application availability monitoring in this role, but not from the dashboard.

For more information on roles and privileges:

See "About the roles and privileges assigned" on page 61.

Monitoring applications across a data center

If you click a data center in the inventory view of the VMware vSphere Client, and then click the Symantec High Availability tab, the dashboard appears, displaying the aggregate health information of applications running inside various ESX clusters.

You can use filters to drill down from all applications running across the data center and view a single application and its various instances in the data center.

Monitoring applications across an ESX cluster

If you click an ESX cluster in the inventory view of the VMware vSphere Client, and then click the tab, the dashboard displays the consolidated information on the systems and applications running in the ESX cluster. The dashboard also displays the application health and application monitoring information.

You can use filters to drill down from all applications running in the ESX cluster, to view a single application and its various instances in the ESX cluster.

Monitoring applications running on Symantec ApplicationHA guests

Symantec High Availability dashboard displays applications running on Symantec ApplicationHA guests as well as those running on Veritas Cluster Server systems. The dashboard presents a unified view of monitored applications on the two types of systems in a data center.

For easy application monitoring, the dashboard displays an application-centric view, not a product-centric view. You cannot therefore always determine which application is under the control of which Symantec High Availability product.

However, you can conclude that applications configured for failover are under VCS control. Applications configured for monitoring without a failover system may either be under VCS control or under ApplicationHA control.

Searching for application instances by using filters

The High Availability dashboard lets you search for all instances of a particular application in the selected datacenter or an ESX cluster. Various filters enable to

search for the application that you want to monitor. You can use multiple filters simultaneously to search for an application.

The following table lists each field in the filter menu and its description:

Field	Description
Application	Lets you specify the name of the application that you want to filter in the application table. A drop-down list displays all the applications that are configured in the datacenter or ESX cluster. Click to select the name of the application that you want to filter.
Status	Lets you specify the status of the application by which you want to filter the application table. A drop-down list displays the following status values: Online, Offline, Faulted, and Partial.
Search	Lets you search for an application by using a string or pattern of characters. Enter the string using which you want to filter applications. As you enter the string in the Search box, the dashboard dynamically filters the applications. **Note:** The dashboard searches for the specified string in the Systems column.

Selecting multiple applications for batch operations

You can select one or more instances of an application for administering by using the dashboard as follows:

- To select one application instance, click inside the row of that application instance.
- To select various instances, keep the **Control** key pressed and then click inside the row of each instance.
- To select a batch of consecutive entries in the application table, keep the **Shift** key pressed, click inside the row of the first instance, and then click inside the row of the last instance. Alternatively, you can keep the **Shift** key pressed and drag the mouse to mark a block of consecutive entries.
- To select all instances in the application table, click **Select All**.

Starting an application using the dashboard

To start an application, perform the following steps in the application table of the dashboard.

To start an application

1. Filter the applications that you want to start.

   See "Searching for application instances by using filters" on page 55.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to perform a batch operation.

   See "Selecting multiple applications for batch operations" on page 56.
3. To start the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).
4. In the Start Application panel, click the systems where you want to start the application. Note that you can start the application on any of the systems displayed for each application.

   Click **OK**.

Stopping an application by using the dashboard

To stop an application on one or more virtual machines, perform the following steps in the application table of the High Availability dashboard.

To stop an application

1. Filter the applications that you want to stop.

   See "Searching for application instances by using filters" on page 55.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to perform a batch operation.

   See "Selecting multiple applications for batch operations" on page 56.
3. To stop the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).
4. In the Stop Application panel, from the dropdown list, click the systems where you want to stop the application.

   Click **OK**.

Entering an application into maintenance mode

You may need to intentionally take an application offline for maintenance purposes, without triggering a corrective response from Veritas Cluster Server (VCS).

To enter an application into maintenance mode, perform the following steps in the application table of the High Availability dashboard.

Note: The maintenance mode configuration is application-specific, not system-specific.

To enter maintenance mode

1. Filter the application that you want to gracefully take offline for maintenance.

   See "Searching for application instances by using filters" on page 55.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to perform a batch operation.

   See "Selecting multiple applications for batch operations" on page 56.
3. To enter maintenance mode, in the taskbar, click the appropriate icon for entering maintenance mode (use the tool tip to recognize the appropriate icon).
4. If a system restarts while the application is in maintenance mode, and you want the application to remain in maintenance mode, then in the Enter Maintenance Mode panel, check the **Suspend the application availability even after reboot**.
5. On the Enter Maintenance Mode panel, click **OK**.

Bringing an application out of maintenance mode

To bring an application out of maintenance mode on one or more systems, perform the following steps in the application table of the High Availability dashboard.

To exit maintenance mode

1. Filter the applications that you want to bring out of maintenance mode.

   See "Searching for application instances by using filters" on page 55.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to bring out of maintenance mode.

   See "Selecting multiple applications for batch operations" on page 56.

3 To bring the applications out of maintenance mode, in the taskbar, click the appropriate icon for exiting maintenance mode (use the tool tip to recognize the appropriate icon).

4 In the Exit Maintenance Mode panel, click **OK**.

Switching an application

To gracefully switch an application from one system to another, perform the following steps in the application table of the dashboard.

Note: You can switch an application only if the application monitoring configuration includes one or more failover systems.

To switch an application

1 Filter the applications that you want to switch to another node.

See "Searching for application instances by using filters" on page 55.

The application table displays all the instances of the filtered applications.

2 If required, select multiple applications or instances to perform a batch operation.

See "Selecting multiple applications for batch operations" on page 56.

3 To switch the applications, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

4 In the Switch Application panel, select the systems where you want to switch the applications, and then click **OK**. Veritas Cluster Server takes the applications offline on the existing systems, and brings them online on the systems that you specified.

Resolving dashboard alerts

The Alerts and Description column in the application table of the High Availability dashboard marks application alerts with the alert **(!)** icon. This occurs in the following cases:

- Stale entries: Stale entries occur either due to a system (virtual machine) issues or connectivity issues. When this occurs, the system fails to send application heartbeats to the dashboard. If the system fails to send the heartbeat for two consecutive heartbeat intervals, the dashboard displays the alert icon.

Note: You can filter stale entries using the **Search** option and searching with the string "stale".

- Application faults: Application faults may occur due to reasons beyond Veritas Cluster Server (VCS) control, such as storage failure. In such cases, you must investigate and appropriately resolve the issue, and then clear the Faulted status of the application. To view only application fault alerts, in the Alerts and Description column, click the **Hide Old Entries** check box.

Note: It is important that you fix application faults, and then clear the Fault status. Else, the VCS cannot fail over applications to the faulted system, and application availability may be compromised. For more information, See "To clear Fault state" on page 46.

Deleting stale records

VCS uses a heartbeat mechanism to monitor the health of a configured application. If a system fails to send two consecutive heartbeats for an application, VCS marks the health status of that application as stale. The Alerts and Description column of the High Availability Dashboard indicates the time elapsed since the last valid health status was recorded.

After troubleshooting the heartbeat failure, you can delete such stale records from the High Availability database.

To delete stale records

1. On the Console host, navigate to the home directory.

   For example:

   ```
   C:\Program Files\Veritas\
   ```

   Where C:\ is the system drive.

2. Run the following command:

   ```
   C:\Program Files\Veritas\VRTSsfmh\bin>perl.exe C:\Program
   Files\Veritas\ApplicationHA
   \bin\delete_stale_records.pl<TimeInterval>
   ```

   Where Time Interval, in minutes, indicates how stale the records must be, for them to be deleted. By default, the script deletes all records that are older than 60 minutes

Appendix A

Roles and privileges

This appendix includes the following topics:

About the roles and privileges assigned

The following set of privileges are available after you install the Symantec High Availability Console. These privileges define the operations that a user can perform on the system. You can create roles and then assign privileges to them or assign privileges to the existing roles that are available in the vSphere environment. Application monitoring operations are enabled or disabled depending on the privileges that are assigned to the vCenter user account. For example, the Admin privilege is required for configuring application monitoring on a system.

vCenter Server administrators can use these privileges to configure access control while monitoring an application.

- View Application State (Guest)
  Can view the application status on the system. The Guest cannot perform any application monitoring operations.
- Control Application Availability (Operator)
  Can perform all the operations that include start and stop configured applications, enable and disable application monitoring, specify the application monitoring configuration settings, enter and exit application maintenance mode, and view the application status.
  The Operator cannot configure or unconfigure application monitoring on the system.
- Configure Application Availability (Admin)

Can perform all operations that include configure and unconfigure application monitoring, start and stop configured applications, enable and disable application monitoring, specify the application monitoring configuration settings, enter and exit application maintenance mode, and view application status.

Assigning customized privileges to VMwareDisks agent

This section describes a procedure exclusively for users who want to assign customized privileges to the VMwareDisks agent on an ESX host, instead of administrative or root user privileges. If you want to assign administrative or root user privileges, skip this section.

The following subsections describe the background and the configuration workflow in detail.

About assigning privileges to VMwareDisks agent

The application monitoring configuration for Veritas Cluster Server (VCS) agents in a VMware virtual environment involves the VMwareDisks agent. In the event of an application failure, the VMwareDisks agent sends a disk-detach request to the ESX host, and then attaches the disk to the failover target system.

To enable the VMwareDisks agent to communicate with the ESX host, during the application monitoring configuration workflow, you must specify an ESX user account. The specified ESX user account must have administrative privileges, or should be a root user. If the ESX user account does not have these privileges, you must create a role, add certain privileges to the created role, and then assign the role to the ESX user account.

If you do not want to assign the role to an existing ESX user account, you can create a new ESX user account, and then assign the role. You can further integrate the new ESX user account with an Active Directory-based authentication service if available in the VMware environment. The VMwareDisks agent can then use

the same user account to perform its tasks on all ESX hosts linked to the Active Directory.

Creating a role with customized privileges for VMwareDisks agent

This section provides the steps to create a role with adequate privileges that the VMwareDisks agent can use in an ESX cluster. The assigned privileges do not include administrative or root user privileges:

To create a role

1. Using the VMware vSphere Client, log on to the ESX host, and navigate to **Home** > **Administration** > **Roles**.
2. Click **Add Role**.
3. On the Add New Role panel, specify a name for the new role. For example, "VMwareDisks Resources Manager".
4. To select privileges for the VMwareDisks Resources Manager role, in the Privileges tree, click the following check boxes.
   - **All Privileges** > **Datastore** > **Low level file operations**.
   - **All Privileges** > **Virtual Machine** > **Configuration** > **Adding existing disk**.
   - **All Privileges** > **Virtual Machine** > **Change resource**.
   - **All Privileges** > **Virtual Machine** > **Configuration** > **Remove disk**.
5. Click **OK**.

Creating an ESX user account

If you want to assign the role that you created in the section Creating a role with customized privileges for VMwareDisks agent, to an existing user, skip this section. Proceed to the section Assigning a role to an ESX user account.

If you want to create a new user account to assign the new role to, perform the steps described in this section:

To add a local ESX user

1. Using the VMware vSphere Client, log on to the ESX host, and navigate to **Home** > **Inventory**.
2. In the left pane, click the ESX host and in the right pane, click **Local Users & Groups**.

   The Users list appears by default.

3 If the Users list is not displayed, to view the Users list, on the View bar, click **Users**.

4 To add a new user, right-click any existing user, and click **Add**.

5 In the **Add New User** panel, specify a Login and Password to define a new user account for configuring VMwareDisks resources.

To confirm the password, retype the password.

To define the new user account, you can also specify a descriptive User Name and user ID (UID). If you do not specify the UID, the vCenter server automatically assigns one.

6 Click **OK**.

Integrating an ESX user account with Active Directory

After you create a new ESX user account for the VMwareDisks agent to communicate with an ESX host, you can optionally integrate the account with any existing Active Directory authentication in your environment. Else, the new ESX user account depends on the local authentication mechanism on the ESX host, and you will need to configure one account per host.

Integrating with an existing Active Directory mechanism helps you leverage the same ESX user account across multiple ESX hosts for VMwareDisks agent configurations.

To integrate with Active Directory

1 Create a domain user in the Active Directory.

2 Using the VMware vSphere Client, log on to the ESX host, and navigate to **Home** > **Inventory**.

3 In the left pane, click the ESX host and in the right pane, click **Configuration**.

4 In the Software panel, click **Authentication Services**.

5 Review the Directory Services Configuration.

If the Directory Service Type is not Active Directory, in the top right corner, click **Properties**.

6 In the Directory Service Configuration panel, from the Select Directory Service Type drop down list, select **Active Directory**.

7 In the Domain Settings area, specify the **Domain**, and click **Join Domain**.

Alternatively, configure vSphere Authentication proxy.

8 Enter the user name and password of a directory service user that has permissions to join the host to the domain, and click **OK**.

Assigning a role to an ESX user account

This section describes the steps to assign a role to an ESX user:

To assign the role to a user

1. Using the VMware vSphere Client, log on to the ESX host, and navigate to **Home** > **Inventory**.
2. In the left pane, click the ESX host and in the right pane, click **Permissions**.
3. In the Permissions tab, right-click the blank space, and click **Add Permission**.
4. In the Assign Permissions panel, click **Add**.
5. In the Users and Groups frame of the Select Users and Groups panel, specify the user(s) that you want to assign the new role for storage management (for example, VMwareDisks Resources Manager).

   Press the **Ctrl** key and click to select multiple users, if required, and then click **Add** and click **OK**.
6. In the Assigned Role drop down list, click the new role (for example, VMwareDisks Resources Manager), and then click **OK**.

Appendix B

Guest component installation parameters

This appendix includes the following topics:

Symantec High Availability guest components installation parameters

This section provides the list of tunable parameters while installing the guest components (VCS), using the vCenter integrated menu.

These parameters are listed in the "appServerConfig.properties" file that is located on the Console host at the following location:

C:\ProgramData\Symantec\ApplicationHA\conf\appServerConfig.properties

Note: After you edit the parameter values, you must restart the Symantec High Availability service.

Table B-1 lists the guest components parameters for which you can customize the default values.

Table B-1 Guest components tunable parameters

Parameter	Description
VIIMaxInstallerThreadCount	Determines the number of virtual machines on which the guest installer package is simultaneously copied. Default value= 4

Table B-1 Guest components tunable parameters *(continued)*

Parameter	Description
VIIPollingInterval	Determines the time interval for polling the installation progress on the virtual machine. Default value = 15 minutes.
VIIQueueTimeout	Determines the time span for which a virtual machine is queued for installation. Default= 120 minutes. If the virtual machine is queued for installation for more than the time period specified in the attribute, a timeout error occurs and the virtual machine is removed from the installation queue.
VIICopyTimeout	Determines the time span for copying the guest installer package to the virtual machine, from the Console host. Default= 45 mins If the time taken to copy the installer package exceeds the time specified in the attribute, a time out error occurs and the installation is aborted.
VIIGuestInstallTimeout	Determines the time taken to complete the guest installation. Default= 45 mins If the time taken for installation exceeds the time specified in the attribute, a time out error occurs and the installation is aborted.

Appendix C

Troubleshooting

This appendix includes the following topics:

Agent logging on virtual machine

Symantec High Availability agents generate log files that are appended by letters. Letter A indicates the first log file, B the second, C the third, and so on.

The agent log components are defined as follows:

- Timestamp: the date and time the message was generated.
- Mnemonic: the string ID that represents the product (for example, VCS).
- Severity: levels include CRITICAL, ERROR, WARNING, NOTICE, and INFO (most to least severe, respectively).
- UMI: a unique message ID.
- Message Text: the actual message generated by the agent.

The agent logs are located in the following location:

`/var/VRTSvcs/log/<agentname>_A.log`

The format of the agent log is as follows:

```
Timestamp (Year/MM/DD) | Mnemonic | Severity | UMI | Agent Type |
Resource Name | Entry point | Message text
```

A typical agent log resembles:

```
2012/08/15 13:34:44 VCS ERROR V-16-2-13067 Thread(4146068336) Agent
is calling clean for resource(MQ1) because the resource became OFFLINE
unexpectedly, on its own.
```

Troubleshooting Symantec High Availability guest components installation and SSO configuration issues

This section lists the common troubleshooting scenarios that you may encounter while or after installing the Symantec High Availability guest components and configuring single sign-on.

Restarting the vCenter Server or its service during the Symantec High Availability guest components installation displays "Error" in vSphere Client tasks

If the vCenter Server or its service happen to fail or restart during the VCS installation, the vSphere Client displays "Error" as the installation status. However, the guest components installation may continue on the virtual machines.

Workaround: After the vCenter Server or its service restarts, click on each of the selected virtual machine and verify if the Symantec High Availability tab appears in the vSphere Client.

Presence of the **Symantec High Availability** tab indicates successful installation of the guest components. However, if the **Symantec High Availability** tab is not present, refer to the Symantec High Availability logs for installation details.

The Symantec High Availability logs are located on the virtual machine at the following locations:

- /opt/INSTALLER/vii_logs
- /opt/INSTALLER/vii_logs_backup
- /opt/VRTS/install/logs

Reverting the system snapshot requires you to cancel the Symantec High Availability guest components installation

If you revert the virtual machine snapshot during the Symantec High Availability guest components installation, the vSphere Client continues to show a stale entry of the installation task and displays the error "There is one entry in Queue for the virtual machine", if you initiate the installation again.

Workaround: Before initiating the installation again, run the following utility to cancel the installation task from the vSphere Client.

```
https://SymantecHighAvailabilityConsole_IP:14152/ac/
CancelGuestInstallation?
VmId=VirtualMachine_ID
&VmUser=UserName&VmPassword=Password
```

Alternatively,

```
https://Console_IP:14152/ac/CancelGuestInstallation?
VmId=VirtualMachine_ID&VmUser=UserName&VmPassword=Password
```

Where, the virtual machine user name and password must be the one specified during the guest installation.

Note: You can also use this utility if you plan to cancel the queued installation task or to cancel the installation tasks that held-up in the same state for a long time.

Reversal to snapshot leads to an IP resource fault

If you capture a VM configuration snapshot while an IP resource is online, and later revert to the snapshot, VCS reports the state of the IP resource as faulted.

When you revert to a virtual machine configuration snapshot , the network connections undergo a restart. The virtual IP plumbed on the virtual machine is unplumbed. As a result, if you have configured the IP resource for monitoring with VCS, then VCS reports the IP resource as faulted. (2879258)

Workaround: Before capturing the VM configuration snapshot, set the value of the App.RestartLimit attribute for the IP resource to 1.

Perform the following steps

1 Make the VM configuration file editable:

```
# haconf -makerw
```

2 Set the value of the App.RestartLimit attribute to 1:

```
# hatype -modify IP RestartLimit 1
```

3 Save the change and make the VM configuration file read-only:

```
# haconf -dump -makero
```

SSO configuration failure

The single sign-on configuration might fail if you are installing the Symantec High Availability guest components on two or more systems simultaneously and one of them is the Console host.

Workaround: Manually configure the single sign-on, using the Symantec High Availability tab on the vCenter Server.

Issues to due disruption of SSO configuration

You may experience the following issues if the SSO configuration between the guest systems and the Console host breaks:

- The guest system may fail to appear in the Symantec Availability Dashboard
- The Symantec Availability Dashboard may display stale entries and application status
- The Symantec High Availability tab prompts for administrator user account details

The SSO configuration breaks if you have changed the Console server IP address after the SSO was configured.

Workaround: Reconfigure SSO for each cluster system.

Powering on a suspended system leads to an IP resource fault

If you suspend a system, and then power on the system , VCS reports the state of the IP resource as faulted.

When you power on a suspended virtual machine, the network connections undergo a restart. The virtual IP plumbed on the virtual machine is unplumbed. As a result,

if you have configured the IP resource for monitoring with VCS, then VCS reports the IP resource as faulted. (2927874)

Workaround: Set the value of the App.RestartLimit attribute for the IP resource to 1 using the following steps

Perform the following steps

1 Make the VM configuration file editable:

```
# haconf -makerw
```

2 Set the value of the App.RestartLimit attribute to 1:

```
# hatype -modify IP RestartLimit 1
```

3 Save the change and make the VM configuration file read-only:

```
# haconf -dump -makero
```

Troubleshooting application monitoring configuration issues

This section lists common troubleshooting scenarios that you may encounter while or after configuring application monitoring.

Symantec High Availability Configuration Wizard displays blank panels

The Symantec High Availability Configuration Wizard may fail to display the wizard panels. The window may appear blank.

Verify that the Symantec ApplicationHA Service is running on the Symantec High Availability Console host and then launch the wizard again.

The Symantec High Availability Configuration wizard displays the "hadiscover is not recognized as an internal or external command" error

While configuring application monitoring the Symantec High Availability Configuration wizard may display the "hadiscover is not recognized as an internal or external command" error, after you click Next on the Application Selection panel.

This issue occurs if you launch the wizard from a system where you have reinstalled the Symantec High Availability guest components.

Workaround: Exit the wizard, restart the Veritas Storage Foundation Messaging Service and then re-run the wizard.

Running the ‘hastop –all’ command detaches virtual disks

The 'hastop –all' command takes offline all the components and components groups of a configured application, and then stops the VCS cluster. In the process, the command detaches the virtual disks from the VCS cluster nodes. (2920101)

Workaround: If you want to stop the VCS cluster (and not the applications running on cluster nodes), instead of the “hastop –all”, use the following command:

```
hastop -all -force
```

This command stops the cluster without affecting the virtual disks attached to the VCS cluster nodes.

Validation may fail when you add a failover system

On the Configuration Inputs panel, when you add a failover system using the Add System option, you may see the following error message:

`Validation has failed for <System Name>.`

Workaround: Verify the following:

- The Symantec High Availability guest components are installed on the system.
- The operating system running on the system is supported by this product.
- The specified system name or IP address is valid and the system is switched on and accessible over the network.
- The firewall settings allow access on port 5634 used by the Storage Foundation Messaging Service.
- If xprtld daemon is running on the system, restarting the xprtld service may resolve the issue.

Adding a failover system may fail when you configure a cluster with communication links over UDP

When you configure a cluster with communication links over UDP and add a failover system, you may see the following error message:

```
The same network adapter is specified for one or more links on the
system. You must select a different network adapter for each
communication link.
```

This issue occurs when you unplumb an IP address from one of the configured communication links. In this scenario, VCS may also go into jeopardy.

Workaround: Plumb the IP address again.

Troubleshooting dashboard issues

This section lists common troubleshooting scenarios that you may encounter when using the Symantec High Availability Dashboard:

A system does not appear on the dashboard

This behavior may occur if one MAC address is plumbed on more than one virtual systems in the data center. In such cases, the dashboard is able to resolve application health reports from only one system, using the MAC address. The dashboard does not display the other system/s with the same MAC address. (2863755)

Workaround: Ensure that no two virtual systems in the data center have the same MAC address.

Task-specific panels launched from dashboard, do not display description for alerts

When you perform administrative tasks such as starting or stopping an application using the Symantec High Availability Dashboard, a task-specific panel appears. In the panel, you can specify the system where you want to perform the administrative task. For some the configured systems listed in the panel, an alert icon appears. However, no description for the reason of the alert is displayed.

The alert icon (!) typically appears when a system reports a stale application health record, or an application fault. Without known such information about the alert, it may be difficult to select the appropriate system for the administrative task. (2919069)

Workaround

Navigate to the appropriate row in the Application table of dashboard. Alert details, such as time stamp of the stale record, are displayed in the Alerts and Description column.

Reporting on the Dashboard

The Dashboard may not report one or more configured failover systems. This can happen:

- If one or more failover systems have MAC addresses that are already in use by other virtual machines in the same datacenter.
  Workaround: Ensure that the cluster systems have unique MAC addresses.
- If one or more cluster systems have not established single sign-on (SSO) with Symantec High Availability Console.
  Workaround: Perform the following steps:
  - a) In the Inventory view of the vSphere Client GUI, navigate to the required virtual machine.
  - Click the Symantec High Availability tab.
  - Enter the username and password of the virtual machine to configure SSO with the Symantec High Availability Console.

Troubleshooting Symantec High Availability tab view issues

This section lists common troubleshooting scenarios that you may encounter when using the Symantec High Availability tab.

High Availability tab not visible from a cluster node

If you click a system in the inventory view of the VMware vSphere client GUI, then the Symantec High Availability tab displays the cluster view (consolidated cluster-level health information of the configured application/s running on the selected system). In some multi-node cluster, the view is not visible from at least one of the cluster nodes.

This behavior occurs if connectivity of the configured LLT links fail. This may be a networking error. (2863649)

Workaround

Ensure that valid LLT links are configured for the affected cluster node, and then retry.

Symantec High Availability tab does not display the application monitoring status

The Symantec High Availability tab in the vSphere Client console may either display a HTTP 404 Not Found error or may not show the application health status at all.

Verify the following conditions and then refresh the Symantec High Availability tab in the vSphere Client console:

- Verify that the Symantec High Availability Console host is running and is accessible over the network.
- Verify that the VMware Web Service is running on the vCenter Server.
- Verify that the VMware Tools Service is running on the guest virtual machine.
- Verify that the Veritas Storage Foundation Messaging Service (xprtld process) is running on the Symantec High Availability Console and the virtual machine. If it is stopped, type the following on the command prompt:

  ```
  net start xprtld
  ```

- Verify that ports 14152, 14153, and 5634 are not blocked by a firewall.
- Log out of the vSphere Client and then login again. Then, verify that the Symantec High Availability plugin is installed and enabled.

Symantec High Availability tab may freeze due to special characters in application display name

For a monitored application, if you specify a display name that contains special characters, one or both of the following symptoms may occur:

- The Symantec high availability tab may freeze
- The Symantec high availability tab may display an Adobe exception error message

  Based on your browser settings, the Adobe exception message may or may not appear. However, in both cases the tab may freeze. (2923079)

  Workaround: Reset the display name using only those characters that belong to the following list:

  - any alphanumeric character
  - space
  - underscore

  Use the following command to reset the display name:

```
hagrp -modify sg name UserAssoc -update Name modified display name
without special characters
```

If the Console host abruptly restarts, the high availability tab may disappear

If the system that hosts the Symantec High Availability Console abruptly restarts, then the registration of the Symantec High Availability plugin with the VMware vCenter Server does not persist.

As a result, the Symantec High Availability tab does not appear on the vSphere Client GUI. (2919549)

Workaround: Repair the Console installation.

In the Symantec High Availability tab, the Add Failover System link is dimmed

If the system that you clicked in the inventory view of the vSphere Client GUI to launch the Symantec High Availability tab is not part of the list of failover target systems for that application, the Add Failover System link is dimmed. (2932281)

Workaround: In the vSphere Client GUI inventory view, click a system from the existing list of failover target systems for the application, to launch the Symantec High Availability tab.The Add Failover System link that appears in the drop down list if you click **More**, is no longer dimmed.

Symantec high availability tab may fail to load or refresh

The Symantec High Availability tab displays health information of monitored applications in a VCS cluster. The tab display may fail to load. It may alternatively fail to refresh itself after the default interval of 60 seconds. (2932028)

Workaround: Restarting the xprtld service may resolve the issue.

To restart the xprtld service

1. Stop the xprtld service:

   # /etc/init.d/xprtld stop

2. Ensure that xprtld is stopped:

   # ps -ef | grep xprtld

   If the services is not stopped, terminate the process:

   # kill -9 *pid*

   Where pid is the process ID of the xprtld process.

3. Start xprtld service:

   # /etc/init.d/xprtld start

An alert icon appears in the Symantec High Availability tab

An Alert icon appears in the title bar of the Symantec High Availabiity tab of the vSphere Client GUI only if the communication between Symantec High Availability Console and a failover system fails. As a result, the Symantec High Availability dashboard fails to display the system, or displays stale application health data for the system.

Workaround:

Perform the following steps

1. Configure single sign-on between the Symantec High Availability Console host and the system.

   For information on configuring single sign-on, see the *Symantec High Availability Console Installation and Configuration Guide*.

2. Bring the VCSInfraSG group online:

   # hagrp -online VCSInfraSG -any