Symantec™ ApplicationHA Installation Guide

Linux on KVM

6.0

November 2011

Symantec

Symantec™ ApplicationHA Installation Guide

Product version: 6.0

Document version: 6.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's 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 Web site 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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec Web site.

https://sort.symantec.com/documents

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

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

Contents

Chapter 1

Introducing Symantec ApplicationHA

This chapter includes the following topics:

What is Symantec ApplicationHA

Symantec ApplicationHA provides monitoring capabilities for applications running inside guest virtual machines in the KVM virtualization environment. Symantec ApplicationHA adds a layer of application awareness to the core high availability (HA) functionality offered by Veritas™ Cluster Server (VCS) in the physical host.

Symantec ApplicationHA is based on VCS and uses similar concepts such as agents, resources, and service groups. However, it does not include the high availability cluster components such as the Group Membership and Atomic Broadcast (GAB), Low Latency Transport (LLT), Asynchronous Monitoring Framework (AMF), and Veritas Fencing (VxFEN). Symantec ApplicationHA has a lightweight server footprint that allows faster installation and configuration.

Key benefits include the following:

- Out of the box integration with VCS.
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside virtual machines.
- High availability of the application as well as the virtual machine inside which the application runs.
- Graded application fault-management responses such as:-
  - Application restart
  - ApplicationHA-initiated, graceful internal reboot (soft reboot) of a virtual machine
  - VCS-initiated, external reboot (hard reboot) of virtual machine
  - Failover of the virtual machine to another VCS node.
- Standardized way to manage applications using a single interface that is integrated with the Veritas Operations Manager (VOM) console.
- Specialized Application Maintenance mode, in which ApplicationHA allows you to intentionally take an application out of its purview for maintenance or troubleshooting.

How ApplicationHA is deployed in the KVM environment

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on AMD64 and Intel64 hardware. KVM lets you create and manage multiple virtual machines on a single physical host.

In the KVM virtualization environment, ApplicationHA provides high availability of applications running on virtual machines. Veritas Cluster Server (VCS) provides high availability of the virtual machines that run on the physical host.

The following figure illustrates how ApplicationHA and VCS are deployed in a typical KVM virtualization environment.

ApplicationHA is installed on the virtual machine, and provides high availability to a configured application running on the virtual machine. VCS is installed on the physical host, as part of a Storage Foundation Cluster File Server High Availability (SFCFSHA) stack installation. VCS provides high availability to the virtual machine where the configured application runs.

To ensure application-aware monitoring of virtual machines, you must enable VCS support for ApplicationHA.

When you enable VCS to support ApplicationHA, a private VLAN is created between monitored virtual machines and the VCS node (physical host). The private VLAN facilitates heartbeat communication between VCS in the physical host and ApplicationHA in the virtual machines.

Veritas Operations Manager (VOM) provides you with a centralized management console (GUI) to administer application monitoring with ApplicationHA.

For more information on how VCS monitors virtual machines for high availability, see the *SFHA Virtualization Solutions Guide for Linux*.

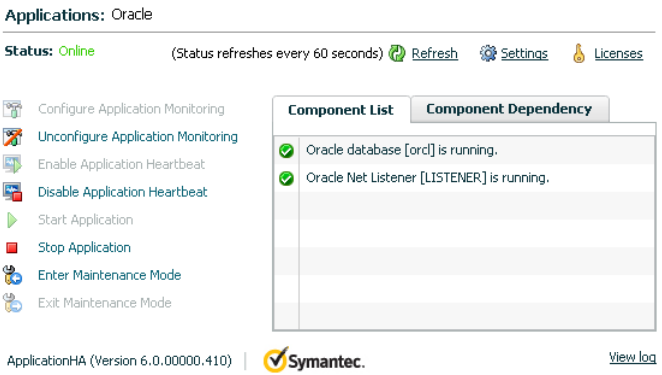
How Symantec ApplicationHA works with VCS

Symantec ApplicationHA installed in virtual machines communicates directly with VCS installed in the physical host. Symantec ApplicationHA conveys the application health status to VCS in the form of a heartbeat. If VCS does not receive the heartbeat from a particular virtual machine within a specified interval, VCS either restarts that virtual machine or fails it over to another physical host.

You can monitor an application running on a virtual machine by using Veritas Operations Manager (VOM). An ApplicationHA add-on for VOM integrates the ApplicationHA tab with VOM.

The ApplicationHA tab is the primary interface for performing the application monitoring operations on a virtual machine. From this tab, you configure application monitoring and then monitor and control the configured application on the virtual machine. After configuring application monitoring, the ApplicationHA tab displays the state of the application and the component dependencies.

The following figure displays the ApplicationHA tab where Oracle is configured for monitoring.



How Symantec ApplicationHA detects application failures

Symantec ApplicationHA architecture uses the agent framework to monitor the state of the applications and their dependent components running inside the virtual machines. Symantec ApplicationHA agents monitor the overall health of the configured applications by running specific commands, tests, or scripts. For

more details, see the agent functions section of the application-specific agent guides or the generic agent guide distributed with ApplicationHA.

The ApplicationHA Heartbeat agent is auto-configured in the virtual machine when you configure application monitoring. The Heartbeat agent sends the application heartbeat to VCS in the physical host. Symantec ApplicationHA uses the application heartbeat as the communication medium to convey the status of the application to VCS.

If an application fails, the application agents attempt to restart the application for a configurable number of times. If the agents are unable to start the application, ApplicationHA tries to reboot the virtual machine. After the virtual machine is restarted, Symantec ApplicationHA attempts to start the application and its dependent components in a predefined order.

Components of the Symantec ApplicationHA setup

A Symantec ApplicationHA setup in the KVM virtualization environment comprises of the following components:.

- Symantec ApplicationHA guest components for virtual machines
- VCS in the virtualization infrastructure
- VOM add-on for Symantec ApplicationHA Management

Symantec ApplicationHA guest components for virtual machines

The Symantec ApplicationHA guest components are installed separately on the virtual machines where you wish to monitor applications. The guest components include the configuration wizard and the ApplicationHA agents that are used for configuring and monitoring applications.

The guest components also include the Veritas Storage Foundation Messaging Service (xprtld). This service communicates the status of the applications running on the virtual machine and displays it in the ApplicationHA tab of the Veritas Operations Manager console.

VCS in the virtualization infrastructure

Veritas Cluster Server (VCS) is installed as part of a Storage Foundation Cluster File System High Availability (SFCFSHA) stack installation on a physical host. VCS is installed on more than one physical host to form a VCS cluster. As a result, VCS provides high availability in the infrastructure layer of the KVM virtualization environment on such physical hosts. VCS mainly ensures high availability of the virtual machines on which ApplicationHA monitors configured applications.

For more information on how ApplicationHA and VCS are integrated in the KVM virtualization environment:

See " How ApplicationHA is deployed in the KVM environment" on page 12.

For more information on how to install VCS as part of an SFCFSHA installation, see the *SFCFSHA Installation Guide*.

VOM add-on for Symantec ApplicationHA Management

The Veritas Operations Manager (VOM) Add-on for ApplicationHA Management is installed on the VOM Management Server. You must also add as managed hosts to VOM, the virtual machines where you want ApplicationHA to monitor applications. The ApplicationHA tab then appears on the VOM console for the respective virtual machine, and lets you administer application monitoring with ApplicationHA in the KVM environment.

Symantec ApplicationHA user privileges

Symantec ApplicationHA provides a set of privileges that are available when using VOM Console to manage ApplicationHA. These privileges define the application monitoring operations that a user can perform on the virtual machines. You can create roles and then assign privileges to the roles or assign privileges to the existing roles that are available in the virtualization environment. Application monitoring operations are enabled or disabled depending on the privileges that are assigned to the VOM user account. For example, the Admin privilege is required for configuring application monitoring on a virtual machine.

VOM administrators can use these privileges to configure access control in an application monitoring environment.

Symantec ApplicationHA provides the following privileges:

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

Can perform all ApplicationHA 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 monitoring maintenance mode, and view application monitoring status.

Symantec ApplicationHA agents

Agents are application-specific modules that plug into the ApplicationHA framework that manages applications and resources of predefined resource types on a system. The agents are installed when you install Symantec ApplicationHA guest components. These agents start, stop, and monitor the resources configured for the applications and report state changes. If an application or its components fail, ApplicationHA restarts the application and its resources on the virtual machine.

Symantec ApplicationHA agents are classified as follows:

- Infrastructure agents

  Agents such as NIC, IP, and Mount are classified as infrastructure agents. Infrastructure agents are automatically installed as part of the ApplicationHA installation on virtual machines.

  For more details about the infrastructure agents, refer to the *Veritas Cluster Server 6.0 Bundled Agents Reference Guide (Linux).*

- Application agents

  Application agents are used to monitor third party applications such as Oracle. These agents are packaged separately and are available in the form of an agent pack that gets installed when you install Symantec ApplicationHA guest components.

  The ApplicationHA agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing ApplicationHA guest components installation.

  Refer to the Symantec Operations Readiness Tools (SORT) Web site for information on the latest agent pack availability.

  https://sort.symantec.com/agents

  Refer to the agent-specific configuration guide for more details about the application agents.

About Symantec ApplicationHA licensing

Symantec ApplicationHA is a licensed product. Licensing for Symantec ApplicationHA is applicable for ApplicationHA guest components and is based on the server operating systems in use.

An evaluation license key is embedded in the product. This license key is valid only for a period of 2 months. If you are installing ApplicationHA for the first time, you can use the embedded license key or procure a permanent license key and enter the same while installing the product.

You can add or view the license keys from a virtual machine that has ApplicationHA guest components installed. You can add a license key through the command line or the ApplicationHA tab. For more information:

See "About managing ApplicationHA licenses" on page 53.

Ensuring high availability of applications

You can ensure high availability of applications running inside virtual machines by using ApplicationHA. To provide high availability to the applications, perform the following steps:

- Install Veritas Operations Manager Add-on for ApplicationHA Management on the VOM Management Server.
- Install ApplicationHA on the virtual machine
- Add the virtual machine as a managed host to Veritas Operations Manager (VOM)
- Configure application monitoring on the virtual machine.

The following figure illustrates the workflow for ensuring high availability of applications with ApplicationHA. The figure also indicates the corresponding document that you must refer for detailed instructions at each step.

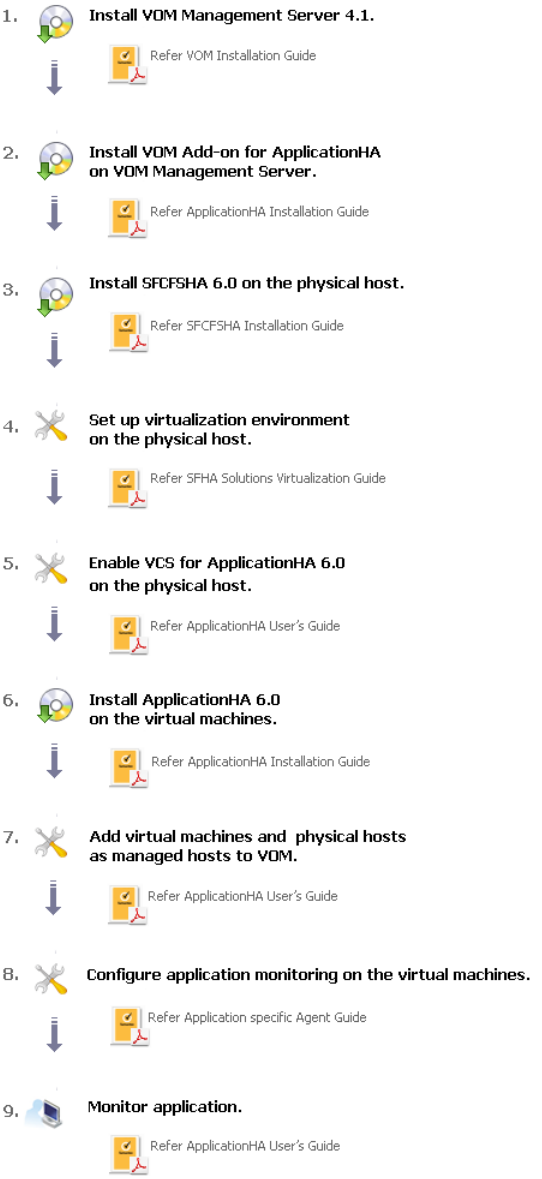

1.
Install VOM Management Server 4.1.
Refer VOM Installation Guide
2.
Install VOM Add-on for ApplicationHA
on VOM Management Server.
Refer ApplicationHA Installation Guide
3.
Install ApplicationHA 6.0
on the virtual machines.
Refer ApplicationHA Installation Guide
4.
Add virtual machines and physical hosts
as managed hosts to VOM.
Refer ApplicationHA User's Guide
5.
Configure application monitoring on the virtual machines.
Refer Application specific Agent Guide
6.
Monitor application.
Refer ApplicationHA User's Guide

Ensuring high availability of virtualization infrastructure

In addition to high availability of applications using ApplicationHA, you can also ensure high availability of the virtualization infrastructure with VCS. By using VCS, you can externally restart virtual machines and fail over the virtual machines in case of application failures or virtual machine failures. To ensure high availability of the virtualization environment, perform the following steps:

- Install Veritas Operations Manager Add-on for ApplicationHA Management on the VOM Management Server.
- Install SFCFS HA on the physical host.
- Enable ApplicationHA capabilities in underlying VCS in the physical host.
- Install ApplicationHA on the virtual machine.
- Add virtual machine and physical host as managed hosts to Veritas Operations Manager (VOM).
- Configure application monitoring on the virtual machine.

The following figure illustrates the workflow for ensuring high availability of the applications running inside the virtual machine and the virtualization infrastructure. The figure also indicates the corresponding documents that you must refer for detailed instructions at each step.


1. Install VOM Management Server 4.1.
Refer VOM Installation Guide
2. Install VOM Add-on for ApplicationHA on VOM Management Server.
Refer ApplicationHA Installation Guide
3. Install SFCFSHA 6.0 on the physical host.
Refer SFCFSHA Installation Guide
4. Set up virtualization environment on the physical host.
Refer SFHA Solutions Virtualization Guide
5. Enable VCS for ApplicationHA 6.0 on the physical host.
Refer ApplicationHA User's Guide
6. Install ApplicationHA 6.0 on the virtual machines.
Refer ApplicationHA Installation Guide
7. Add virtual machines and physical hosts as managed hosts to VOM.
Refer ApplicationHA User's Guide
8. Configure application monitoring on the virtual machines.
Refer Application specific Agent Guide
9. Monitor application.
Refer ApplicationHA User's Guide

Chapter 2

Planning to install Symantec ApplicationHA

This chapter includes the following topics:

About installing Symantec ApplicationHA

Table 2-1 describes the installation tasks for ensuring high availability of the applications.

Table 2-1 Installation tasks for ensuring high availability of applications

Task	Description
Install VOM Management Server 4.1 and install the ApplicationHA add-on	Download the installer for VOM Management Server 4.1. The installer is available here: http://sort.symantec.com On the VOM Management Server 4.1, install the VOM add-on for ApplicationHA. The add-on is available here: http://www.symantec.com/sfm_addons

Table 2-1 Installation tasks for ensuring high availability of applications *(continued)*

Task	Description
Install Symantec ApplicationHA guest components for virtual machines	Install the Symantec ApplicationHA guest components on the virtual machines where you want to monitor applications. Symantec ApplicationHA guest components include ApplicationHA agents and configuration wizards.
Add required virtual machines to VOM as managed hosts	Add the virtual machines where you want to monitor applications, to the list of managed hosts in VOM. As a result, when you click a configured virtual machine in the VOM console, the ApplicationHA tab appears.
Configure application monitoring on the virtual machines	In the ApplicationHA tab, click Configure application monitoring to launch the Application Monitoring Configuration Wizard.
Administer application monitoring on the virtual machines	Click the appropriate links in the ApplicationHA tab, to perform administrative actions on configured applications.

Table 2-2 describes the installation tasks for ensuring high availability of applications and the virtualization infrastructure on which the applications run.

Table 2-2 Installation tasks for ensuring high availability of applications and virtualization infrastructure

Task	Description
Install VOM Management Server 4.1 and install the ApplicationHA add-on on the server	Download the installer for VOM Management Server 4.1. The installer is available here: http://sort.symantec.com On the VOM Management Server 4.1, install the VOM add-on for ApplicationHA. The add-on is available here: http://www.symantec.com/sfm_addons
Install SFCFSHA 6.0 on the physical host	SFCFSHA 6.0 enables you to ensure high availability of the virtualization infrastructure in terms of restart and failover of failed virtual machines.

Table 2-2 Installation tasks for ensuring high availability of applications and virtualization infrastructure *(continued)*

Task	Description
Enable ApplicationHA capabilities for underlying VCS 6.0	Run the enable_applicationha script from /opt/VRTSvcs/bin/utils path on each physical host. The enable_applicationha script configures the infrastructure settings. It also enables communication between VCS in the physical host and ApplicationHA in the virtual machines.
Install Symantec ApplicationHA guest components for virtual machines	Install the Symantec ApplicationHA guest components on the virtual machines where you want to monitor applications. Symantec ApplicationHA guest components include ApplicationHA agents and configuration wizards.
Add required virtual machines and physical host to VOM as managed hosts	Add the virtual machines where you want to monitor applications, to the list of managed hosts in VOM. You may optionally add the physical hosts to VOM. This allows you to co-relate a virtual machine with the physical host hosting it.
Configure application monitoring on the virtual machines	In the ApplicationHA tab, click Configure application monitoring to launch the Application Monitoring Configuration Wizard.
Administer application monitoring on the virtual machines	Click the appropriate links in the ApplicationHA tab, to perform administrative actions on configured applications.

Requirements for installing ApplicationHA on virtual machines

You can install Symantec ApplicationHA Guest Components on virtual machines running Linux. The virtual machine where you want to install ApplicationHA Guest Components must meet the following requirements.

For the latest information on system requirements, refer to the latest version of the product documentation on the Symantec Operations Readiness Tools (SORT) Web site: https://sort.symantec.com

Supported virtualization environments

Symantec ApplicationHA can be installed and run inside virtual machines in a KVM virtualization environment, running Red Hat Enterprise Linux (RHEL) 6, Update 1 in the physical host.

Supported operating systems on virtual machines

Table 2-3 shows the supported operating systems for Symantec ApplicationHA 6.0.

Table 2-3 Supported guest operating systems

Operating systems	Levels	Kernel version
Red Hat Enterprise Linux 5	U3 or later	2.6.18-128.el5
Red Hat Enterprise Linux 6	Base or later	2.6.32-71.el6

Note: 64-bit operating systems are only supported.

If your system is running a lower level of Red Hat Enterprise Linux, than indicated in Table 2-3, you must upgrade it before attempting to install Symantec ApplicationHA. Consult the Red Hat documentation for more information on upgrading or reinstalling your operating system.

Symantec supports only Red Hat distributed kernel binaries.

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

Required Linux RPMs for Symantec ApplicationHA

Make sure you install the following operating system-specific RPMs on the systems where you want to install ApplicationHA. ApplicationHA will support any updates made to the following RPMs, provided the RPMs maintain the ABI compatibility.

Table 2-4 lists the RPMs that ApplicationHA requires for a given Linux operating system.

Table 2-4 Required RPMs

Operating system	Required RPMs
RHEL 5	compat-libstdc++-33-3.2.3-61.x86_64.rpm glibc-2.5-58.i686.rpm glibc-2.5-58.x86_64.rpm ksh-20100202-1.el5_5.1.x86_64.rpm libgcc-4.1.2-50.el5.i386.rpm libgcc-4.1.2-50.el5.x86_64.rpm libstdc++-4.1.2-50.el5.i386.rpm pam-0.99.6.2-6.el5_5.2.x86_64.rpm
RHEL 6	compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm glibc-2.12-1.7.el6.x86_64.rpm glibc-2.12-1.7.el6.i686.rpm ksh-20100621-2.el6.x86_64.rpm libgcc-4.4.4-13.el6.i686.rpm libgcc-4.4.4-13.el6.x86_64.rpm libstdc++-4.4.4-13.el6.i686.rpm libstdc++-4.4.4-13.el6.x86_64.rpm pam-1.1.1-4.el6.x86_64.rpm

Supported applications

Table 2-5 lists the applications that Symantec ApplicationHA 6.0 currently supports on virtual machines.

Table 2-5 Symantec ApplicationHA supported applications

Application	Version
Oracle Database	10gR2, 11gR1, and 11gR2
WebSphere Application Server	7.x
WebSphere MQ	7.x
Apache HTTP Server	1.3, 2.0, and 2.2. Also supports the IBM HTTP Server 7.x.

Table 2-5 Symantec ApplicationHA supported applications *(continued)*

Application	Version
DB2	9.5 and 9.7

Note: Alternatively, you can use the Generic Agent to configure other applications that are not listed in the above support matrix. For more information refer to *Symantec ApplicationHA Generic Agent Configuration Guide*.

Permissions requirements

The following permissions are required for installing the ApplicationHA guest components on the virtual machines:

- You must have root privileges on the virtual machine where you install the guest components.
  In case of remote installation, you must also have root privileges on all the virtual machines where you install the ApplicationHA guest components.

Ports and firewall settings for application high availability

ApplicationHA uses certain ports and services during installation and configuration. If you have configured a firewall, ensure that the firewall settings allow access to these ports and services on the virtual machines.

Table 2-6 displays the services and ports used by ApplicationHA.

Table 2-6 Services and ports used by Symantec ApplicationHA

Component Name	Port	Settings	Description
Veritas Storage Foundation Messaging Service (xprtld)	5634	Allow inbound and outbound	Used for communications between the VOM Console and the virtual machines.
Veritas Operations Manager (VOM)	14161	Allow inbound and outbound	Used by the Tomcat server on VOM Console to receive Web service requests and for local administration.

Requirements for providing high availability of virtualization environment

The following are the requirements for providing high availability of the virtualization environment:

- Install SFCFSHA 6.0 on the physical host
  Refer to *Veritas Storage Foundation Cluster File System Installation Guide - Linux*
- Review the settings of the virtualization environment for which you want to provide high availability
  Refer to *Veritas Storage Foundation and High Availability Solutions Virtualization Guide - Linux*
- Enable ApplicationHA capabilities for underlying VCS 6.0
  Refer to *Symantec ApplicationHA User's Guide - Linux on KVM*

Ports and firewall settings for virtualization infrastructure high availability

ApplicationHA uses certain ports and services when providing high availability of the virtualization environment. If you have configured a firewall, ensure that the firewall settings allow access to these ports and services on the virtual machines.

Table 2-7 displays the services and ports used by ApplicationHA for providing high availability of the virtualization environment.

Table 2-7 Services and ports used by Symantec ApplicationHA

Component Name	Port	Settings	Description
Veritas Storage Foundation Messaging Service (xprtld)	5634	Allow inbound and outbound	Used for communications between the VOM Console host machine and the virtual machines.
Veritas Operations Manager (VOM)	14161	Allow inbound and outbound	Used by the Tomcat server on VOM Console to receive Web service requests and for local administration.

Table 2-7 Services and ports used by Symantec ApplicationHA *(continued)*

Component Name	Port	Settings	Description
Internal communication component	14142	Allow inbound and outbound	Used for communication between, VCS in the physical host and ApplicationHA in the virtual machine

Additional requirements

The following additional software requirements apply:

- Internet Explorer or Firefox Web browser is required on the systems where you access the Veritas Operations Manager console to manage the virtual machines.
  Microsoft Internet Explorer 6.x, 7.x, 8.x, and 9.x are supported.
  Mozilla Firefox 3.x, 4.x, 5.x, and 6.x are supported.
- Adobe Flash Player
  Install Adobe Flash Player (version 9.0 or later) on the systems from where you access the Veritas Operations Manager console to manage the virtual machines.
- Symantec ApplicationHA license
  An evaluation key is embedded in the product and is valid for two months. You can use all the product features during that period. To continue unrestricted usage, you must procure a valid license key.
- When installing Symantec ApplicationHA, ensure that there are no parallel installations in progress.

Chapter 3

Installing Symantec ApplicationHA Guest Components

This chapter includes the following topics:

About preparing to install Symantec ApplicationHA guest components

Before you perform the preinstallation tasks, ensure that you meet the following installation requirements, set up the basic hardware, and plan your ApplicationHA setup.

- See "Supported virtualization environments" on page 26.
- See "Supported operating systems on virtual machines" on page 26.
- See "Required Linux RPMs for Symantec ApplicationHA" on page 26.
- See "Supported applications" on page 27.
- See "Permissions requirements" on page 28.

- See "Ports and firewall settings for application high availability" on page 28.
- See "Additional requirements" on page 30.

Performing preinstallation tasks

Table 3-1 lists the tasks you must perform before proceeding to install ApplicationHA.

Table 3-1 Preinstallation tasks

Task	Reference
Obtain license keys	See "Obtaining Symantec ApplicationHA license keys" on page 32.
Set the PATH variable	See "Setting the PATH variable" on page 33.
Mount the product disc	See "Mounting the product disc" on page 33.
Verify the system before installation	See "Performing an automated preinstallation check" on page 34.

Obtaining Symantec ApplicationHA license keys

You must obtain and install a license key for ApplicationHA.

See "About Symantec ApplicationHA licensing " on page 18.

This product includes a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased. A single key lets you install the product on the number and type of systems for which you purchased the license. A key may enable the operation of more products than are specified on the certificate. However, you are legally limited to the number of product licenses purchased. The product installation procedure describes how to activate the key.

To register and receive a software license key, go to the Symantec Licensing Portal at the following location:

https://licensing.symantec.com

Make sure you have your Software Product License document. You need information in this document to retrieve and manage license keys for your Symantec product. After you receive the license key, you can install the product.

Click the Help link at this site to access the License Portal User Guide and FAQ.

The VRTSvlic package enables product licensing. After the VRTSvlic is installed, the following commands and their manual pages are available on the system:

vxlicinst	Installs a license key for a Symantec product
vxlicrep	Displays currently installed licenses
vxlictest	Retrieves the features and their descriptions that are encoded in a license key

Setting the PATH variable

Installation commands as well as other commands reside in the /opt/VRTS/bin directory. Add this directory to your PATH environment variable.

To set the PATH variable

- Do one of the following
  - For the Bourne Shell (bash or sh) or Korn Shell (ksh), type:

    ```
    $ PATH=/opt/VRTS/bin:$PATH; export PATH
    ```

  - For the C Shell (csh or tcsh), type:

    ```
    $ setenv PATH :/opt/VRTS/bin:$PATH
    ```

Mounting the product disc

You must have super user (root) privileges to load the ApplicationHA software.

To mount the product disc

1. Log in as super user on the system from where you want to install ApplicationHA.

   The system must run the supported operating system version. You can either install ApplicationHA on the node where you run the install program, or you can install ApplicationHA on a remote node.

2. Insert the product disc with the ApplicationHA software into a drive that is connected to the system.

   The disc is automatically mounted.

3 If the disc does not automatically mount, then enter:

```
# mount -o ro /dev/cdrom /mnt/cdrom
```

4 Navigate to the location of the install program for the required operating system:

Operating system	Folder name
Red Hat Enterprise Linux 5	cdrom_root/linux-x86_64-kvm/rhel5_x86_64/applicationha
Red Hat Enterprise Linux 6	cdrom_root/linux-x86_64-kvm/rhel6_x86_64/applicationha

For example, to install ApplicationHA on a machine running the RHEL 5 operating system,

```
# cd cdrom_root/linux-x86_64-kvm/rhel5_x86_64/applicationha
```

Performing an automated preinstallation check

Before you begin the installation of ApplicationHA software, you can check the readiness of the system where you plan to install Symantec ApplicationHA.

To check the system

1 Navigate to the folder that contains the installapplicationha program.

See "Mounting the product disc" on page 33.

2 Start the preinstallation check:

```
# ./installer -precheck system1
```

The program proceeds in a non-interactive mode to examine the system for licenses, RPMs, disk space, and system-to-system communications.

3 Review the output as the program displays the results of the check and saves the results of the check in a log file.

ApplicationHA installation methods for guest components

Table 3-2 lists the different methods that you can choose to install ApplicationHA guest components on virtual machines running the Linux operating system:

Table 3-2 ApplicationHA installation methods

Method	Description
Interactive installation using the installapplicationha program	The install program asks you a few questions and installs ApplicationHA, based on the information you provide. One of the options is directly installing ApplicationHA using the install program, which internally uses the installapplicationha program.
Automated installation using the ApplicationHA response files	At the end of each successful installation, the install program creates response files. You can use these response files to perform multiple installations to set up multiple virtual machines.
Manual installation using the Linux commands and utilities	You can install ApplicationHA using the operating system `rpm -i` command.

Installing Symantec ApplicationHA using the install program

Perform the following steps to install ApplicationHA:

Note: The system from where you install ApplicationHA must run the same Linux distribution as the target virtual machines.

To install ApplicationHA

1. Confirm that you are logged in as the super user and you mounted the product disc.

   See "Mounting the product disc" on page 33.

2. Navigate to the directory that contains the installation program for the required operating system:

Operating system	Directory
Red Hat Enterprise Linux 5	linux-x86_64-kvm/rhel5_x86_64
Red Hat Enterprise Linux 6	linux-x86_64-kvm/rhel6_x86_64

   For example, to install ApplicationHA on a machine running the RHEL 5 operating system,

   ```
   # cd cdrom_root/linux-x86_64-kvm/rhel5_x86_64/applicationha
   ```

3. Run the installer to start installation on the guest.

   ```
   # ./installapplicationha
   ```

4. Enter **y** to agree to the End User License Agreement (EULA).

   ```
   Do you agree with the terms of the End User License Agreement
   as specified in the EULA.pdf file present on media? [y,n,q,?] y
   ```

5. Enter the name of the systems where you want to install ApplicationHA.

   The install program does the following:

   - Checks that the local system that runs the install program can communicate with the remote system.
     If the install program finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
     If the default communication method ssh fails, the install program attempts to use rsh.
   - Makes sure the system uses one of the supported operating systems.
     See "Supported operating systems on virtual machines" on page 26.
   - Makes sure that either ssh or rsh communication is enabled between the systems. Else, the install program prompts you for the root password and allows you to enable communication using either ssh or rsh.
   - Makes sure that the system has the required operating system patches.

If the install program reports that any of the patches are not available, install the patches on the system before proceeding with the ApplicationHA installation.
See "Required Linux RPMs for Symantec ApplicationHA" on page 26.

- Checks for product licenses.
- Checks for the required file system space and makes sure that any processes that are running do not conflict with the installation.
  If requirements for installation are not met, the install program stops and indicates the actions that you must perform to proceed with the process.
- Checks whether any of the RPMs already exist on a system.
  If the current version of any RPMs exists, the install program removes the RPMs from the installation list for the system.

6 Review the list of RPMs that the install program would install on the virtual machine.

The install program installs the ApplicationHA RPMs on the system that you specified in step 5. For example, galaxy.

7 If the system on which you install ApplicationHA does not have a permanent license key installed, the install program prompts you for the license type.

Based on the license type that you want to use, perform one of the following:

- To specify a new license key, enter **y** and when the installer prompts, specify the new license key.
- To use the evaluation license key, enter **n**.

The install program registers the license, and proceeds with the installation.

8 Enter y at the prompt to send the installation information to Symantec.

```
Would you like to send the information about this installation
to Symantec to help improve installation in the future? [y,n,q,?] (y)
y
```

The install program provides an option to collect data about the installation process each time you complete an installation of the product. The install program transfers the contents of the install log files to an internal Symantec site. The information is used only to gather metrics about how you use the install program. No personal customer data is collected, and no information will be shared with any other parties. Information gathered may include the product and the version installed or upgraded, the number of systems installed, and the time spent in any section of the install process.

9 After the installation, note the location of the installation log files, the summary file, and the response file for future reference.

These files provide useful information that can assist you with future installations.

summary file	Lists the RPMs that are installed on each system.
log file	Details the entire installation.
response file	Contains the installation information that can be used to perform unattended or automated installations on other systems. See "Installing Symantec ApplicationHA using response files" on page 38.

Installing Symantec ApplicationHA using response files

When you install ApplicationHA on a virtual machine using the install program, it generates a response file. You can use the response file to install ApplicationHA on other virtual machines. You can also generate the response file using the `-makeresponsefile` option on the install program.

To install ApplicationHA using response files

1. Make sure the system where you want to install ApplicationHA meet the installation requirements.

   See "Requirements for installing ApplicationHA on virtual machines" on page 25.

2. Make sure the preinstallation tasks are completed.

   See "Performing preinstallation tasks" on page 32.

3. Create a response file on the system where you want to run the installer.

   See "Response file variables to install Symantec ApplicationHA" on page 39.

   See "Sample response file for installing Symantec ApplicationHA" on page 41.

4. Mount the product disc and navigate to the folder that contains the installation program.

5. Start the installation from the system to which you copied the response file. For example:

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

   # ./installapplicationha -responsefile response_file
   ```

   Where *response_file* is the response file's full path name.

Response file variables to install Symantec ApplicationHA

Table 3-3 lists the response file variables that you can define to install ApplicationHA.

Table 3-3 Response file variables specific to installing Symantec ApplicationHA

Variable	List or Scalar	Description
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)
CFG{opt}{install}	Scalar	Installs Symantec ApplicationHA RPMs. (Required)
CFG{systems}	List	Name of the systems on which the product is to be installed. (Required)

Table 3-3 Response file variables specific to installing Symantec ApplicationHA *(continued)*

Variable	List or Scalar	Description
CFG{prod}	Scalar	Defines the product to be installed. The value is APPLICATIONHA60. (Required)
CFG{keys} {system}	Scalar	List of keys to be registered on the system. (Optional) **Note:** If you do not provide a valid license key or if the systems where you install the product do not have a valid license key installed, then the installer will install the evaluation license key on these systems.
CFG{uploadlogs}	Scalar	Specifies whether the installer log files must be uploaded to the telemetrics server for troubleshooting. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of the ssh keyfile that is used to communicate with the remote system. (Optional)
CFG{opt}{pkgpath}	Scalar	Defines a location, typically an NFS mount, from which the remote system can install product RPMs. The location must be accessible from the target system. (Optional)

Table 3-3 Response file variables specific to installing Symantec ApplicationHA *(continued)*

Variable	List or Scalar	Description
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The install program copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for installing Symantec ApplicationHA

Review the response file variables and their definitions.

See "Response file variables to install Symantec ApplicationHA" on page 39.

```
#
# Configuration Values:
#
our %CFG;

$CFG{accepteula}=1;
$CFG{keys}{galaxy}="LICENSEKEY";
$CFG{opt}{configure}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="APPLICATIONHA60";
$CFG{systems}=[ qw(galaxy) ];
$CFG{uploadlogs}=1;
```

Chapter 4

Installing the VOM add-on for ApplicationHA

This chapter includes the following topics:

Prerequisites for using the Veritas Operations Manager Add-on for ApplicationHA

The following table describes the versions of the components that are required for installing and running the Veritas Operations Manager Add-on for ApplicationHA Management:

Table 4-1 Versions for the required components

Component	Version
Veritas Operations Manager Management Server	4.1 or later
Veritas Operations Manager managed host	Linux: 4.1 or later
Symantec ApplicationHA on the virtual machine	6.0 or later

Installing the VOM add-on for ApplicationHA

To be able to view the ApplicationHA tab on the Veritas Operations Manager (VOM) console, you must install the VOM add-on for ApplicationHA Management on the VOM Management Server. You can download the add-on from the Symantec support site:

http://www.symantec.com/sfm_addons

You must first upload the add-on to the VOM repository, and then install the add-on.

To upload the VOM add-on

1. On the VOM console, click **Settings** > **Deployment Management**.
2. Select **ApplicationHA Management**.
3. Click **Actions** > **Upload**.
4. On the Upload to Repository page, click **Browse**.
5. Navigate to the location where you downloaded the VOM add-on for ApplicationHA Management, and click **OK**.

To install the VOM add-on

1. On the VOM console, select **Settings** > **Deployment Management**.
2. Select the add-on for ApplicationHA, and click **Install**.
3. Select the option to install the add-on only on the Management Server, and click **Install**.

   Note: After the add-on is installed, restart the Web Server on the VOM Management Server.

4. Click **OK**.

For information on how to use the VOM add-on for ApplicationHA, refer to the *Symantec ApplicationHA User's Guide*.

Chapter 5

Performing post-installation tasks

This chapter includes the following topics:

Accessing the Symantec ApplicationHA documentation

The software disc contains the documentation for ApplicationHA in Portable Document Format (PDF). After you install ApplicationHA, Symantec recommends that you copy the PDF version of the documents to each virtual machine to make it available for reference.

To make the ApplicationHA documentation accessible from virtual machines

1 Navigate to the directory that contains the PDF version of the documents for the required operating system:

Operating system	Directory
Red Hat Enterprise Linux 5	linux-x86_64-kvm/rhel5_x86_64
Red Hat Enterprise Linux 6	linux-x86_64-kvm/rhel6_x86_64

For example, to access the documents for the RHEL 5 operating system,

```
# cd cdrom_root/linux-x86_64-kvm/rhel5_x86_64/docs/
```

2 To copy the PDF to the /opt/VRTS/docs directory, run the following command:

```
# cp *.pdf /opt/VRTS/docs
```

You can also download the latest version of the product documentation from the Symantec Operations Readiness Tools (SORT) Web site.

https://sort.symantec.com

Removing permissions for communication

Make sure you completed the installation of ApplicationHA. If you used `rsh`, remove the temporary `rsh` access permissions that you set for the virtual machines and restore the connections to the public network.

If the virtual machines use `ssh` for secure communications, and you temporarily removed the connections to the public network, restore the connections.

Chapter 6

Uninstalling Symantec ApplicationHA Guest Components

This chapter includes the following topics:

Preparing to uninstall Symantec ApplicationHA

Before you uninstall ApplicationHA from any virtual machine:

- Shut down the applications that depend on ApplicationHA. For example, applications configuration wizards or any high availability agents for ApplicationHA.

You must meet the following conditions to remotely uninstall ApplicationHA from the virtual machines, using the uninstallapplicationha program:

- Make sure that the communication exists between virtual machines. By default, the uninstall program uses ssh.
- Make sure you can execute `ssh` or `rsh` commands as super user on the virtual machines.

If you cannot meet the prerequisites, you will not be able to remotely uninstall ApplicationHA. You must run the uninstallapplicationha program on the virtual machine from which you want to uninstall ApplicationHA.

The uninstallapplicationha program removes all ApplicationHA RPMs.

The following section describes how to uninstall ApplicationHA using the uninstallapplicationha program. The example procedure uninstalls ApplicationHA from the selected or provided virtual machine.

Uninstalling Symantec ApplicationHA using the uninstall program

The program stops the ApplicationHA processes that are currently running during the uninstallation process.

To uninstall ApplicationHA

1. Log in as super user in the system where you want to uninstall ApplicationHA.
2. Start the uninstallapplicationha program.

   ```
   # cd /opt/VRTS/install
   # ./uninstallapplicationha
   ```

   The program specifies the directory where the logs are created. The program displays a copyright notice and a description of the virtual machine.
3. Enter the name of the systems from which you want to uninstall ApplicationHA.

   The program performs the following:

   - Verifies the communication between systems
   - Checks the installation on the system to determine the RPMs to be uninstalled.
   - Asks to stop all running ApplicationHA processes.
4. Enter **y** to stop all the ApplicationHA processes.

   The program proceeds with uninstalling the software.
5. Review the output as the uninstall program stops processes and removes the RPMs.
6. Note the location of summary and log files that the uninstall program creates after removing all the RPMs.

Running uninstallapplicationha program from the ApplicationHA media

You may need to use the uninstallapplicationha program on the ApplicationHA 6.0 media in one of the following cases:

- You need to uninstall ApplicationHA after an incomplete installation.
- The uninstallapplicationha program is not available in /opt/VRTS/install.

If you have mounted the ApplicationHA media at `/mnt/cdrom` then, you can find the uninstallapplicationha program in the following location:

`/mnt/cdrom/directory/applicationha/`

Where *directory* is the folder containing the uninstallapplicationha program for the respective operating system.

Operating system	Directory
Red Hat Enterprise Linux 5	linux-x86_64-kvm/rhel5_x86_64
Red Hat Enterprise Linux 6	linux-x86_64-kvm/rhel6_x86_64

For example, to uninstall ApplicationHA on a machine running RHEL 5 operating system, you can find the uninstallapplicationha program in the following location:
`/mnt/cdrom/linux-x86_64-kvm/rhel5_x86_64/applicationha/`

For information on how to use the uninstallapplicationha program:

See "Uninstalling Symantec ApplicationHA using the uninstall program" on page 48.

Uninstalling Symantec ApplicationHA using response files

Typically, you can use the response file that the install program generates after you perform ApplicationHA uninstallation on one virtual machine.

To perform automated ApplicationHA uninstallation

1. Make sure that you are prepared to uninstall ApplicationHA.

   See "Preparing to uninstall Symantec ApplicationHA" on page 47.

2. Copy the response file to the system where you want to uninstall ApplicationHA.

   See "Sample response file for uninstalling Symantec ApplicationHA" on page 51.

3. Edit the values of the response file variables as necessary.

   See "Response file variables to uninstall Symantec ApplicationHA" on page 50.

4. Start the uninstallation from the system to which you copied the response file. For example:

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

# ./uninstallapplicationha -responsefile response_file
```

   Where *response_file* is the response file's full path name.

Response file variables to uninstall Symantec ApplicationHA

Table 6-1 lists the response file variables that you can define to uninstall ApplicationHA.

Table 6-1 Response file variables specific to uninstalling ApplicationHA

Variable	List or Scalar	Description
CFG{opt}{uninstall}	Scalar	Uninstalls ApplicationHA RPMs. (Required)
CFG{systems}	List	Name of the system on which the product is to be uninstalled. (Required)
CFG{prod}	Scalar	Defines the product to be uninstalled. The value is APPLICATIONHA60. (Required)
CFG{uploadlogs}	Scalar	Specifies whether the installer log files must be uploaded to the telemetrics server for troubleshooting. (Optional)

Table 6-1 Response file variables specific to uninstalling ApplicationHA *(continued)*

Variable	List or Scalar	Description
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of the ssh keyfile that is used to communicate with the remote system. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the depots that are needed during the uninstall. The default location is /var/tmp. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The install program copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for uninstalling Symantec ApplicationHA

Review the response file variables and their definitions.

See "Response file variables to uninstall Symantec ApplicationHA" on page 50.

```
#
# Configuration Values:
#
our %CFG;

$CFG{opt}{uninstall}=1;
$CFG{prod}="APPLICATIONHA60";
$CFG{systems}=[ qw(galaxy) ];
```

Chapter 7

Managing Symantec ApplicationHA licenses

This chapter includes the following topics:

About managing ApplicationHA licenses

When the embedded, two-month, evaluation license key expires, you may want to add a permanent license key.

You can add or view the license key from any virtual machine that has ApplicationHA guest components installed. You can use one of the following methods to manage the licenses:

- From the command line, run the following commands:
  To view an existing license:
  `/opt/VRTS/bin/vxlicrep`
  To install a new license:
  `/opt/VRTS/bin/vxlicinst`
- When you run the CPI installer to install or upgrade ApplicationHA, you can specify a new license key.
- Connect to the Veritas Operations Manager console and select the virtual machine for which you want to update the licenses. Select the **ApplicationHA** tab and click **Licenses**. Use this path to manage licenses for the local virtual machine.
  See "Managing ApplicationHA licenses through ApplicationHA tab" on page 54.

Managing ApplicationHA licenses through ApplicationHA tab

Perform the following steps to manage ApplicationHA licenses through the ApplicationHA tab.

To manage the ApplicationHA licenses

1. Connect to the Veritas Operations Manager.
2. In the Veritas Operations Manager console, click **Manage** > **Servers** > **Hosts**.
3. In the left pane, in the **License** list box, select the **ApplicationHA** check box.
4. In the right pane, click the virtual machine where you want to perform administrative actions.
5. Click the **ApplicationHA** tab and then click **Licenses**.
6. On the License Management panel, enter the new license key in the **Enter license key** text box and then click **Add**.
7. Click **Close**.

Appendix A

ApplicationHA installation packages

This appendix includes the following topics:

Symantec ApplicationHA installation RPMs

Table A-1 shows the RPM name and contents for each Veritas Cluster Server RPM.

Table A-1 Symantec ApplicationHA RPMs

RPM	Contents
VRTSvlic	Contains the binaries for Symantec License Utilities.
VRTSperl	Contains Veritas Perl 5.10.0 redistribution by Symantec.
VRTSspt	Contains the binaries for Veritas Software Support Tools by Symantec.
VRTSsfmh	Contains the binaries for Veritas Storage Foundation Managed Host by Symantec.
VRTSvcs	VRTSvcs contains the following components: ■ Contains the binaries for Veritas Cluster Server. ■ Contains the binaries for Veritas Cluster Server manual pages. ■ Contains the binaries for Veritas Cluster Server English message catalogs. ■ Contains the binaries for Veritas Cluster Server utilities. These utilities include security services.

Table A-1 Symantec ApplicationHA RPMs *(continued)*

RPM	Contents
VRTSvcsag	Contains the binaries for Veritas Cluster Server bundled agents by Symantec.
VRTSvcsvmw	Contains the ApplicationHA virtual machine wizards for application monitoring configurations by Symantec.
VRTSsapnw04	Contains the binaries for Veritas High Availability Agent for SAP NetWeaver. **Note:** This RPM is automatically installed as part of the ApplicationHA installation. However, ApplicationHA does not currently support monitoring of SAP NetWeaver in a KVM environment.
VRTSacclib	Contains the binaries for Veritas Cluster Server ACC libraries by Symantec.
VRTSvcsea	VRTSvcsea contains the binaries for Veritas DBED agents (Oracle, DB2, and Sybase).
VRTSwls9	VRTSwls9 contains the binaries for Veritas high availability agent for WebLogic Server by Symantec. **Note:** This RPM is automatically installed as part of the ApplicationHA installation. However, ApplicationHA does not currently support monitoring of WebLogic Server in a KVM environment.
VRTSvcswas	VRTSvcswas contains the binaries for Veritas high availability agent for WebSphere Application Server by Symantec.
VRTSmq6	VRTSmq6 contains the binaries for Veritas high availability agent for WebSphere MQ by Symantec.
VRTSvbs	VRTSvbs contains the binaries for Virtual Business Services by Symantec.

Appendix B

Troubleshooting Symantec ApplicationHA installation

This appendix includes the following topics:

Symantec ApplicationHA logging

This section describes how to troubleshoot common problems that may occur while installing Symantec ApplicationHA. The chapter lists the error messages and describes the associated problem. Recommended resolution is included, where applicable.

Troubleshooting issues require looking at the log files created by the various components.

ApplicationHA guest components logging

Symantec ApplicationHA guest components installer logs contain details about the installation tasks and the overall progress status. These logs are useful for resolving common installation related issues.

When installing ApplicationHA guest components by using the installapplicationha program or by using the response file option, the logs are located in the following location:

```
/opt/VRTS/install/logs
```

Note: When installing ApplicationHA guest components using the response file option, the log files are stored in the location specified inside the response file.

Agent logging on virtual machine

Symantec ApplicationHA 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/<agent name>_A.txt
```

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:

2010/08/22 18:46:44 VCS ERROR V-16-10051-6010 GenericService:Service_ClipSrv_res:online:Failed to start the service 'ClipSrv'. Error = 1058.

Veritas Operations Manager Management Server logging

The Veritas Operations Manager (VOM) Management Server logs contain error and debug information. These logs are useful for resolving issues related to tasks, communication issues between Management Server and the Managed Hosts and configuration issues.

The logs are located at the following location:

```
/var/opt/VRTSsfmcs/logs
```

To set the VOM log levels

1. Connect to the Veritas Operations Manager.
2. In the Veritas Operations Manager console, click **Settings** > **Management Server** > **General**.
3. In the Web Server Settings pane, select the appropriate level from the **Log level** dropdown list.

   You can select one of the following levels:

   - Severe
   - Warning
   - Info
   - Debug
   - Fine

Note: For the log level to be effective, after step 3, you must restart the Web server.

Installation error on Linux guests

During the installation of ApplicationHA guest components on virtual machines that are running the Linux operation system, you may receive the following error messages:

- The CPI installer for ApplicationHA fails with error message:

  ```
  Symantec ApplicationHA Guest Components Install did not complete
  successfully

     VRTSacclib rpm failed to install on nodename
     VRTSmq6 rpm failed to install on nodename
     VRTSvcswas rpm failed to install on nodename
  ```

  If you run a query to view the installed guest components (RPMs), an error message appears.
  For example, if you run the following command:

  ```
  # rpm -q  VRTSmq6
  ```

  The following error appears:

```
package VRTSmq6 is not installed
```

Resolution: The problem may not be with the installation but with the RPM database. To resolve the error message, rebuild the RPM database. For information on rebuilding the RPM database, refer the operating system documentation.
To confirm the success of rebuilding the RPM database, run the following command:

```
# rpm -q VRTSmq6
```

The following success message appears:

```
VRTSmq6-5.1.9.0-GA_GENERIC_noarch
```

- The CPI installer for ApplicationHA fails with error message:

```
CPI ERROR V-9-30-1383 The following required OS rpms
were not found on nodename:
```

Resolution: Before you run the CPI installer, ensure that all the required 32-bit compatible RPMs are installed on the virtual machine.
See "Required Linux RPMs for Symantec ApplicationHA" on page 26.

Index