

Symantec™ ApplicationHA 6.1 Installation and Upgrade Guide - Linux on VMware

Symantec™ ApplicationHA 6.1 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: 6.1

Document version: 6.1 Rev 2

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_apac@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America [supportolutions@symantec.com](mailto: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
	Components of Symantec ApplicationHA 11
	Symantec High Availability Console 11
	Symantec ApplicationHA guest components 13
	Symantec ApplicationHA user privileges 13
	Symantec ApplicationHA agents 14
	Licensing Symantec ApplicationHA 14
	Getting started with Symantec ApplicationHA (vCenter-integration) 16
	Getting started with Symantec ApplicationHA (VOM-integration) 18
Chapter 2	Planning to install Symantec ApplicationHA 20
	About installing Symantec ApplicationHA 20
	Requirements for installing ApplicationHA on virtual machines 22
	Supported VMware versions 22
	Supported guest operating systems 22
	Required Linux RPMs for Symantec ApplicationHA 40
	Supported applications 25
	Permissions requirements 26
	Ports and firewall settings for application high availability 26
	Additional requirements 27
Chapter 3	Installing Symantec ApplicationHA Guest Components 28
	About preparing to install Symantec ApplicationHA guest components 28
	Performing preinstallation tasks 29
	Obtaining Symantec ApplicationHA license keys 29
	Setting the PATH variable 30
	Mounting the product disc 30
	Performing an automated preinstallation check 31

	ApplicationHA installation methods for guest components	32
	Installing Symantec ApplicationHA guest components using the vSphere Client menu	32
	Copying the guest components installation package	36
	Installing Symantec ApplicationHA using the install program	37
	Encrypting a password	42
	Installing Symantec ApplicationHA using response files	43
	Response file variables to install Symantec ApplicationHA	44
	Sample response file for installing Symantec ApplicationHA	47
Chapter 4	Performing post-installation tasks	49
	Accessing the Symantec ApplicationHA documentation	49
	Removing permissions for communication	50
Chapter 5	Upgrading Symantec ApplicationHA	51
	About upgrading Symantec ApplicationHA	51
	Upgrade matrix	52
	Upgrading the ApplicationHA guest components using the vSphere Client menu	52
	Upgrading Symantec ApplicationHA using the install program	56
	Upgrading Symantec ApplicationHA using response files	60
	Response file variables to Upgrade Symantec ApplicationHA	61
	Sample response file for Upgrading Symantec ApplicationHA	63
Chapter 6	Uninstalling Symantec ApplicationHA Guest Components	65
	Preparing to uninstall Symantec ApplicationHA	65
	Uninstalling Symantec ApplicationHA using the uninstall program	66
	Running uninstallapplicationha program from the ApplicationHA media	67
	Uninstalling Symantec ApplicationHA using response files	67
	Response file variables to uninstall Symantec ApplicationHA	68
	Sample response file for uninstalling Symantec ApplicationHA	69
Chapter 7	Managing Symantec ApplicationHA licenses	70
	About managing ApplicationHA licenses	70
	Managing ApplicationHA licenses through vSphere Client menu	71

	Managing ApplicationHA licenses through Symantec High Availability tab	72
	Managing ApplicationHA licenses from the command line	72
Appendix A	ApplicationHA installation packages	74
	ApplicationHA installation RPMs	74
Appendix B	Troubleshooting Symantec ApplicationHA installation	76
	Symantec ApplicationHA logging	76
	Symantec High Availability Console logging	77
	ApplicationHA guest components logging	77
	Agent logging on virtual machine	78
	SSO configuration failure	78
	Restarting the vCenter Server or its service during the ApplicationHA guest components installation displays "Error" in vSphere Client tasks	79
	Reverting the virtual machine snapshot requires you to cancel the ApplicationHA guest components installation	79
	Non-supported operating system icon displayed for the selected virtual machine	80
	Installation of ApplicationHA guest components using vSphere GUI may fail	80
Appendix C	ApplicationHA tunable parameters	81
	ApplicationHA guest components installation parameters	81
Index		83

Introducing Symantec ApplicationHA

This chapter includes the following topics:

- [What is Symantec ApplicationHA](#)
- [Components of Symantec ApplicationHA](#)
- [Symantec ApplicationHA user privileges](#)
- [Symantec ApplicationHA agents](#)
- [Licensing Symantec ApplicationHA](#)
- [Getting started with Symantec ApplicationHA \(vCenter-integration\)](#)
- [Getting started with Symantec ApplicationHA \(VOM-integration\)](#)

What is Symantec ApplicationHA

ApplicationHA is one of the application availability management solutions from Symantec. It provides monitoring capabilities for applications running inside virtual machines managed by a VMware vCenter Server. Symantec ApplicationHA adds a layer of application awareness to the core HA functionality offered by VMware virtualization technology.

Alternately, Symantec ApplicationHA provides monitoring capabilities for applications running inside virtual machines managed by Veritas Operations Manager (VOM) Management Server 6.0.

Symantec ApplicationHA is based on Symantec™ Cluster Server (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), Intelligent Monitoring Framework (IMF), 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 the VMware vCenter Server.
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside virtual machines.
- Standardized way to manage applications using a single interface that is integrated with either VMware vSphere Client or the VOM Management Server console.
- Specialized Application Maintenance mode, in which ApplicationHA allows you to intentionally take an application out of its purview for maintenance or troubleshooting.
- Integration with VMware SRM Server that provides the capability to resume application monitoring after the virtual machines are started on the recovery site.

Components of Symantec ApplicationHA

Symantec ApplicationHA consists of the following components in a VMware virtualization environment:

- [Symantec High Availability Console](#)
- [Symantec ApplicationHA guest components](#)

Symantec High Availability Console

The Symantec High Availability Console enables Symantec High Availability integration with VMware vSphere Client. The Console must be installed separately in the Symantec ApplicationHA monitoring environment and should reside on a separate virtual machine or a physical host.

Note: You must not install the Console on a machine where VMware vCenter Server is installed.

The Symantec High Availability Console performs the following functions:

- As part of the Console installation, the installer registers the Symantec High Availability plugin for VMware vCenter Server. The plugin enables Symantec ApplicationHA integration with VMware vSphere Client and adds the Symantec

High Availability tab, the Symantec High Availability dashboard, and the Symantec High Availability home page to the VMware vSphere Client.

This plugin is required to view the Symantec High Availability tab, the Symantec High Availability dashboard, and the Symantec High Availability home page, in the vSphere Client.

The plugin enables you to install ApplicationHA guest components from the vSphere Client GUI. It also enables you to ensure disaster recovery of the monitored applications by using VMware Site Recovery Manager.

You can use the Symantec High Availability tab to configure application monitoring, control application start and stop, and monitor the application status on a virtual machine.

You can use the Symantec High Availability dashboard to administer application monitoring on a VMware cluster or datacenter.

The Symantec High Availability home page is added as an vSphere Client extension under the VMware Solutions and Applications pane. You can use the Symantec High Availability home page to perform any of the following tasks:

- Install ApplicationHA or Symantec High Availability guest components
- Manage ApplicationHA or Symantec High Availability licenses
- Configure single sign-on between sites for application monitoring continuity. The cross-site single sign-on is required to configure ApplicationHA in a VMware site recovery environment.
- The Symantec High Availability Console provides a single sign-on mechanism so that an authenticated vCenter user does not have to provide the virtual machine user credentials to configure and control application monitoring. The user also does not have to log on each time to connect to the virtual machine from the vSphere Client.
- The Console uses Symantec ApplicationHA Authentication service to provide secure communication between the virtual machine and the vSphere Client. It uses digital certificates for authentication and uses SSL to encrypt communications. Symantec ApplicationHA uses platform-based authentication; it does not store user passwords.
- The Console adds the Symantec ApplicationHA privileges to the vSphere Client environment. You can use the privileges to configure access control for vCenter Server users and groups.

Note: If you do not require the vSphere Client-integrated features described above, you need not install the Symantec High Availability Console. You can alternately configure and administer ApplicationHA from the Symantec High Availability view of the Veritas Operations Manager Management Server Console. For details, see VOM documentation

Symantec ApplicationHA guest components

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 application monitoring status on the virtual machine and displays it in the Symantec High Availability tab.

Symantec ApplicationHA user privileges

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

vCenter Server 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 *Symantec Cluster Server Bundled Agents Reference Guide (Linux)*.
- **Application agents**
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 72.
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 72.

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 Symantec High Availability tab. For more information:

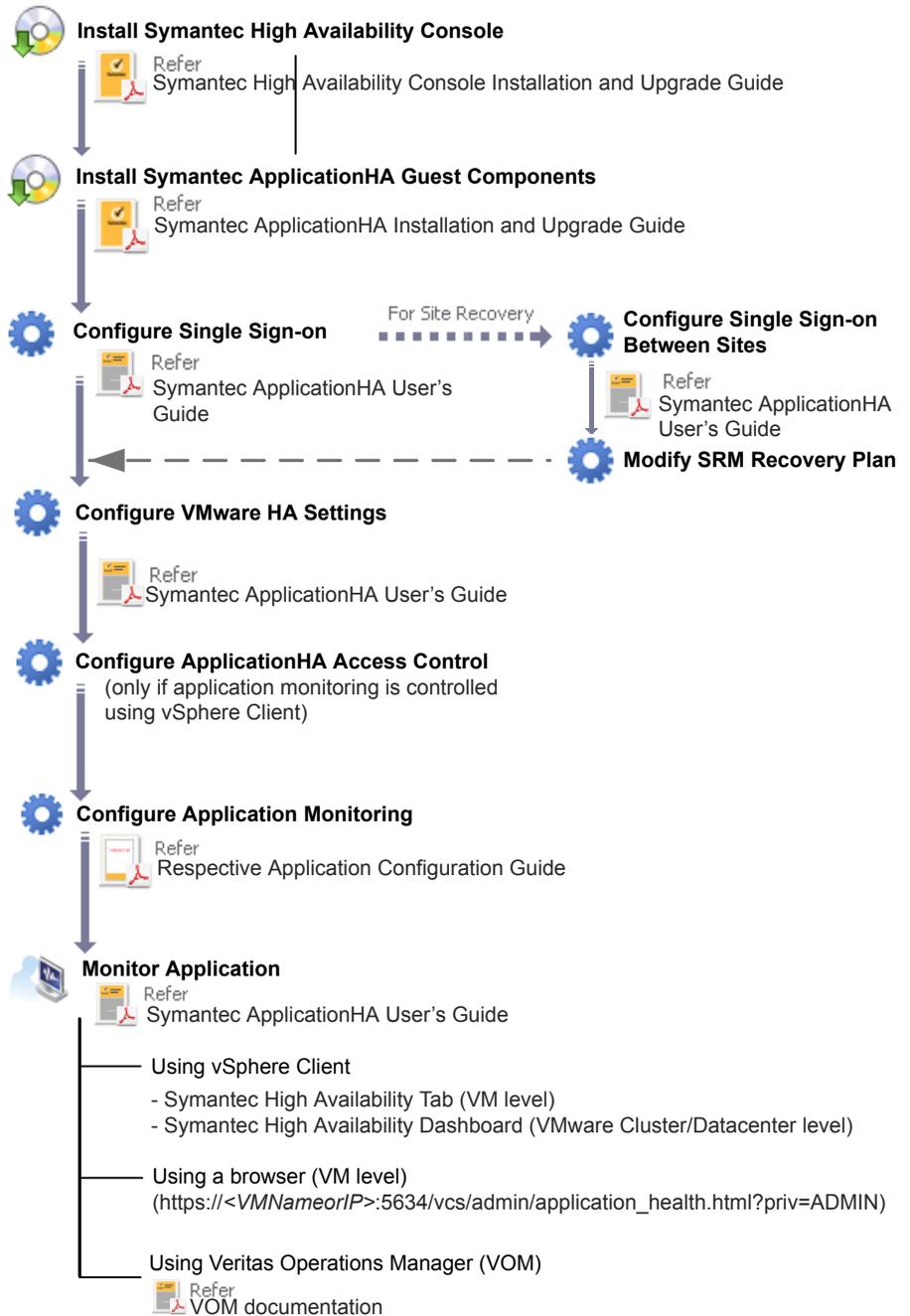
See [“About managing ApplicationHA licenses”](#) on page 70.

Getting started with Symantec ApplicationHA (vCenter-integration)

You can get started with ApplicationHA following broad steps:

- Install ApplicationHA
- Configure ApplicationHA
- Configure application monitoring

The following figure represents the detailed workflow for getting started with ApplicationHA and the corresponding document you must refer for details.



To configure and administer ApplicationHA from Veritas Operations Manager Console:

See [“Getting started with Symantec ApplicationHA \(VOM-integration\)”](#) on page 18.

Getting started with Symantec ApplicationHA (VOM-integration)

If you want to administer application availability over Veritas Operations Manager Management Server (VOM MS) Console, you can do so with the following simple steps.

Note that only installer-based or response-file-based installation and upgrades are supported in the VOM-integrated route. You configure and monitor application availability with ApplicationHA from the Symantec High Availability view of the Server perspective of VOM MS. VMware Site Recovery manager is not supported in this route.

- Install VOM Management Server 6.0
- Install ApplicationHA
- Add guest virtual machines as managed hosts to VOM
- Configure application monitoring
- Monitor applications

The following figure describes each step and the corresponding document that you must refer for details.

1.  **Install VOM Management Server 6.0**
  Refer VOM Installation and Configuration Guide
2.  **Install ApplicationHA 6.1 on the virtual machines.**
  Refer ApplicationHA Installation and Upgrade Guide
3.  **Add guest virtual machines as managed hosts to VOM.**
  Refer ApplicationHA User's Guide
4.  **Configure application monitoring on the virtual machines.**
  Refer Application specific Agent Guide
5.  **Monitor application.**
  Refer ApplicationHA User's Guide

To install, configure, and administer ApplicationHA from the vSphere Client:
See [“Getting started with Symantec ApplicationHA \(vCenter-integration\)”](#) on page 16.

Planning to install Symantec ApplicationHA

This chapter includes the following topics:

- [About installing Symantec ApplicationHA](#)
- [Requirements for installing ApplicationHA on virtual machines](#)
- [Additional requirements](#)

About installing Symantec ApplicationHA

[Table 2-1](#) describes the tasks for installing and setting up Symantec ApplicationHA in a VMware virtualization environment.

Table 2-1 Tasks for installing Symantec ApplicationHA

Task	Description
Installing Symantec High Availability Console	<p>Install the Symantec High Availability Console on a separate physical or virtual machine. This installation registers the Symantec High Availability plugin on the vCenter Server.</p> <p>For more information, see the <i>Symantec High Availability Console Installation Guide</i>.</p> <p>Note: If you are deploying a disaster recovery setup and plan to configure ApplicationHA for application monitoring continuity, you must install the Console host at both, the protected site and the recovery site.</p> <p>After the installation is complete, the Symantec High Availability tab, Symantec High Availability dashboard, and the Symantec High Availability home page are added to the vSphere client. The Symantec High Availability tab is visible when you select a virtual machine from the VMware vCenter Server inventory. The Symantec High Availability dashboard is visible when you select a cluster or a datacenter from the VMware vCenter Server inventory. The Symantec High Availability home page is added as a vSphere Client extension under its Solutions and Applications pane.</p> <p>Use the Symantec High Availability home page to perform any of the following tasks:</p> <ul style="list-style-type: none"> ■ Install ApplicationHA guest components ■ Manage ApplicationHA licenses ■ Configure SSO for disaster recovery <p>Use the Symantec High Availability tab to configure and control application monitoring on virtual machines that are managed from the VMware vCenter Server. You can perform these operations per virtual machine.</p> <p>Use the Symantec High Availability dashboard to administer the configured applications on virtual machines in a VMware datacenter. You can perform these operations at a VMware cluster or datacenter-level.</p>
Installing Symantec ApplicationHA guest components for virtual machines	<p>Install the ApplicationHA guest components on all the virtual machines where you wish to configure application monitoring. This installs the ApplicationHA agents and configuration wizard on the virtual machines</p> <p>Note: You must install the Console, before you install the guest components.</p>

Table 2-1 Tasks for installing Symantec ApplicationHA (*continued*)

Task	Description
Editing VMware VM monitoring settings to enable application monitoring	<p>After installing Symantec ApplicationHA components, you must manually edit the VM monitoring settings to enable application monitoring.</p> <p>This involves the following tasks:</p> <ul style="list-style-type: none"> ■ Editing the VM cluster settings from the vSphere Client You must manually change these settings from the vSphere Client. ■ Editing the settings from each virtual machine This is an optional task. To edit the settings, you must manually do so from the vSphere Client.

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 VMware versions

The following VMware Servers and management clients are currently supported:

- VMware ESX Server version 4.1 Update 3, 5.0 Update 2, and 5.1
- VMware ESXi Server version 5.0 Update 2, 5.1 Update 1 and 5.5
- VMware vCenter Server version 4.1 Update 2, 5.0, 5.1, and 5.5

Note: VMware Fault Tolerance is not supported in case of vCenter Server 4.1

- VMware vSphere Client version 4.1 Update 2, 5.0, 5.1, and 5.5
- VMware vCenter Site Recovery Manager (SRM) 5.0 and 5.1

Supported guest operating systems

[Table 2-2](#) shows the supported operating systems for this release.

Table 2-2 Supported guest operating systems

Operating systems	Levels	Kernel version
Oracle Linux 5	Update 5, 6, 7, 8, 9	2.6.18-194.el5
		2.6.18-238.el5
		2.6.18-274.el5
		2.6.18-308.el5
		2.6.18-348.el5
Oracle Linux 6	Update 3, 4	2.6.32-279.el6
		2.6.32-358.el6
Red Hat Enterprise Linux 5	Update 5, 6, 7, 8, 9	2.6.18-194.el5
		2.6.18-238.el5
		2.6.18-274.el5
		2.6.18-308.el5
		2.6.18-348.el5
Red Hat Enterprise Linux 6	Update 3, 4	2.6.32-279.el6
		2.6.32-358.el6
SUSE Linux Enterprise 11	SP 2	3.0.13-0.27.1
	SP 3	3.0.76-0.11.1

Note: 64-bit operating systems are only supported.

If your system is running a lower level of either Red Hat Enterprise Linux, SUSE Linux Enterprise Server, or Oracle Linux, than indicated in [Table 2-2](#), you must upgrade it before attempting to install Symantec ApplicationHA. Consult the Red Hat, SUSE, or Oracle documentation for more information on upgrading or reinstalling your system.

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

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

Required Linux RPMs for Symantec ApplicationHA

Make sure you install the following operating system-specific RPMs on the systems where you want to install or upgrade ApplicationHA. ApplicationHA will support any

updates made to the following RPMs, provided the RPMs maintain the ABI compatibility.

Table 2-3 lists the RPMs that ApplicationHA requires for a given Linux operating system.

Table 2-3 Required RPMs

Operating system	Required RPMs
OEL 5	compat-libstdc++-33-3.2.3-61.x86_64.rpm glibc-2.5-58.i686.rpm glibc-common-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 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

Table 2-3 Required RPMs (*continued*)

Operating system	Required RPMs
SLES 11	glibc-2.11.1-0.17.4.x86_64.rpm glibc-32bit-2.11.1-0.17.4.x86_64.rpm ksh-93t-9.9.8.x86_64.rpm libgcc43-32bit-4.3.4_20091019-0.7.35.x86_64.rpm libgcc43-4.3.4_20091019-0.7.35.x86_64.rpm libstdc++33-3.3.3-11.9.x86_64.rpm libstdc++43-32bit-4.3.4_20091019-0.7.35.x86_64.rpm

Supported applications

[Table 2-4](#) lists the applications that ApplicationHA Agent Pack currently supports on virtual machines.

Table 2-4 ApplicationHA Agent Pack supported applications

Application	Version	Document
SAP Netweaver	7.0	<i>Symantec ApplicationHA Agent for SAP NetWeaver Configuration Guide</i>
SAP Web Application Server	7.1, 7.3	<i>Symantec ApplicationHA Agent for SAP Web Application Configuration Guide</i>
Oracle Database	10gR2, 11gR1, and 11gR2; 12cR1	<i>Symantec ApplicationHA Agent for Oracle Configuration Guide</i>
WebLogic Server	9.x and 10.x	<i>Symantec ApplicationHA Agent for WebLogic Server Configuration Guide</i>
WebSphere MQ	7.0, 7.1, and 7.5	<i>Symantec ApplicationHA Agent for WebSphere MQ Configuration Guide</i>
WebSphere Application Server	7.x, 8.x	<i>Symantec ApplicationHA Agent for WebSphere Application Server Configuration Guide</i>
Apache HTTP server	1.3, 2.0, and 2.2. Also supports IBM HTTP Server 7.x.	<i>Symantec ApplicationHA Agent for Apache HTTP server Configuration Guide</i>
DB2	9.5 and 9.7	<i>Symantec ApplicationHA Agent for DB2 Configuration Guide</i>

Table 2-4 ApplicationHA Agent Pack supported applications (*continued*)

Application	Version	Document
JBoss Application Server	5.1.x	<i>Symantec ApplicationHA Agent for JBoss Application Server Configuration Guide</i>
MySQL	5.x	<i>Symantec ApplicationHA Agent for MySQL 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 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.
- When you use the vSphere Client menu to install the guest components, the installer prompts for the vCenter Server user name and password during the installation.
 This user account must have the privileges to enumerate the virtual machines visible in the vSphere Client.
 The installer uses this account to discover the virtual machine names in the vCenter Server inventory.

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 2-5](#) displays the services and ports used by ApplicationHA.

Table 2-5 Services and ports used by Symantec ApplicationHA

Component Name	Port	Settings	Description
Veritas Storage Foundation Messaging Service (xprtd)	5634	Allow inbound and outbound	Used for communications between the Symantec High Availability Console host machine and the virtual machines.
Symantec ApplicationHA Service	14151, 14152	Allow inbound and outbound	Used by the Tomcat server on console to receive web service requests and for local administration.
Symantec ApplicationHA Authentication Service	14153	Allow inbound and outbound	Used by Symantec High Availability Console to receive authentication requests from virtual machines.
Symantec ApplicationHA Database Service	14154	Allow inbound and outbound	Used by ApplicationHA locally for database services between the Symantec High Availability Console and the virtual machines.

Additional requirements

The following additional software requirements apply:

- Internet Explorer or Firefox Web browser is required on the system where the vSphere client is running.
 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 VMware vSphere Client to manage the virtual machines.
- 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 70.
- 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 guest components using the vSphere Client menu](#)
- [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 VMware versions”](#) on page 22.
- See [“Supported guest operating systems”](#) on page 22.
- See [“Required Linux RPMs for Symantec ApplicationHA”](#) on page 40.

- See “Supported applications” on page 25.
- See “Permissions requirements” on page 26.
- See “Ports and firewall settings for application high availability” on page 26.
- See “Additional requirements” on page 27.

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 29.
Set the PATH variable	See “Setting the PATH variable” on page 30.
Mount the product disc	See “Mounting the product disc” on page 30.
Verify the system before installation	See “Performing an automated preinstallation check” on page 31.
Install VMware Tools	See VMware documentation.

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 required operating system:

Operating system	Location
Oracle Enterprise Linux 5	cdrom_root/rhel5_x86_64/applicationha
Oracle Enterprise Linux 6	cdrom_root/rhel6_x86_64/applicationha
Red Hat Enterprise Linux 5	cdrom_root/rhel5_x86_64/applicationha
Red Hat Enterprise Linux 6	cdrom_root/rhel6_x86_64/applicationha
SUSE Linux Enterprise Server 11	cdrom_root/sles11_x86_64/applicationha

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

```
# cd cdrom_root/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.

Note: If you want to install the guest components by using the VMware vCenter menu, you can skip this check.

To check the system

- 1 Navigate to the folder that contains the installation program.

See [“Mounting the product disc”](#) on page 30.

- 2 Start the preinstallation check:

```
# ./installapplicationha -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 vCenter menu	You can install ApplicationHA using the vCenter menu. Note: You can simultaneously install ApplicationHA on multiple virtual machines using the vCenter menu.
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 <code>installapplicationha61</code> 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 <code>rpm -i</code> command.

Installing Symantec ApplicationHA guest components using the vSphere Client menu

Consider the following points before you proceed with the installation.

- The installer uses the logged-on user account context for installation. Verify that the logged-on user has local administrator privileges on the system where you want to install.
- Symantec recommends that you first install the Symantec High Availability Console before installing the guest components. The ApplicationHA plugin is registered during the Symantec High Availability Console installation.

During the guest components installation, the installer verifies the ApplicationHA plugin registration on the vCenter Server. If the plugin is not registered, the installer displays a prompt.

You can choose to proceed with the guest components installation; however the ApplicationHA plugin registration is required for configuring application monitoring from the vSphere Client.

- Installation of guest components also configures single sign-on between the virtual machine and the Console host. However, if the SSO configuration fails, you must manually configure it after the guest installation is complete. Use the Symantec High Availability tab to configure the SSO manually.

For details refer to *Symantec™ ApplicationHA User's Guide*.

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

- The installer allows remote installation. You can launch the installer from any virtual machine, cluster or a datacenter in your network.
In case of remote installations, ensure that the logged-on user has local administrator privileges on all the remote systems where you wish to install the guest components.

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

For details, See [“Copying the guest components installation package”](#) on page 36.

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

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

- 1 Using the vSphere Client, connect to the vCenter Server and navigate to **Home > Solutions and Applications > Symantec High Availability**.

On the Getting Started tab, click **Install Guest Components**

Alternatively,

Using the vSphere Client, connect to the vCenter Server and navigate to **Home > Hosts and Clusters**.

From the vCenter inventory tree view, right-click on the datacenter, cluster or any of the virtual machine and select **Symantec High Availability > Install Guest Components**.

This launches the Symantec ApplicationHA Guest Components Installer.

- 2 On the Welcome panel, review the prerequisites, and click **Next**.
- 3 On the vCenter Server Details panel, specify the vCenter Server user credentials and then click **Next**.

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

The specified user must have the following privileges:

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

- 4 On the Product Selection panel, select the product (ApplicationHA) that you want to install.

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

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

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

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

See ["Copying the guest components installation package"](#) on page 36.

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

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

To select the virtual machines

- Skip this sub-step if you launched the installation wizard by right-clicking a system in the inventory view of the vSphere Client GUI.
Click **Add**.
- On the Select Virtual Machines panel, select the desired virtual machines, specify the required details and click **OK**.
The specified details apply to all the selected virtual machines. If they are different for one or more machines, you can edit them later.
- If required, edit the user credentials and the license key details.
If the user credentials and license key is different for an individual virtual machine, you can edit the details inline.
If the details to be edited are same for multiple virtual machines, select the desired machines and click **Edit**. On the **Edit Virtual Machine Details** panel, enter the details that apply to the selected virtual machines and click **OK**.
- Click **Install** to begin the installation.
The installer performs the required validation checks on the selected virtual machines and moves to the Installation panel, if all the selected virtual machines pass the validation checks.
If the validation checks fail on any of the virtual machines, the status is reflected as follows:
For virtual machines that pass the validation checks: **Ready for install**.
For virtual machines that do not pass the validation checks: **Verification failed**
To view the cause of validation failure, select the virtual machine. The details are displayed in the Verification Details box.
Rectify the issue and then click **Install**.
The installer re-validates the failed virtual machines.

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

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

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

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

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

For details, refer to the individual application configuration guide.

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

Copying the guest components installation package

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

Perform the following to copy the guest installer package

- 1 Insert the product software disc for Windows operating system into your system drive.
- 2 On the Console host, navigate to the following path.
<Installation Path>\ApplicationHA\Console\installer

- 3 Run the Copyinstaller.bat file.
- 4 Enter the parameters in the following format.

```
CopyInstaller <Source>
```

Where,

Source: The directory path where the installer disc is mounted or copied.

For example,

```
CopyInstaller <D:>dvd2-linux\rhe15_x86_64
```

```
CopyInstaller <F:>dvd2-linux\sles11_x86_64
```

```
CopyInstaller <F:>dvd2-linux\win2k8_x86_64
```

Installing Symantec ApplicationHA using the install program

Note: You can simultaneously install ApplicationHA on multiple virtual machines across a variety of operating systems, only when using the vCenter menu. In installer-based methods, such batch installations are supported across any one operating system.

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

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 30.

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

Operating system	Directory
Oracle Enterprise Linux 5	rhel5_x86_64
Oracle Enterprise Linux 6	rhel6_x86_64
Red Hat Enterprise Linux 5	rhel5_x86_64
Red Hat Enterprise Linux 6	rhel6_x86_64
SUSE Linux Enterprise Server 11	sles11_x86_64

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

```
# cd cdrom_root/rhel5_x86_64/applicationha
```

3 Run the installer to start installation on the guest.

You can set up single sign on at the time of installation. If you want to install ApplicationHA without the single sign-on mechanism enabled, start the `installapplicationha` program:

```
# ./installapplicationha61
```

If you want to install ApplicationHA with single sign-on enabled, execute the following steps:

a. Create a file, say **<SSO input file>**, in the `tmp` folder with the following contents:

```
$Obj::pool{Cfg}{sso_console_ip} = '1.2.3.4';
```

```
$Obj::pool{Cfg}{sso_local_username} = 'root';
```

```
$Obj::pool{Cfg}{sso_local_password} = 'encryptedpassword';
```

Note: You must enter only encrypted passwords in the SSO input files. See [“Encrypting a password”](#) on page 42.

b. Start the installation program:

```
# ./installapplicationha61 – require <SSO input file>
```

The install program starts with a copyright message and specifies the directory where the logs are created.

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 system 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 guest operating systems”](#) on page 22.

- 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 40.
 - 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, 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 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 43.

Encrypting a password

You must encrypt passwords before adding them to the SSO input files or the response files. Symantec ApplicationHA provides the `vcencrypt` utility to encrypt passwords. You can find this utility in the Symantec ApplicationHA product disc.

For example, to install ApplicationHA on a machine running the RHEL 5 operating system, you can find the utility in the following location:

```
cdrom_root/rhel5_x86_64/scripts/vcencrypt
```

To encrypt a password:

- 1 Navigate to the directory that contains the encryption utility for the required operating system:

Operating system	Directory
Oracle Enterprise Linux 5	rhel5_x86_64
Oracle Enterprise Linux 6	rhel6_x86_64
Red Hat Enterprise Linux 5	rhel5_x86_64
Red Hat Enterprise Linux 6	rhel6_x86_64
SUSE Linux Enterprise Server 11	sles11_x86_64

For example, to encrypt a password when installing Symantec ApplicationHA on a machine running the RHEL 5 operating system:

```
# cd cdrom_root/rhel5_x86_64/scripts/
```

- 2 Run the encrypt utility by using the following command:

```
# ./vcsencrypt -agent
```

- 3 Enter the password.

The encrypt program displays the encrypted password. Copy the encrypted password to the SSO input files or the response files.

Installing Symantec ApplicationHA using response files

Note: You can simultaneously install ApplicationHA on multiple virtual machines, only when using the vCenter menu.

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 22.
- 2 Make sure the preinstallation tasks are completed.
 See [“Performing preinstallation tasks”](#) on page 29.
- 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 44.
 See [“Sample response file for installing Symantec ApplicationHA”](#) on page 47.

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

```
# cd /opt/VRTS/install/
# ./installapplicationha61 -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)

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

Variable	List or Scalar	Description
CFG{systems}	List	Name of the systems on which the product is to be installed. (Required)
CFG{prod}	Scalar	Defines the product to be installed. The value is APPLICATIONHA61. (Required)
CFG{sso_console_ip}	Scalar	Specifies the IP address of the associated Symantec High Availability Console. (Required)
CFG{sso_local_username}	Scalar	Specifies the user name (administrative user account) by using which you can install the guest components on the required virtual machine. (Required)
CFG{sso_local_password}	Scalar	Specifies the password (for the administrative user account) by using which you can install the guest components on the required virtual machine. (Required) Note: You must enter only encrypted passwords in the response files. See “Encrypting a password” on page 42.
CFG{keys} {system}	Scalar	List of keys to be registered on the system. (Optional)

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

Variable	List or Scalar	Description
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 RPMs. The location must be accessible from the target 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 install. The default location is <i>/var/tmp</i> . (Optional)

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

Variable	List or Scalar	Description
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 44.

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}="APPLICATIONHA61";
$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}="APPLICATIONHA61";  
$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 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
Oracle Linux 5	rhel5_x86_64/docs/applicationha/vmware
Oracle Linux 5	rhel6_x86_64/docs/applicationha/vmware
Red Hat Enterprise Linux 5	rhel5_x86_64/docs/applicationha/vmware
Red Hat Enterprise Linux 6	rhel6_x86_64/docs/applicationha/vmware
SUSE Linux Enterprise Server 11	sles11_x86_64/docs/applicationha/vmware

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

```
# cd cdrom_root/rhel5_x86_64/
```

- 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 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.

Upgrading Symantec ApplicationHA

This chapter includes the following topics:

- [About upgrading Symantec ApplicationHA](#)
- [Upgrade matrix](#)
- [Upgrading the ApplicationHA guest components using the vSphere Client menu](#)
- [Upgrading Symantec ApplicationHA using the install program](#)
- [Upgrading Symantec ApplicationHA using response files](#)

About upgrading Symantec ApplicationHA

Upgrading Symantec ApplicationHA involves upgrade of the guest components.

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 20.
- Review the licensing details.
See [“Licensing Symantec ApplicationHA ”](#) on page 14.
- Review the supported upgrade matrix
See [“Upgrade matrix”](#) on page 52.

[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 vCenter menu</p> <p>See “Upgrading the ApplicationHA guest components using the vSphere Client menu” on page 52.</p> <p>For upgrading by using the installer (interactive mode)</p> <p>See “Upgrading Symantec ApplicationHA using the install program” on page 56.</p> <p>For upgrading by using response files</p> <p>See “Upgrading Symantec ApplicationHA using response files” on page 60.</p>

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 5.1 Guest Components	ApplicationHA 6 .1 Guest Components	RHEL 5
ApplicationHA 5.1 SP2 Guest Components	ApplicationHA 6.1 Guest Components	RHEL 5, SLES 11, and OEL 5
ApplicationHA 6.0 Guest Components	ApplicationHA 6.1 Guest Components	RHEL 5, RHEL 6, SLES 11, OEL 5, and OEL 6

Upgrading the ApplicationHA guest components using the vSphere Client menu

Perform the following steps to upgrade the ApplicationHA guest components on the virtual machines, through the vSphere Client menu.

You can upgrade the guest components on virtual machines running Windows as well as any of the supported Linux operating systems.

Note: Ensure that the platform-specific ApplicationHA guest components installation package is available on the Console.

To copy the software, run the CopyInstaller.bat file on the Console host. The file is located at the following location:

<Installation Path>\applicationha\console\installer

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

To upgrade the ApplicationHA guest components

- 1 Using the vSphere Client, connect to the vCenter Server and navigate to **Home > Solutions and Applications > Symantec High Availability**.

On the Getting Started tab, click **Install Guest Components**

Alternatively,

Using the vSphere Client, connect to the vCenter Server and navigate to **Home > Hosts and Clusters**.

From the vCenter inventory tree view, right-click on the datacenter, cluster or any of the virtual machine and select **Symantec High Availability > Install Guest Components**.

This launches the Symantec ApplicationHA Guest Components Installer.

- 2 On the Welcome panel, review the prerequisites and the Symantec Software License Agreement and then click **Next**.
- 3 On the vCenter Server Details panel, specify the vCenter Server user credentials. Click **Next**.

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

The specified user must have the following privileges:

- ApplicationHA administrator privileges to perform the installation on the virtual machines.

- vCenter privileges to "create tasks", "update tasks" and "acquire guest control ticket" on the virtual machines.

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

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

The specified user must have the following privileges:

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

- 5 On the Product Selection panel, select the product (ApplicationHA) that you want to upgrade.

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

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

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

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

See ["Copying the guest components installation package"](#) on page 36.

- 6 On the System Selection panel, perform the following tasks:

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

To select the virtual machines

- Skip this sub-step if you launched the installation wizard by right-clicking a system in the inventory view of the vSphere Client GUI.
Click **Add**.

- On the Select Virtual Machines panel, select the desired virtual machines, specify the required details and click **OK**.

The specified details apply to all the selected virtual machines. If they are different for one or more machines, you can edit them later.

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

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

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

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

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

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

For details, refer to the individual application configuration guide.

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

Upgrading Symantec ApplicationHA using the install program

Perform the following steps to upgrade ApplicationHA:

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

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 30.

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

Operating system	Directory
Oracle Linux 5	rhel5_x86_64
Oracle Linux 6	rhel6_x86_64
Red Hat Enterprise Linux 5	rhel5_x86_64
Red Hat Enterprise Linux 6	rhel6_x86_64
SUSE Linux Enterprise Server 11	sles11_x86_64

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

```
# cd cdrom_root/rhel5_x86_64/applicationha
```

3 Run the installer to start upgrading ApplicationHA on the guest.

You can set up single sign on at the time of upgrade. If you want to upgrade ApplicationHA without the single sign-on mechanism enabled, start the installation program:

```
# ./installapplicationha61
```

If you want to upgrade ApplicationHA with single sign-on enabled, execute the following steps:

a. Create a file, say **<SSO input file>**, in the `tmp` folder with the following contents:

```
$Obj::pool{Cfg}{sso_console_ip} = '1.2.3.4';
$Obj::pool{Cfg}{sso_local_username} = 'root';
$Obj::pool{Cfg}{sso_local_password} = 'encryptedpassword';
```

Note: You must enter only encrypted passwords in the SSO input files. See [“Encrypting a password”](#) on page 42.

b. Start the installation program:

```
# ./installapplicationha61 – require <SSO input file>
```

The install program starts with a copyright message and specifies the directory where the logs are created.

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 system 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 guest operating systems”](#) on page 22.

- 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 40.
 - 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 upgrade on each virtual machine.
- The install program upgrades the ApplicationHA RPMs 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 RPMs 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 60.

Upgrading Symantec ApplicationHA using response files

When you upgrade ApplicationHA on a virtual machine using the install program, it generates a response file. You can use the response file to upgrade ApplicationHA on other virtual machines. 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 virtual machines”](#) on page 22.
- 2 Make sure the preinstallation tasks are completed.
 See [“Performing preinstallation tasks”](#) on page 29.
- 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 61.
 See [“Sample response file for Upgrading Symantec ApplicationHA”](#) on page 63.

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 RHEL6 disc, use the following command:

```
# cd /cdrom_root/rhel6_x86_64/applicationha
```

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

```
# ./installapplicationha61 -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 RPMs. (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 APPLICATIONHA61. (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 depots 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 61.

For permanent license:

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

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="APPLICATIONHA61";
$CFG{systems}=[ qw(system1) ];
$CFG{sso_console_ip}="<IP address>";
$CFG{sso_local_username}="<user name>";
$CFG{sso_local_password}="<password>";
$CFG{keys}{ 'system1' }=["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}="APPLICATIONHA61";  
$CFG{systems}=[ qw(system1) ];  
$CFG{sso_console_ip}="<IP address>";  
$CFG{sso_local_username}="<user name>";  
$CFG{sso_local_password}="<password>";  
$CFG{uploadlogs}=1;  
$CFG{opt}{vxkeyless}=1;
```

Uninstalling Symantec ApplicationHA Guest Components

This chapter includes the following topics:

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

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 a virtual machine, using the `uninstallapplicationha` program:

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

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  
# ./uninstallapplicationha61
```

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 system 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.

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

Running `uninstallapplicationha` program from the ApplicationHA media

You may need to use the `uninstallapplicationha` program on the ApplicationHA 6.1 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
Oracle Linux 5	<code>rhel5_x86_64</code>
Oracle Linux 6	<code>rhel6_x86_64</code>
Red Hat Enterprise Linux 5	<code>rhel5_x86_64</code>
Red Hat Enterprise Linux 6	<code>rhel6_x86_64</code>
SUSE Linux Enterprise Server 11	<code>sles11_x86_64</code>

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/rhel5_x86_64/applicationha/
```

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

See [“Uninstalling Symantec ApplicationHA using the `uninstall` program”](#) on page 66.

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 65.
- 2 Copy the response file to the system where you want to uninstall ApplicationHA.
 See “[Sample response file for uninstalling Symantec ApplicationHA](#)” on page 69.
- 3 Edit the values of the response file variables as necessary.
 See “[Response file variables to uninstall Symantec ApplicationHA](#)” on page 68.
- 4 Start the uninstallation from the system to which you copied the response file.
 For example:

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

# ./uninstallapplicationha61 -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 APPLICATIONHA61. (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 <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 depots 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 68.

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

$CFG{opt}{uninstall}=1;
$CFG{prod}="APPLICATIONHA61";
$CFG{systems}=[ qw(system1) ];
```

Managing Symantec ApplicationHA licenses

This chapter includes the following topics:

- [About managing ApplicationHA licenses](#)
- [Managing ApplicationHA licenses through vSphere Client menu](#)
- [Managing ApplicationHA licenses through Symantec High Availability tab](#)
- [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 72.

- If you have not installed ApplicationHA, you can navigate to the Symantec High Availability tab in the vSphere client, and click **Install ApplicationHA Guest Components**, under Basic Tasks. This launches a wizard, where you can specify a license.
- Connect to the vCenter Server and navigate to **Home > Solutions and Application > Symantec ApplicationHA**. Use this path to manage the licenses for local and remote virtual machines.
See “[Managing ApplicationHA licenses through vSphere Client menu](#)” on page 71.
- Connect to the vCenter Server and select the virtual machine for which you want to update the licenses. Select the **Symantec High Availability** tab and click **Licenses**. Use this path to manage licenses for the local virtual machine.
See “[Managing ApplicationHA licenses through Symantec High Availability tab](#)” on page 72.
- You can also access the Symantec High Availability tab 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 vSphere Client menu

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

To manage the ApplicationHA licenses

- 1 Connect to the vCenter Server and navigate to **Home > Solutions and Applications > Symantec ApplicationHA**
- 2 Click the **License Management** tab.
- 3 Select the desired virtual machines and click **Next**.
Only the machines that are powered ON can be selected.
- 4 Select a virtual machine and click **Add License**.
Use the **CTRL** key to select multiple virtual machines.

- 5 Enter the license key in the **Add License Key** text box and click **Validate Key**.

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

- 6 Click **Apply**.

The specified license keys take effect immediately.

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

Managing ApplicationHA licenses through Symantec High Availability tab

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

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

To manage the ApplicationHA licenses

- 1 Connect to the vCenter Server and from the Host and Clusters select the virtual machine for which you want to update the licenses.
- 2 Click the **Symantec High Availability** tab and then click **Licenses**.
- 3 On the License Management panel, enter the permanent license key in the **Enter license key** text box and then click **Add**.
- 4 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 RPMs](#)

ApplicationHA installation RPMs

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

Table A-1 Symantec ApplicationHA RPMs

RPM	Contents
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.
VRTSvcsvcs	VRTSvcsvcs contains the following components: <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.
VRTSvcsvcsag	Contains the binaries for Symantec Cluster Server bundled agents by Symantec.

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

RPM	Contents
VRTSvcsvmw	Contains the ApplicationHA virtual machine wizards for application monitoring configurations by Symantec.
VRTSsapnw04	Contains the binaries for Symantec High Availability Agent for SAP NetWeaver.
VRTSsapwebas71	Contains the binaries for Symantec High Availability Agent for SAP Web Application Server.
VRTSjboss	Contains the binaries for Symantec High Availability Agent for JBoss Application Server
VRTSmysql	Contains the binaries for Symantec High Availability agent for MySQL
VRTSacclib	Contains the binaries for Symantec Cluster Server ACC libraries by Symantec.
VRTSvcsea	VRTSvcsea contains the binaries for Symantec DBED agents (Oracle, DB2, and Sybase).
VRTSwls	VRTSwls contains the binaries for Veritas high availability agent for WebLogic Server by Symantec.
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.
VRTSsfcp61	<p>VRTSsfcp61 contains the binaries for the Symantec Storage Foundation Common Product Installer. This mandatory RPM 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](#)
- [SSO configuration failure](#)
- [Restarting the vCenter Server or its service during the ApplicationHA guest components installation displays "Error" in vSphere Client tasks](#)
- [Reverting the virtual machine snapshot requires you to cancel the ApplicationHA guest components installation](#)
- [Non-supported operating system icon displayed for the selected virtual machine](#)
- [Installation of ApplicationHA guest components using vSphere GUI may fail](#)

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.

Symantec High Availability Console logging

Use the `hagetcf` utility to collect the Symantec High Availability Console logs. This utility retrieves and writes detailed diagnostic information about the monitoring configuration. These details are useful for debugging configuration related issues.

After you install the Symantec High Availability Console the `hagetcf` utility is available in the following directory on the Console host:

```
<installdirectory>\ApplicationHA\bin
```

Here, *<installdirectory>* is the directory where you install the Console, typically, `C:\Program Files\Veritas`.

Perform the following steps to collect the Symantec High Availability Console logs:

- 1 On the Symantec High Availability Console host, navigate to the following directory from the command prompt:

```
<installdirectory>\ApplicationHA\bin
```

- 2 Run the `hagetcf` utility from the directory. Type the following command:

```
hagetcf -appserver
```

The `hagetcf` utility writes the output to `%systemdrive%\hagetcf\mmyy_hhmm` directory.

For example, `C:\hagetcf\0819_2316`.

The directory contains several folders and log files representing 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 Symantec ApplicationHA guest components by using the vSphere Client menu, the logs are located in the following location:

```
/opt/AppHAInstaller/vii_backup/
```

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 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.
```

SSO configuration failure

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

Workaround:

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

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

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

Workaround:

After the vCenter Server or its service restarts, click on each of the selected virtual machine and verify if the ApplicationHA health view appears in the vSphere Client.

Presence of ApplicationHA health view indicates successful installation of the guest components. However, if the ApplicationHA health view is not present, refer to the ApplicationHA logs for installation details.

The ApplicationHA logs are located on the virtual machine at the following location:

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

Reverting the virtual machine snapshot requires you to cancel the ApplicationHA guest components installation

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

Workaround:

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

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

Alternatively,

```
https://ApplicationHAConsole_IP:14152/ac/CancelGuestInstallation?  
VmName=VirtualMachine_Name&VmUser=UserName&VmPassword=Password
```

Where,

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

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

Non-supported operating system icon displayed for the selected virtual machine

Even if the virtual machine runs a supported operating system the System Selection page of the guest installation wizard launched using the vSphere Client menu displays a non-supported operating system icon.

This situation occurs if you run the ApplicationHA guest installation wizard from the vSphere Client menu immediately after,

- the virtual machine is powered on
- reverting the virtual machine snapshot

The wizard shows the non-supported operating system icon for the virtual machine due to the delay in retrieving the virtual machine operating system details.

Workaround:

Allow certain time lapse after you power on or revert the snapshot of a virtual machine and then proceed to install the guest components.

Installation of ApplicationHA guest components using vSphere GUI may fail

Before you install ApplicationHA guest components using vSphere GUI, you must archive the guest components to the Symantec High Availability console using CopyInstaller. Some users may save the guest components in a local Windows folder. They may then specify the folder as a source folder for CopyInstaller. In this case, due to the mismatch between the Windows environment and Linux guest components, CopyInstaller may not be able to successfully archive the guest components to the Symantec High Availability console. As a result, installation from the vSphere GUI may fail.

Workaround

When you save the guest components to a local folder, save them in the binary mode.

ApplicationHA tunable parameters

This appendix includes the following topics:

- [ApplicationHA guest components installation parameters](#)

ApplicationHA guest components installation parameters

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

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

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

Note: After you edit the parameter values, you must restart the Symantec ApplicationHA Service.

[Table C-1](#) lists the guest components parameters for which you can customize the default values.

Table C-1 Guest components tunable parameters

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

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

Parameter	Description
VIPollingInterval	Determines the time interval for polling the installation progress on the virtual machine. The default interval between two consecutive polling tasks is 15 minutes.
VIIQueueTimeout	Determines the time span for which a virtual machine is queued for installation. Default= 120 minutes. If the virtual machine is queued for installation for more than 120 mins a time out error occurs and the virtual machine is removed from the installation queue.
VIICopyTimeout	Determines the time span for copying the guest installer package to the virtual machine, from the Console host. Default= 45 mins If the time taken to copy the installer package exceeds 45 mins, a time out error occurs and the installation is aborted.
VIIGuestInstallTimeout	Determines the time taken to complete the guest installation. Default= 45 mins If the time taken for installation exceeds 45 mins, a time out error occurs and the installation is aborted.

Index

A

- about
 - upgrade 51
- ApplicationHA
 - about 10

C

- client license 14

F

- firewall settings
 - for application high availability 26

I

- install
 - guest components; vSphere Client menu 32
- installation
 - methods 32
 - of Symantec ApplicationHA
 - using install program 37
 - using response files 43
 - packages 74
 - preparing 28
- installing Symantec ApplicationHA using install program 37
- installing Symantec ApplicationHA using response files 43, 60

L

- license key 14
- License management
 - local machine; Symantec High Availability tab 72
- licensing 14
- Logs
 - agents 78
 - installer 77
 - Symantec High Availability Console 77

O

- obtaining license keys 29

P

- port settings
 - for application high availability 26
- pre-installation
 - checking the systems 31
 - obtaining license keys 29
 - setting PATH variable 30
- pre-installation checks 31
- product licensing 14

R

- response files
 - generate a response file 43, 60
 - installing Symantec ApplicationHA
 - sample response file 47
 - variables 44, 61
 - uninstalling Symantec ApplicationHA
 - sample response file 69
 - variables 68
 - upgrading Symantec ApplicationHA
 - sample response file 63

S

- setting PATH variable 30
- Symantec ApplicationHA
 - installation using install program 37
 - installation using response file 43
 - license 14
 - uninstallation using response file 67
 - upgrade using install program 56
 - upgrading using response file 60

T

- tunable parameters 81

U

uninstallation

- using response files 67

uninstalling Symantec ApplicationHA

- removing packages 66

update

- ApplicationHA license keys; vSphere Client menu 71

upgrade

- guest components; vSphere Client menu 52

- matrix 52

- Symantec ApplicationHA

 - using install program 56

upgrade scenarios

- ApplicationHA Guest Components. 52

upgrade Symantec ApplicationHA using install

- program 56

upgrading

- Symantec ApplicationHA

 - using response files 60