

Symantec™ ApplicationHA 6.2 Installation and Upgrade Guide - Solaris on Oracle VM Server for SPARC

Symantec™ ApplicationHA Installation and Upgrade Guide

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

Product version: 6.2

Document version: 6.2 Rev 1

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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_apj@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 website.

<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

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>

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

Technical Support	4	
Chapter 1	Introducing Symantec ApplicationHA	10
	What is Symantec ApplicationHA	10
	How ApplicationHA is deployed in the Oracle VM Server for SPARC environment	11
	How Symantec ApplicationHA works with VCS	13
	How Symantec ApplicationHA detects application failures	13
	Components of the Symantec ApplicationHA setup	14
	Symantec ApplicationHA guest components for guest domains	14
	VCS in the virtualization infrastructure	14
	Symantec ApplicationHA user privileges	15
	Symantec ApplicationHA agents	15
	Licensing Symantec ApplicationHA	16
	Ensuring high availability of applications	18
	Ensuring high availability of virtualization infrastructure	20
Chapter 2	Planning to install Symantec ApplicationHA	22
	About installing Symantec ApplicationHA	22
	Support for centralized installations using the Deployment Server	24
	Requirements for installing ApplicationHA on guest domains	25
	Supported virtualization environments	25
	Supported operating systems on guest domains	26
	Required Solaris packages for Symantec ApplicationHA	26
	Supported applications	26
	Permissions requirements	27
	Ports and firewall settings for application high availability	27
	Requirements for providing high availability of virtualization environment	28
	Ports and firewall settings for virtualization infrastructure high availability	28
	Additional requirements	29

Chapter 3	Installing Symantec ApplicationHA Guest Components	30
	About preparing to install Symantec ApplicationHA guest components	30
	Performing preinstallation tasks	31
	Obtaining Symantec ApplicationHA license keys	31
	Setting the PATH variable	32
	Mounting the product disc	32
	Performing an automated preinstallation check	33
	ApplicationHA installation methods for guest components	33
	Installing Symantec ApplicationHA using the install program	34
	Installing Symantec ApplicationHA using response files	37
	Response file variables to install Symantec ApplicationHA	38
	Sample response file for installing Symantec ApplicationHA	40
Chapter 4	Performing post-installation tasks	42
	Accessing the Symantec ApplicationHA documentation	42
	Removing permissions for communication	43
Chapter 5	Upgrading Symantec ApplicationHA	44
	About upgrading Symantec ApplicationHA	44
	Upgrade matrix	45
	Upgrading Symantec ApplicationHA using the install program	46
	Upgrading Symantec ApplicationHA using response files	48
	Response file variables to Upgrade Symantec ApplicationHA	49
	Sample response file for Upgrading Symantec ApplicationHA	51
	Performing an online upgrade by using the install program	52
Chapter 6	Uninstalling Symantec ApplicationHA Guest Components	54
	Preparing to uninstall Symantec ApplicationHA	54
	Uninstalling Symantec ApplicationHA using the uninstall program	55
	Running uninstall program from the ApplicationHA media	56
	Uninstalling Symantec ApplicationHA using response files	56
	Response file variables to uninstall Symantec ApplicationHA	57
	Sample response file for uninstalling Symantec ApplicationHA	58

Chapter 7	Managing Symantec ApplicationHA licenses	59
	About managing ApplicationHA licenses	59
	Managing ApplicationHA licenses through Symantec High Availability view	60
	Managing ApplicationHA licenses from the command line	61
Appendix A	ApplicationHA installation packages	62
	ApplicationHA installation packages	62
Appendix B	Troubleshooting Symantec ApplicationHA installation	64
	Symantec ApplicationHA logging	64
	ApplicationHA guest components logging	64
	Agent logging on guest domain	65
	Veritas Operations Manager Management Server logging	65
Index		67

Introducing Symantec ApplicationHA

This chapter includes the following topics:

- [What is Symantec ApplicationHA](#)
- [Components of the Symantec ApplicationHA setup](#)
- [Symantec ApplicationHA user privileges](#)
- [Symantec ApplicationHA agents](#)
- [Licensing Symantec ApplicationHA](#)
- [Ensuring high availability of applications](#)
- [Ensuring high availability of virtualization infrastructure](#)

What is Symantec ApplicationHA

Symantec ApplicationHA provides monitoring capabilities for applications running inside logical domains in the Oracle VM Server for SPARC virtualization environment. Symantec ApplicationHA adds a layer of application awareness to the core high availability (HA) functionality offered by Symantec™ Cluster Server (VCS) in the control domain.

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), and Veritas Fencing (VxFEN). Symantec ApplicationHA has a lightweight server footprint that allows faster installation and configuration.

Key benefits include the following:

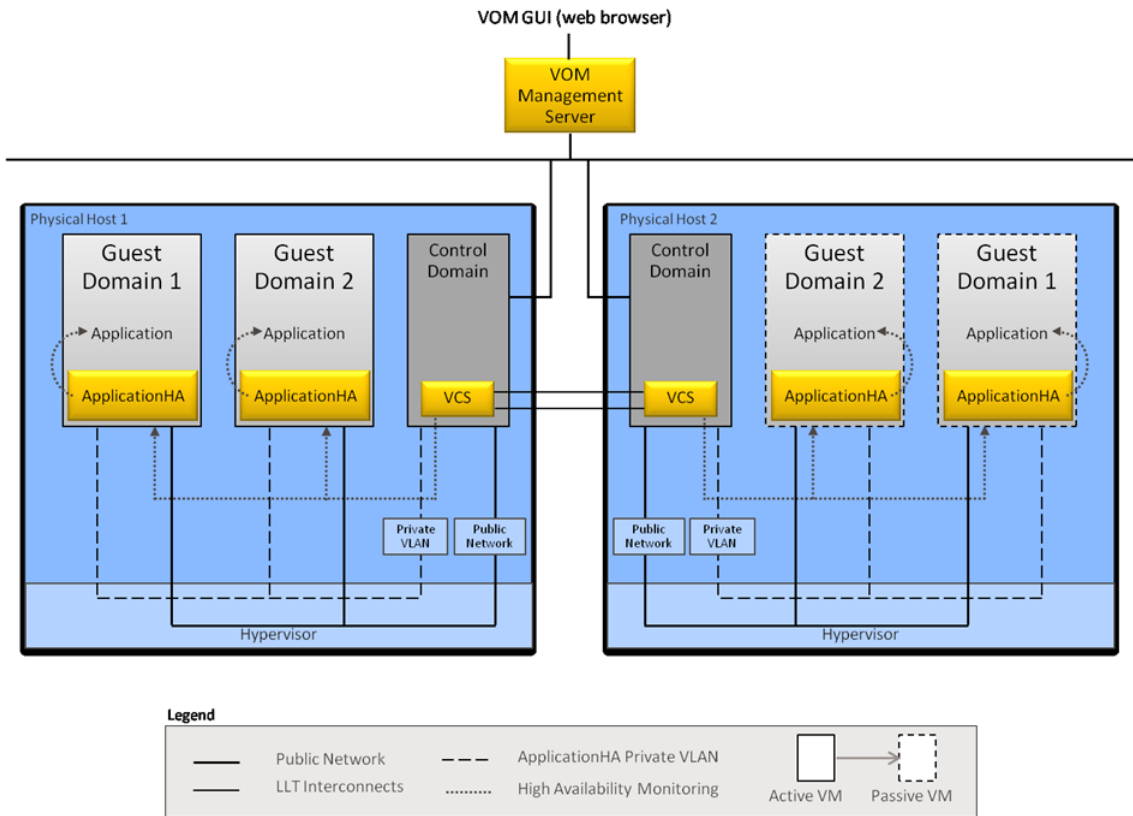
- Out of the box integration with VCS.
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside guest domains.
- High availability of the application as well as the guest domain inside which the application runs.
- Graded application fault-management responses such as:-
 - Application restart
 - ApplicationHA-initiated, graceful internal reboot (soft reboot) of a guest domain
 - VCS-initiated, external reboot (hard reboot) of guest domain
 - Failover of the guest domain to another VCS node.
- 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 Oracle VM Server for SPARC environment

Oracle VM Server for SPARC is a virtualization and partitioning solution supported on Oracle Solaris CoolThreads technology-based servers. Oracle VM Server for SPARC lets you create multiple virtual systems called logical domains, on a single physical host.

In the Oracle VM Server for SPARC virtualization environment, ApplicationHA provides high availability of applications running on guest domains. Symantec Cluster Server (VCS) provides high availability of the guest domains that run on the physical host.

The following figure illustrates how ApplicationHA and VCS are deployed in a typical Oracle VM Server for SPARC virtualization environment.



When you install the Oracle VM Server for SPARC software, the first logical domain that you create in a physical host is the control domain. For the other logical domains on the same physical host, this document uses the term “guest domains”.

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

To ensure application-aware monitoring of guest domains, you must enable VCS support for ApplicationHA (using the `enable_applicationha` script).

When you enable VCS to support ApplicationHA, a private VLAN is created between monitored guest domains and the VCS node (control domain). The private VLAN facilitates heartbeat communication between VCS in the control domain and ApplicationHA in the guest domains.

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 guest domains for high availability, see the *SFHA Virtualization Solutions Guide for Solaris*.

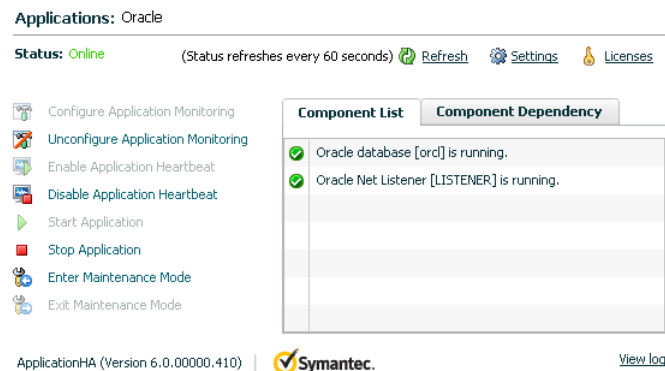
How Symantec ApplicationHA works with VCS

Symantec ApplicationHA installed in guest domains communicates directly with VCS installed in the control domain. 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 guest domain within a specified interval, VCS either restarts that guest domain or fails it over to another physical host that is part of a VCS cluster.

You can monitor an application running on a guest domain by using Veritas Operations Manager (VOM).

You can access the Symantec High Availability view from the VOM client to perform application monitoring operations on a guest domain. From this view, you configure application monitoring and then monitor and control the configured application on the guest domain. After configuring application monitoring, the Symantec High Availability tab displays the state of the application and its component dependencies.

The following figure displays the Symantec High Availability view 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 guest domains. 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 guest domain when you configure application monitoring. The Heartbeat agent sends the application heartbeat to VCS in the control domain. 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 guest domain. After the guest domain is restarted, Symantec ApplicationHA attempts to start the application and its dependent components in a predefined order.

Components of the Symantec ApplicationHA setup

Symantec ApplicationHA guest components for guest domains

The Symantec ApplicationHA guest components are installed separately on the guest domains 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 guest domain and displays it in the Symantec High Availability view of the Veritas Operations Manager MS console.

VCS in the virtualization infrastructure

Symantec Cluster Server (VCS) is installed as part of a Storage Foundation Cluster File System High Availability (SFCFSHA) stack installation on the control domain. VCS is installed on control domains in more than one physical host, to form a VCS cluster. As a result, VCS provides high availability in the infrastructure layer of the Oracle VM Server for SPARC virtualization environment on such physical hosts. VCS mainly ensures high availability of the guest domains on which ApplicationHA monitors configured applications.

For more information on how ApplicationHA and VCS are integrated in the Oracle VM Server for SPARC virtualization environment:

See “[How ApplicationHA is deployed in the Oracle VM Server for SPARC environment](#)” on page 11.

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

Symantec ApplicationHA user privileges

Symantec ApplicationHA provides a set of privileges that are available when using VOM Management Server Console to manage ApplicationHA. These privileges define the application monitoring operations that a user can perform on the guest domains. 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. For example, the Admin privilege is required for configuring application monitoring on a guest domain.

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 guest domain. 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 guest domain.
- 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 guest domain.

The agents that support Intelligent Monitoring Framework (IMF) also monitor the application components asynchronously. These agents register with the IMF notification module for component state change notifications. IMF-enabled agents lead to significant performance benefits in terms of system resource utilization and quicker fault detection.

For more information on Intelligent Monitoring Framework see the *Symantec ApplicationHA User's Guide*

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 guest domains.
For more details about the infrastructure agents, refer to the *Symantec Cluster Server Bundled Agents Reference Guide (Solaris)*.
- 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.

Licensing Symantec ApplicationHA

Symantec ApplicationHA is a licensed product. Licensing Symantec ApplicationHA is applicable to ApplicationHA guest components and is based on the operating systems running on the guests.

You have the option to install Symantec products without a license key. Installation without a license does not eliminate the need to obtain a license. A software license is a legal instrument governing the usage or redistribution of copyright protected

software. The administrator and company representatives must ensure that a server or cluster is entitled to the license level for the products installed. Symantec reserves the right to ensure entitlement and compliance through auditing.

If you encounter problems while licensing this product, visit the following Symantec Licensing support site:

http://www.symantec.com/products-solutions/licensing/activating-software/detail.jsp?detail_id=licensing_portal

The Symantec ApplicationHA installer prompts you to select one of the following licensing methods:

- Install a license key for the product and features that you want to install.
When you purchase a Symantec product, you receive a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased.
- Continue to install without a license key.
The installer prompts for the product modes and options that you want to install, and then sets the required product level.
Within 60 days of choosing this option, you must install a permanent license key corresponding to the license level entitled. If you do not comply with the terms, continuing to use the Symantec product is a violation of your End User License Agreement, and results in warning messages
For more information about keyless licensing, see the following URL:
<http://go.symantec.com/sfhakeyless>

If you upgrade to this release from a prior release of Symantec ApplicationHA, and the existing license key has expired, the installer asks whether you want to upgrade the key to the new version.

If you upgrade with the product installer, or if you install or upgrade with a method other than the product installer, you must do one of the following to license the products:

- Run the `vxkeyless` command to set the product level for the products you have purchased.
See “[Managing ApplicationHA licenses from the command line](#)” on page 61.
This option also requires that you manage the server or cluster with a management server.
- Use the `vxlicinst` command to install a valid product license key for the products you have purchased.
See “[Managing ApplicationHA licenses from the command line](#)” on page 61.

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

See [“About managing ApplicationHA licenses”](#) on page 59.

Ensuring high availability of applications

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

- Install ApplicationHA on the guest domain

Note: Ensure that Managed Host (MH) binaries of Veritas Operations Manager 6.0 or later are installed as part of the ApplicationHA installation.

- Add the guest domain as a managed host to Veritas Operations Manager (VOM) MS
- Configure application monitoring on the guest domain.


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.

Note: To ensure that you install and configure the appropriate version of each product or component in the steps below, carefully review the indicated documents. The most recent version of VOM MS is recommended.

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 guest domains.**




Refer ApplicationHA Installation Guide

4.  **Add guest domains and control domains as managed hosts to VOM.**



Refer ApplicationHA User's Guide

5.  **Configure application monitoring on the guest domains.**



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 guest domains and fail over the guest domains in case of application failures or guest domain failures. To ensure high availability of the virtualization environment, perform the following steps:

- Install SFCFSHA on the control domain.
- Enable ApplicationHA capabilities in underlying VCS in the control domain.
- Install ApplicationHA on the guest domain.
- Add guest domain and control domain as managed hosts to Veritas Operations Manager (VOM) Management Server

Note: Ensure that Veritas Operations Manager 6.0 Managed Host (MH) or later binaries are installed on both the guest domain and control domain.

- Configure application monitoring on the guest domain.

The following figure illustrates the workflow for ensuring high availability of the applications running inside the guest domain and the virtualization infrastructure. The figure also indicates the corresponding documents that you must refer for detailed instructions at each step. Review the documents carefully to ensure you install and configure the appropriate versions of each component. The most recent version of VOM MS is recommended

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 control domain.**
  Refer SFCFSHA Installation Guide
4.  **Set up virtualization environment on the control domain.**
  Refer SFHA Solutions Virtualization Guide
5.  **Enable VCS for ApplicationHA 6.0 on the control domain.**
  Refer ApplicationHA User's Guide
6.  **Install ApplicationHA 6.0 on the guest domains.**
  Refer ApplicationHA Installation Guide
7.  **Add guest domains and control domains as managed hosts to VOM.**
  Refer ApplicationHA User's Guide
8.  **Configure application monitoring on the guest domains.**
  Refer Application specific Agent Guide
9.  **Monitor application.**
  Refer ApplicationHA User's Guide

Planning to install Symantec ApplicationHA

This chapter includes the following topics:

- [About installing Symantec ApplicationHA](#)
- [Support for centralized installations using the Deployment Server](#)
- [Requirements for installing ApplicationHA on guest domains](#)
- [Requirements for providing high availability of virtualization environment](#)
- [Additional requirements](#)

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 6.0 or later	Download the installer for VOM Management Server 6.0 or later. The installer is available here: http://sort.symantec.com
Install Symantec ApplicationHA guest components for guest domains	Install the Symantec ApplicationHA guest components on the guest domains where you want to monitor applications. Symantec ApplicationHA guest components include ApplicationHA agents and configuration wizards.

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

Task	Description
Add required guest domains to VOM as managed hosts	In the Home page of the VOM Management Server console, from the Settings menu, add the guest domains where you want to monitor applications, as managed hosts in VOM.
Configure application monitoring on the guest domains	In the Server perspective of the Management Server console, right-click the guest domain (managed host), and select Manage ApplicationHA to launch the ApplicationHA management window. In the window, click Configure Application Monitoring to launch the application monitoring configuration wizard.
Administer application monitoring on the guest domains	Click the appropriate links in the ApplicationHA management window, 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 6.0 or later	Download the latest installer for VOM Management Server (6.0 or later). The installer is available here: http://sort.symantec.com
Install SFCFSHA on the control domain	SFCFSHA enables you to ensure high availability of the virtualization infrastructure in terms of restart and failover of failed guest domains.
Enable VCS support for ApplicationHA	Run the enable_applicationha script from /opt/VRTSvcs/bin/utills path on each control domain. The enable_applicationha script configures the infrastructure settings. It also enables communication between VCS in the control domain and ApplicationHA in the guest domains.

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

Task	Description
Install Symantec ApplicationHA guest components for guest domains	Install the Symantec ApplicationHA guest components on the guest domains where you want to monitor applications. Symantec ApplicationHA guest components include ApplicationHA agents and configuration wizards.
Add required guest domains and control domain to VOM as managed hosts	In the Add the guest domains where you want to monitor applications, to the list of managed hosts in VOM. You may optionally add the control domains to VOM. This allows you to co-relate a guest domain with the control domain hosting it.
Configure application monitoring on the guest domains	In the Server perspective of the Management Server console, right-click the guest domain (managed host), and select Manage ApplicationHA to launch the ApplicationHA management window. In the ApplicationHA management window, click Configure Application Monitoring to launch the Application Monitoring Configuration Wizard.
Administer application monitoring on the guest domains	Click the appropriate links in the ApplicationHA tab, to perform administrative actions on configured applications.

Support for centralized installations using the Deployment Server

If your data center deploys multiple storage and high availability management products from Symantec, you can leverage the Deployment Server component for centralized installation management.

Deployment Server lets you store multiple release images in one central location and deploy them to systems of any supported platform. You can load and store product binaries for Symantec products dating back to version 5.1 in a central repository.

You can use the Deployment Server for performing the following tasks:

- Version checking
- Release image management

- Install or upgrade systems
- Update metadata and preferences

ApplicationHA 6.1 or later supports the Deployment Server feature for managing centralized installations and upgrades.

For detailed information on installing and leveraging Deployment Server, see the *Symantec Cluster Server (VCS) Installation Guide*.

Requirements for installing ApplicationHA on guest domains

You can install Symantec ApplicationHA Guest Components on guest domains running Solaris. The guest domain 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 guest domains in an Oracle VM Server for SPARC virtualization environment. The following versions are supported:

Table 2-3 Supported versions

Server version
Oracle VM Server for SPARC 2.0
Oracle VM Server for SPARC 2.1
Oracle VM Server for SPARC 2.2
Oracle VM Server for SPARC 3.0
Oracle VM Server for SPARC 3.1

Note: Ensure that you upgrade to the latest firmware version that is applicable to your server.

Refer to Oracle VM Server for SPARC Release Notes, for more information on the required firmware versions.

Supported operating systems on guest domains

This section lists the supported operating systems for Symantec ApplicationHA 6.2.

[Table 2-4](#) shows the supported operating systems for this release. The indicated operating systems apply to both control domain as well as guest domains.

Table 2-4 Supported guest operating systems

Operating systems	Levels	Chipsets
Solaris 10	Update 9, 10, and 11	SPARC

Required Solaris packages for Symantec ApplicationHA

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

[Table 2-5](#) lists the packages that ApplicationHA requires for a given Solaris operating system.

Table 2-5 Required packages

Operating system	Required packages
Solaris SPARC 10	The following Solaris DHCP packages are required: <ul style="list-style-type: none"> ■ SUNWdhcsu ■ SUNWdhcsr

Supported applications

[Table 2-6](#) lists the applications that ApplicationHA Agent Pack currently supports on guest domains.

Table 2-6 ApplicationHA Agent Pack supported applications

Application	Version	Document
Oracle Database	10gR2, 11gR1, and 11gR2; 12cR1	<i>Symantec ApplicationHA Agent for Oracle Configuration Guide</i>

Table 2-6 ApplicationHA Agent Pack supported applications (*continued*)

Application	Version	Document
Apache HTTP server	1.3, 2.0, and 2.2. Also supports IBM HTTP Server 7.x and 8.x.	<i>Symantec ApplicationHA Agent for Apache HTTP server Configuration Guide</i>

Note: Alternatively, you can use the Custom Application wizard to configure and monitor applications that are not listed in the above support matrix. For more information on configuring the custom application, refer to the *Symantec ApplicationHA Generic Agent Configuration Guide*.

Permissions requirements

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

- You must have root privileges on the guest domain where you install the guest components.
In case of remote installation, you must also have root privileges on all the guest domains 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 guest domains.

[Table 2-7](#) displays the services and ports used by ApplicationHA.

Table 2-7 Services and ports used by Symantec ApplicationHA

Component Name	Port	Settings	Description
Veritas Storage Foundation Messaging Service (xprtId)	5634	Allow inbound and outbound	Used for communications between the VOM Console and the guest domains.
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 on the control domain
 Refer to *Symantec Storage Foundation Cluster File System HA Installation Guide - Solaris*
- Review the settings of the virtualization environment for which you want to provide high availability
 Refer to *Symantec Storage Foundation and High Availability Solutions Virtualization Guide - Solaris*
- Enable ApplicationHA capabilities for underlying VCS.
 Refer to *Symantec ApplicationHA User's Guide - Solaris on Oracle VM Server for SPARC*

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 guest domains.

[Table 2-8](#) displays the services and ports used by ApplicationHA for providing high availability of the virtualization environment.

Table 2-8 Services and ports used by Symantec ApplicationHA

Component Name	Port	Settings	Description
Veritas Storage Foundation Messaging Service (xprtId)	5634	Allow inbound and outbound	Used for communications between the VOM Console host machine and the guest domains.
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 2-8 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 control domain and ApplicationHA in the guest domain

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 guest domains. 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 guest domains.
- Symantec ApplicationHA license
You can install ApplicationHA with a keyless license. You can alternatively install ApplicationHA by specifying a valid license key. For details: See [“About managing ApplicationHA licenses”](#) on page 59.
- When installing Symantec ApplicationHA, ensure that there are no parallel installations in progress.

Installing Symantec ApplicationHA Guest Components

This chapter includes the following topics:

- [About preparing to install Symantec ApplicationHA guest components](#)
- [Performing preinstallation tasks](#)
- [ApplicationHA installation methods for guest components](#)
- [Installing Symantec ApplicationHA using the install program](#)
- [Installing Symantec ApplicationHA using response files](#)

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 25.
- See [“Supported operating systems on guest domains”](#) on page 26.
- See [“Required Solaris packages for Symantec ApplicationHA”](#) on page 26.
- See [“Permissions requirements”](#) on page 27.
- See [“Ports and firewall settings for application high availability”](#) on page 27.

- See “[Additional requirements](#)” on page 29.

Performing preinstallation tasks

[Table 3-1](#) lists the tasks you must perform before proceeding to install ApplicationHA.

Table 3-1 Preinstallation tasks

Task	Reference
If you do not want to use keyless licensing, obtain license keys	See “ Obtaining Symantec ApplicationHA license keys ” on page 31.
Set the PATH variable	See “ Setting the PATH variable ” on page 32.
Mount the product disc	See “ Mounting the product disc ” on page 32.
Verify the system before installation	See “ Performing an automated preinstallation check ” on page 33.

Obtaining Symantec ApplicationHA license keys

If you decide not to use the keyless licensing feature, you must obtain and install a license key for ApplicationHA.

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:

http://www.symantec.com/products-solutions/licensing/activating-software/detail.jsp?detail_id=licensing_portal

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 **Get Help** link at the site for contact information and for useful links.

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 Solaris SPARC operating system:

```
# cd cdrom_root/sol10_sparc/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 installation program.

See [“Mounting the product disc”](#) on page 32.

- 2 Start the preinstallation check:

```
# ./installapplicationha -precheck system1
```

The program proceeds in a non-interactive mode to examine the system for licenses, packages, 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 guest domains running the Solaris operating system:

Table 3-2 ApplicationHA installation methods

Method	Description
Interactive installation using the installation 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 installapplicationha62 program (installapplicationha program if installed directly from the installation media).
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 guest domains.
Manual installation using the Solaris commands and utilities	You can install ApplicationHA using the operating system <code>pkgadd</code> command.

Installing Symantec ApplicationHA using the install program

Note: The system from where you install ApplicationHA must run the same Solaris distribution as the target guest domains.

Perform the following steps to install ApplicationHA:

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 32.

- 2 Navigate to the folder that contains the installation program for the Solaris SPARC operating system:

```
# cd cdrom_root/sol110_sparc/applicationha
```

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

```
# ./installapplicationha62
```

- 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 guest domains”](#) 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 Solaris packages 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 packages already exist on a system.
If the current version of any packages exists, the install program removes the packages from the installation list for the system.
- 6 Review the list of packages that the install program would install on the guest domain.
- The install program installs the ApplicationHA packages on the system that you specified in step 5. For example, system1.

7 Select the license type.

- 1) Enter a valid license key
- 2) Enable keyless licensing and complete system licensing later

How would you like to license the system? [1-2,q] (2)

Based on what license type you want to use, enter one of the following:

- 1 You must have a valid license key. Enter the ApplicationHA license key at the prompt:

 Enter an ApplicationHA license key: [b,q,?]
 XXXX-XXXX-XXXX-XXXX-XXXX

- 2 The keyless license option enables you to install ApplicationHA without entering a key. However, to ensure compliance, keyless licensing requires that you manage the systems with a management server.

 For more information, go to the following website:
 <http://go.symantec.com/sfhakeyless>

 Note that this option is the default.

The install program registers the license and completes the installation process.

- 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 packages 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 37.

Installing Symantec ApplicationHA using response files

When you install ApplicationHA on a guest domain using the install program, it generates a response file. You can use the response file to install ApplicationHA on other guest domains. 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 guest domains”](#) on page 25.
- 2 Make sure the preinstallation tasks are completed.
See [“Performing preinstallation tasks”](#) on page 31.
- 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 38.
See [“Sample response file for installing Symantec ApplicationHA”](#) on page 40.
- 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/

# ./installapplicationha62 -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 packages. (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 APPLICATIONHA62. (Required)
CFG{keys} {system}	Scalar	List of keys to be registered on the system. (Optional)
CFG{opt}{vxkeyless}	Scalar	Specifies whether you want to install a keyless license. CFG{opt}{vxkeyless} = 1 indicates that you want to install a keyless license. (Optional)
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 <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of the <i>ssh</i> 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 packages. 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 packages 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 <i>logpath</i> 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 38.

For keyless licensing:

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

$CFG{accepteula}=1;
$CFG{opt}{configure}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{opt}{updatekeys}=1
$CFG{opt}{vxkeyless}=1;
$CFG{prod}="APPLICATIONHA62";
$CFG{systems}=[ qw(system1) ];
$CFG{uploadlogs}=1;
```

For permanent license key:


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

$CFG{accepteula}=1;
$CFG{keys}{system1}="LICENSEKEY";
$CFG{opt}{configure}=1;
$CFG{opt}{install}=1;
$CFG{opt}{installallpkgs}=1;
$CFG{prod}="APPLICATIONHA62";
$CFG{systems}=[ qw(system1) ];
$CFG{uploadlogs}=1;
```

Performing post-installation tasks

This chapter includes the following topics:

- [Accessing the Symantec ApplicationHA documentation](#)
- [Removing permissions for communication](#)

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 guest domain to make it available for reference.

To make the ApplicationHA documentation accessible from guest domains

- 1 Navigate to the folder that contains the PDF version of the documents for the Solaris SPARC operating system:

```
# cd cdrom_root/sol10_sparc/docs/applicationha
```

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

```
# cp -rp docs /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 guest domains and restore the connections to the public network.

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

Upgrading Symantec ApplicationHA

This chapter includes the following topics:

- [About upgrading Symantec ApplicationHA](#)
- [Upgrade matrix](#)
- [Upgrading Symantec ApplicationHA using the install program](#)
- [Upgrading Symantec ApplicationHA using response files](#)
- [Performing an online upgrade by using the install program](#)

About upgrading Symantec ApplicationHA

Upgrading Symantec ApplicationHA involves upgrade of the guest components in the guest domain, Symantec Cluster Server (VCS) in the physical host.

You can either upgrade VCS in the physical host first, and then upgrade ApplicationHA on the guest domain, or vice versa.

Before you begin to upgrade the guest components, perform the following general pre-upgrade tasks:

- Back up all your data.
- Ensure that you meet the required prerequisites.
See [“About installing Symantec ApplicationHA”](#) on page 22.
- Review the licensing details.
See [“Licensing Symantec ApplicationHA ”](#) on page 16.
- Review the supported upgrade matrix
See [“Upgrade matrix”](#) on page 45.

[Table 5-1](#) provides the details for upgrading ApplicationHA components.

Table 5-1 ApplicationHA upgrade details

Component	Upgrade details
Guest	<p>You can upgrade the guest components by using any of the following methods:</p> <p>For upgrading by using the installer (interactive mode)</p> <p>See “Upgrading Symantec ApplicationHA using the install program” on page 46.</p> <p>For upgrading by using response files</p> <p>See “Upgrading Symantec ApplicationHA using response files” on page 48.</p>

Note: After you upgrade the guest components, ensure that you download and install the required application agents from the latest Agent Pack on [SORT](#).

Upgrade matrix

[Table 5-2](#) provides the supported scenarios for upgrading ApplicationHA Guest Components.

Table 5-2 Supported upgrade scenarios for ApplicationHA Guest Components.

Upgrade from	Upgrade to	Operating system
ApplicationHA 6.0 Guest Components	ApplicationHA 6.2 Guest Components	Solaris 10
ApplicationHA 6.1 Guest Components	ApplicationHA 6.2 Guest Components	Solaris 10
ApplicationHA 6.1.1 Guest Components	ApplicationHA 6.2 Guest Components	Solaris 10

Note: For the upgrade matrix for Symantec Cluster Server in the physical host, see the *Symantec Cluster Server Installation Guide*.

Upgrading Symantec ApplicationHA using the install program

Perform the following steps to upgrade ApplicationHA:

Note: The system from where you upgrade ApplicationHA must run the same Solaris SPARC distribution as the target guest domains.

To upgrade 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 32.

- 2 Navigate to the folder that contains the installation program for the Solaris SPARC operating system:

```
# cd cdrom_root/sol110_sparc/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 guest domains”](#) 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 Solaris packages 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 packages already exist on a system.
If the current version of any packages exists, the install program removes the packages from the installation list for the system.
- 6 Review the list of packages that the install program would upgrade on each guest domain.
- The install program upgrades the ApplicationHA packages on the system/s that you specified in step 5. For example, system1.
- 7 Register your license key.

Note: If a valid license key exists, the installer does not display the following prompt.

```
Enter an ApplicationHA license key: [b,q,?]
XXXX-XXXX-XXXX-XXXX-XXXX
```

The install program registers the license, and completes the upgrade process.

Note: To specify keyless licensing, follow the workaround provided in the *Symantec ApplicationHA Release Notes* for incidents 3335745 and 3336308.

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

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

summary file	Lists the packages that are upgrade on each system.
log file	Details the entire upgrade.
response file	Contains the upgrade information that can be used to perform unattended or automated installations on other systems. See “Upgrading Symantec ApplicationHA using response files” on page 48.

Upgrading Symantec ApplicationHA using response files

When you upgrade ApplicationHA on a guest domain using the install program, it generates a response file. You can use the response file to upgrade ApplicationHA on other guest domains. You can also generate the response file using the `-makeresponsefile` option on the install program.

To upgrade ApplicationHA using response files

- 1 Make sure the system where you want to upgrade ApplicationHA meet the installation requirements.
 See [“Requirements for installing ApplicationHA on guest domains”](#) on page 25.
- 2 Make sure the preinstallation tasks are completed.
 See [“Performing preinstallation tasks”](#) on page 31.
- 3 Create a response file on the system where you want to run the installer.
 See [“Response file variables to Upgrade Symantec ApplicationHA”](#) on page 49.
 See [“Sample response file for Upgrading Symantec ApplicationHA”](#) on page 51.

Caution: Make sure that the response file is readable only to the root user because it may contain local user passwords.

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

For example, with the Solaris SPARC 10 disc, use the following command:

```
# cd /cdrom_root/sol10_sparc/applicationha
```

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

```
# ./installapplicationha -responsefile /root/response_file
```

Where */root/response_file* is the response file’s full path name.

Response file variables to Upgrade Symantec ApplicationHA

[Table 5-3](#) lists the response file variables that you can define to upgrade ApplicationHA.

Table 5-3 Response file variables specific to upgrading Symantec ApplicationHA

Variable	List or Scalar	Description
CFG{accepteula}	Scalar	Specifies whether you agree with EULA.pdf on the media. (Required)

Table 5-3 Response file variables specific to upgrading Symantec ApplicationHA (continued)

Variable	List or Scalar	Description
CFG{opt}{upgrade}	Scalar	Upgrades Symantec ApplicationHA packages. (Required)
CFG{systems}	List	Name of the system on which the product is to be installed. (Required)
CFG{prod}	Scalar	Defines the product to be installed. The value is APPLICATIONHA62. (Required)
CFG{opt}{updatekeys}	Scalar	
CFG{opt}{vxkeyless}	Scalar	Specifies whether you want to install a keyless license. CFG{opt}{vxkeyless} = 1 indicates that you want to install a keyless license. (Optional)
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 <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of the <i>ssh</i> 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 packages that are needed during the install. The default location is <i>/var/tmp</i> . (Optional)

Table 5-3 Response file variables specific to upgrading Symantec ApplicationHA (continued)

Variable	List or Scalar	Description
CFG{opt}{logpath}	Scalar	<p>Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs.</p> <p>Note: The install program copies the response files and summary files also to the specified <i>logpath</i> location.</p> <p>(Optional)</p>

Sample response file for Upgrading Symantec ApplicationHA

Review the response file variables and their definitions.

See [“Response file variables to Upgrade Symantec ApplicationHA”](#) on page 49.

For permanent license:

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

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="APPLICATIONHA62";
$CFG{systems}=[ qw(system1) ];
$CFG{keys}{'systemname'}=["LICENSEKEY"];
$CFG{uploadlogs}=1;
```

For keyless license:

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

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{opt}{installall pkgs}=1;
$CFG{prod}="APPLICATIONHA62";
$CFG{systems}=[ qw(system1) ];
```

```
$CFG{uploadlogs}=1;  
$CFG{opt}{vxkeyless}=1;
```

Performing an online upgrade by using the install program

An online upgrade allows you to upgrade to a newer Symantec ApplicationHA version without involving any downtime for the applications monitored by ApplicationHA. You can use the product installer to perform an online upgrade.

Before you choose to perform an online upgrade, consider the following limitations of an online upgrade:

- Online upgrade is available only for Symantec Cluster Server (VCS) and ApplicationHA. If you have Storage Foundation, SFHA, SFCFSHA, or any other solution with Veritas Volume Manager (VxVM) and Veritas File System (VxFS) installed, the online upgrade process is not supported.
- ApplicationHA does not monitor high availability of the applications when the online upgrade is in progress.

To perform an online upgrade

- 1 Log in as super user and mount the product disc.
- 2 Start the installer.

```
# ./installer
```

The installer starts the product installation program with a copyright message.

The installer then specifies where it creates the logs. Note the directory name and path where the logs get stored.

- 3 From the opening Selection Menu, choose: G for "Upgrade a Product."

The system prompts you to select the method by which you want to upgrade the product.

- 4 Choose **3** for Online Upgrade from the upgrade options.

- 5 After selecting the online upgrade method, enter the system name where you want perform the online upgrade.

The installer performs some verification checks and asks the following question:

```
Online upgrade supports application zero downtime.  
Would you like to perform online upgrade on the  
system? [y,n,q] (y)
```

- 6 Enter **Y** to initiate the online upgrade.

Note: To exit the installer, select **q** or to cancel the upgrade, select **n** and select any other system to upgrade at this step.

The installer runs some verification checks on the nodes and asks if you agree with the terms of the End User License Agreement.

- 7 Enter **Y** to agree and continue.

The installer lists the packages to upgrade.

- 8 The installer asks whether you want to stop the ApplicationHA processes.

Enter **Y** to stop the ApplicationHA process. The installer stops the ApplicationHA processes, uninstalls packages, reinstalls or upgrade packages, reconfigures ApplicationHA, and starts the processes.

Uninstalling Symantec ApplicationHA Guest Components

This chapter includes the following topics:

- [Preparing to uninstall Symantec ApplicationHA](#)
- [Uninstalling Symantec ApplicationHA using the uninstall program](#)
- [Running uninstall program from the ApplicationHA media](#)
- [Uninstalling Symantec ApplicationHA using response files](#)

Preparing to uninstall Symantec ApplicationHA

Before you uninstall ApplicationHA from any guest domain:

- 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 guest domains, using the `uninstallapplicationha62` program:

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

If you cannot meet the prerequisites, you will not be able to remotely uninstall ApplicationHA. You must run the `uninstallapplicationha62` program on the guest domain from which you want to uninstall ApplicationHA.

The `uninstallapplicationha62` program removes all ApplicationHA packages.

The following section describes how to uninstall ApplicationHA using the `uninstallapplicationha62` program. The example procedure uninstalls ApplicationHA from the selected or provided guest domain.

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 uninstall program.

```
# cd /opt/VRTS/install  
# ./uninstallapplicationha62
```

The program specifies the directory where the logs are created. The program displays a copyright notice and a description of the guest domain.

- 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 packages 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 packages.

Note that the location of the summary and log files created by uninstall program will be printed after removing all the packages.

Running uninstall program from the ApplicationHA media

You may need to use the uninstall program on the ApplicationHA 6.2 media in one of the following cases:

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

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

```
/mnt/cdrom/sol10_sparc/applicationha
```

For information on how to use the `uninstallapplicationha62` program:

See [“Uninstalling Symantec ApplicationHA using the uninstall program”](#) on page 55.

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 guest domain.

To perform automated ApplicationHA uninstallation

- 1 Make sure that you are prepared to uninstall ApplicationHA.
See [“Preparing to uninstall Symantec ApplicationHA”](#) on page 54.
- 2 Copy the response file to the system where you want to uninstall ApplicationHA.
See [“Sample response file for uninstalling Symantec ApplicationHA”](#) on page 58.
- 3 Edit the values of the response file variables as necessary.
See [“Response file variables to uninstall Symantec ApplicationHA”](#) on page 57.
- 4 Start the uninstallation from the system to which you copied the response file.
For example:

```
# cd /opt/VRTS/install/  
  
# ./uninstallapplicationha62 -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 packages. (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 APPLICATIONHA62. (Required)
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 <i>rsh</i> must be used instead of <i>ssh</i> as the communication method between systems. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the packages that are needed during the uninstall. The default location is <i>/var/tmp</i> . (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is <i>/opt/VRTS/install/logs</i> . Note: The install program copies the response files and summary files also to the specified <i>logpath</i> 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 57.

```
#  
# Configuration Values:  
#  
our %CFG;  
  
$CFG{opt}{uninstall}=1;  
$CFG{prod}="APPLICATIONHA62";  
$CFG{systems}=[ qw(system1) ];
```

Managing Symantec ApplicationHA licenses

This chapter includes the following topics:

- [About managing ApplicationHA licenses](#)
- [Managing ApplicationHA licenses through Symantec High Availability view](#)
- [Managing ApplicationHA licenses from the command line](#)

About managing ApplicationHA licenses

If you are an existing ApplicationHA customer, you can upgrade to Application 6.1 or later, using the keyless licensing feature.

You can also install an additional license key for ApplicationHA using one of the following methods:

Note: If you are an existing ApplicationHA customer, you must use only the command-line methods described in this chapter to avail of keyless licensing or remove keyless licensing. If you are a new ApplicationHA customer, keyless licensing is enabled by default. You can use both GUI-based and command line-based methods to further manage your ApplicationHA licenses.

- When you run the CPI installer to install or upgrade ApplicationHA, you can specify a new license key.
- You can also install a valid license key or enable the keyless licensing feature from the command line.
See [“Managing ApplicationHA licenses from the command line”](#) on page 61.

- Connect to the Veritas Operations Manager console and in the Server perspective, in the left pane expand **Manage**, and in the related Organization or under Uncategorized Hosts, navigate to the guest domain where you want to update the licenses. Right-click the guest domain and from the context menu, select **Manage ApplicationHA** to launch the **Symantec High Availability** view and click **Licenses**. Use this path to manage licenses for the local guest domain.

Note: Keyless licensing is presently not supported through this method. You can install a keyless license only through the command line.

- You can also access the Symantec High Availability view from an Internet browser by using the following URL:
https://<IP_or_Hostname>:5634/vcs/admin/application_health.html?priv=ADMIN
 Where IP_or_Hostname refers to the IP address or host name of the virtual name where you want to manage an ApplicationHA license.

Managing ApplicationHA licenses through Symantec High Availability view

Perform the following steps to manage ApplicationHA licenses through the Symantec High Availability view.

Note: You can use this method to specify a permanent license key, not keyless licensing.

To manage the ApplicationHA licenses

- 1 Connect to the Veritas Operations Manager Management Server (VOM MS).
- 2 In the VOM MS Console, select the Server perspective and expand **Manage** in the left pane.
- 3 Expand the Organization, or **Uncategorized Hosts** to navigate to the guest domain.
- 4 Right-click the required guest domain, and then click **Manage ApplicationHA**. The Symantec High Availability view appears.
- 5 In the Symantec High Availability view, click **Licenses**.
- 6 On the License Management panel, enter the permanent license key in the **Enter license key** text box and then click **Add**.
- 7 Click **Close**.

Managing ApplicationHA licenses from the command line

To view an existing license, or add a license key, or remove an existing license, including keyless licensing, use the appropriate commands as follows:

To view an existing license:

```
/opt/VRTS/bin/vxlicrep
```

To install a valid license key:

```
/opt/VRTS/bin/vxlicinst
```

To use keyless licensing

1 Navigate to the following directory:

```
# cd /opt/VRTSvlic/bin
```

2 View the current setting for all the product levels enabled for keyless licensing.

```
# ./vxkeyless -v display
```

3 View the possible settings for the product level for keyless licensing.

```
# ./vxkeyless displayall
```

4 Enable ApplicationHA keyless licensing along with the other products.

```
# ./vxkeyless set prod_levels
```

Where *prod_levels* is a comma-separated list of keywords. Use the keywords returned by the `vxkeyless displayall` command.

If you want to remove keyless licensing and add a valid license key, you must clear the keyless licenses.

Warning: Clearing the keys disables the ApplicationHA product until you install a new key or set a new product level for keyless licensing.

To remove a keyless license

1 View the current setting for the product license level.

```
# ./vxkeyless -v display
```

2 If there are keyless licenses installed, remove all keyless licenses:

```
# ./vxkeyless [-q] set NONE
```

ApplicationHA installation packages

This appendix includes the following topics:

- [ApplicationHA installation packages](#)

ApplicationHA installation packages

[Table A-1](#) shows the package name and contents for each Symantec Cluster Server package.

Table A-1 Symantec ApplicationHA packages

package	Contents
VRTSsamf	Contains the binaries for the Required Veritas Asynchronous Monitoring Framework kernel driver functionality for all the supported IMF-aware agents.
VRTSvlic	Contains the binaries for Symantec License Utilities.
VRTSperl	Contains Symantec Perl 5.10.0 redistribution by Symantec.
VRTSspt	Contains the binaries for Software Support Tools by Symantec.
VRTSsfmh	Contains the binaries for Symantec Storage Foundation Managed Host.

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

package	Contents
VRTSvcs	<p>VRTSvcs contains the following components:</p> <ul style="list-style-type: none">■ The binaries for Symantec Cluster Server.■ The binaries for Symantec Cluster Server manual pages.■ The binaries for Symantec Cluster Server English message catalogs.■ The binaries for Symantec Cluster Server utilities. These utilities include security services.
VRTSvcsag	<p>Contains the binaries for Symantec Cluster Server bundled agents by Symantec.</p>
VRTSvcsvmw	<p>Contains the ApplicationHA guest domain wizards for application monitoring configurations by Symantec.</p>
VRTSvcssea	<p>VRTSvcssea contains the binaries for Symantec DBED agents (Oracle, DB2, and Sybase).</p>
VRTSvbs	<p>VRTSvbs contains the binaries for Virtual Business Services by Symantec.</p>
VRTSsfpci62	<p>VRTSsfpci62 contains the binaries for the Symantec Storage Foundation Common Product Installer. This mandatory package contains the scripts that perform the following:</p> <ul style="list-style-type: none">■ Installation■ Configuration■ Upgrade■ Uninstallation■ Adds nodes■ Removes nodes <p>You can use this script to simplify the native operating system installations.</p>

Troubleshooting Symantec ApplicationHA installation

This appendix includes the following topics:

- [Symantec ApplicationHA logging](#)
- [Veritas Operations Manager Management Server logging](#)

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 installation 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 guest domain

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:

- Info
- Debug
- Warning

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

Index

A

- about
 - upgrade 44
- ApplicationHA
 - about 10
 - deployment 11

C

- client license 16

D

- Deployment Server
 - Using the 24

F

- firewall settings
 - for application high availability 27
 - for virtualization infrastructure 28

I

- installation
 - methods 33
 - of Symantec ApplicationHA
 - using install program 34
 - using response files 37
 - packages 62
 - preparing 30
- installing Symantec ApplicationHA using install program 34
- installing Symantec ApplicationHA using response files 37, 48

L

- license key 16
- License management
 - local machine; Symantec High Availability view 60
- licensing 16

Logs

- agents 65
- installer 64
- set VOM log levels 65
- VOM Management Server 65

O

- obtaining license keys 31

P

- port settings
 - for application high availability 27
 - for virtualization infrastructure 28
- pre-installation
 - checking the systems 33
 - obtaining license keys 31
 - setting PATH variable 32
- pre-installation checks 33
- product licensing 16

R

- response files
 - generate a response file 37, 48
 - installing Symantec ApplicationHA
 - sample response file 40
 - variables 38, 49
 - uninstalling Symantec ApplicationHA
 - sample response file 58
 - variables 57
 - upgrading Symantec ApplicationHA
 - sample response file 51

S

- setting PATH variable 32
- Symantec ApplicationHA
 - installation using install program 34
 - installation using response file 37
 - license 16
 - uninstallation using response file 56
 - upgrade using install program 46

Symantec ApplicationHA *(continued)*
upgrading using response file 48

U

uninstallation
 using response files 56
uninstalling Symantec ApplicationHA
 removing packages 55
upgrade
 matrix 45
 Symantec ApplicationHA
 using install program 46
upgrade scenarios
 ApplicationHA Guest Components. 45
upgrade Symantec ApplicationHA using install
 program 46
upgrading
 Symantec ApplicationHA
 using response files 48