Symantec™ ApplicationHA 6.1 Installation and Upgrade Guide - AIX on IBM PowerVM

January 2014

Symantec

Symantec™ ApplicationHA 6.1 Installation and Upgrade Guide

Product version: 6.1

Document version: 6.1 Rev 2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

Support agreement resources

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

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

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

Chapter 1

Introducing Symantec ApplicationHA

This chapter includes the following topics:

What is Symantec ApplicationHA

Symantec ApplicationHA provides monitoring capabilities for applications running inside logical partitions in the IBM PowerVM virtualization environment. Symantec ApplicationHA adds a layer of application awareness to the core high availability (HA) functionality offered by Symantec™ Cluster Server (VCS) in the management LPAR.

Symantec ApplicationHA is based on VCS and uses similar concepts such as agents, resources, and service groups. However, it does not include the high availability cluster components such as the Group Membership and Atomic Broadcast (GAB), Low Latency Transport (LLT), 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:

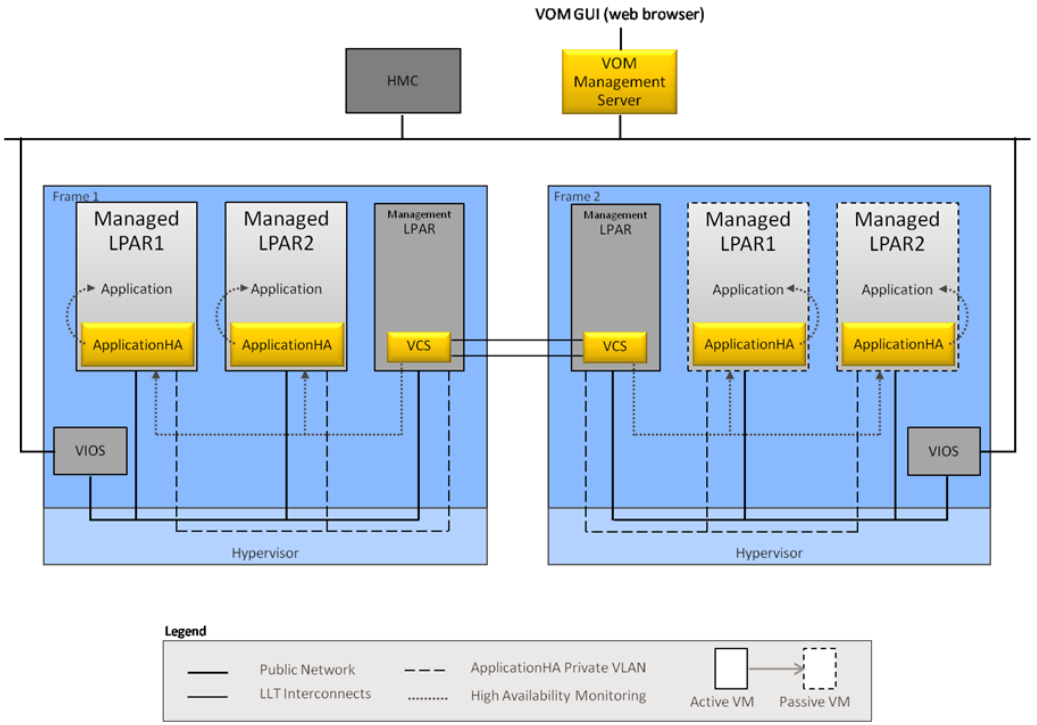
- Out of the box integration with VCS.
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside managed LPARs.
- High availability of the application as well as the managed LPAR inside which the application runs.
- Graded application fault-management responses such as:-
  - Application restart
  - ApplicationHA-initiated, graceful internal reboot (soft reboot) of a managed LPAR
  - VCS-initiated, external reboot (hard reboot) of managed LPAR
  - Failover of the managed LPAR to another VCS node.
- Specialized Application Maintenance mode, in which ApplicationHA allows you to intentionally take an application out of its purview for maintenance or troubleshooting.

How ApplicationHA is deployed in the IBM PowerVM environment

PowerVM is a virtualization and partitioning technology supported on IBM POWER-based System p servers. PowerVM technology lets you create multiple virtual systems, called logical partitions (LPARs), on a single physical frame.

In the IBM PowerVM virtualization environment, ApplicationHA provides high availability of applications running on managed LPARs. Symantec Cluster Server (VCS) provides high availability of the managed LPARs that run on the physical frame.

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



You can use one of the logical partitions to manage the other logical partitions on the same physical frame. This document uses the term management LPAR for such a logical partition. The other logical partitions are termed as managed LPARs.

ApplicationHA is installed on the managed LPAR, and provides high availability to a configured application running on the managed LPAR. VCS is installed on the management LPAR. VCS provides high availability to the managed LPAR where the configured application runs.

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

When you enable VCS to support ApplicationHA, a private VLAN is created between monitored managed LPARs and the VCS node (management LPAR). The private VLAN facilitates heartbeat communication between VCS in the management LPAR and ApplicationHA in the managed LPARs.

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

For more information on how VCS monitors managed LPARs for high availability, see the *SFHA Virtualization Solutions Guide for AIX*.

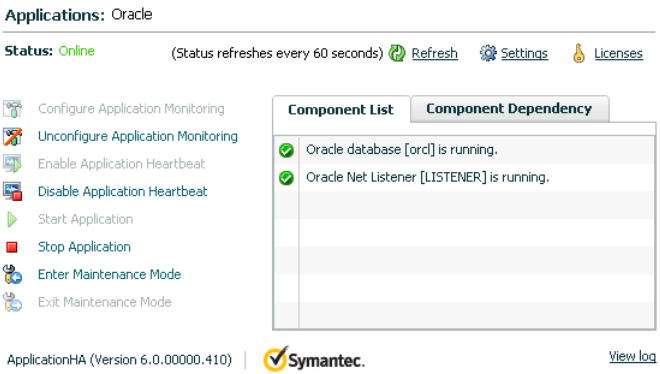
How Symantec ApplicationHA works with VCS

Symantec ApplicationHA installed in managed LPARs communicates directly with VCS installed in the management LPAR. Symantec ApplicationHA conveys the application health status to VCS in the form of a heartbeat. If VCS does not receive the heartbeat from a particular managed LPAR within a specified interval, VCS either restarts that managed LPAR or fails it over to another physical frame that is part of a VCS cluster.

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

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

The following figure displays the Symantec High Availability view where Oracle is configured for monitoring.



How Symantec ApplicationHA detects application failures

Symantec ApplicationHA architecture uses the agent framework to monitor the state of the applications and their dependent components running inside the managed LPARs. Symantec ApplicationHA agents monitor the overall health of the configured applications by running specific commands, tests, or scripts. For more details, see the agent functions section of the application-specific agent guides or the generic agent guide distributed with ApplicationHA.

The ApplicationHA Heartbeat agent is auto-configured when you configure application monitoring. The Heartbeat agent sends the application heartbeat to the management LPAR running VCS. Symantec ApplicationHA uses the application

heartbeat as the communication medium to convey the status of the application to VCS.

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

Components of the Symantec ApplicationHA setup

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

- Symantec ApplicationHA guest components for managed LPARs
- VCS in the virtualization infrastructure

Symantec ApplicationHA guest components for managed LPARs

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

The guest components also include the Veritas Storage Foundation Messaging Service (xprtld). This service communicates the status of the applications running on the managed LPAR and displays it in the Symantec High Availability view of the Veritas Operations Manager MS console.

VCS in the virtualization infrastructure

Symantec Cluster Server by Symantec (VCS) is installed on the management LPAR. The management LPAR runs inside a physical host. VCS is installed on management LPARs in more than one physical frame, to form a VCS cluster. As a result, VCS provides high availability in the infrastructure layer of the IBM PowerVM virtualization environment on such physical hosts. VCS mainly ensures high availability of the managed LPARs on which ApplicationHA monitors configured applications.

Note: You can designate only one management LPAR per physical host.

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

See " How ApplicationHA is deployed in the IBM PowerVM environment" on page 11.

Symantec ApplicationHA user privileges

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

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

Symantec ApplicationHA provides the following privileges:

- View Application Monitoring State (Guest)
  Can view the application monitoring status on the managed LPAR. 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 managed LPAR.
- 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 managed LPAR.

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 managed LPARs.

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

- Application agents

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

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

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

  https://sort.symantec.com/agents

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

Licensing Symantec ApplicationHA

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

You have the option to install Symantec products without a license key. Installation without a license does not eliminate the need to obtain a license. A software license is a legal instrument governing the usage or redistribution of copyright protected software. The administrator and company representatives must ensure that a server or cluster is entitled to the license level for the products installed. Symantec reserves the right to ensure entitlement and compliance through auditing.

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

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

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

- Install a license key for the product and features that you want to install.

When you purchase a Symantec product, you receive a License Key certificate. The certificate specifies the product keys and the number of product licenses purchased.

- Continue to install witout 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 59.
  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 59.

You can add or view the license keys from a managed LPAR 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 57.

Ensuring high availability of applications

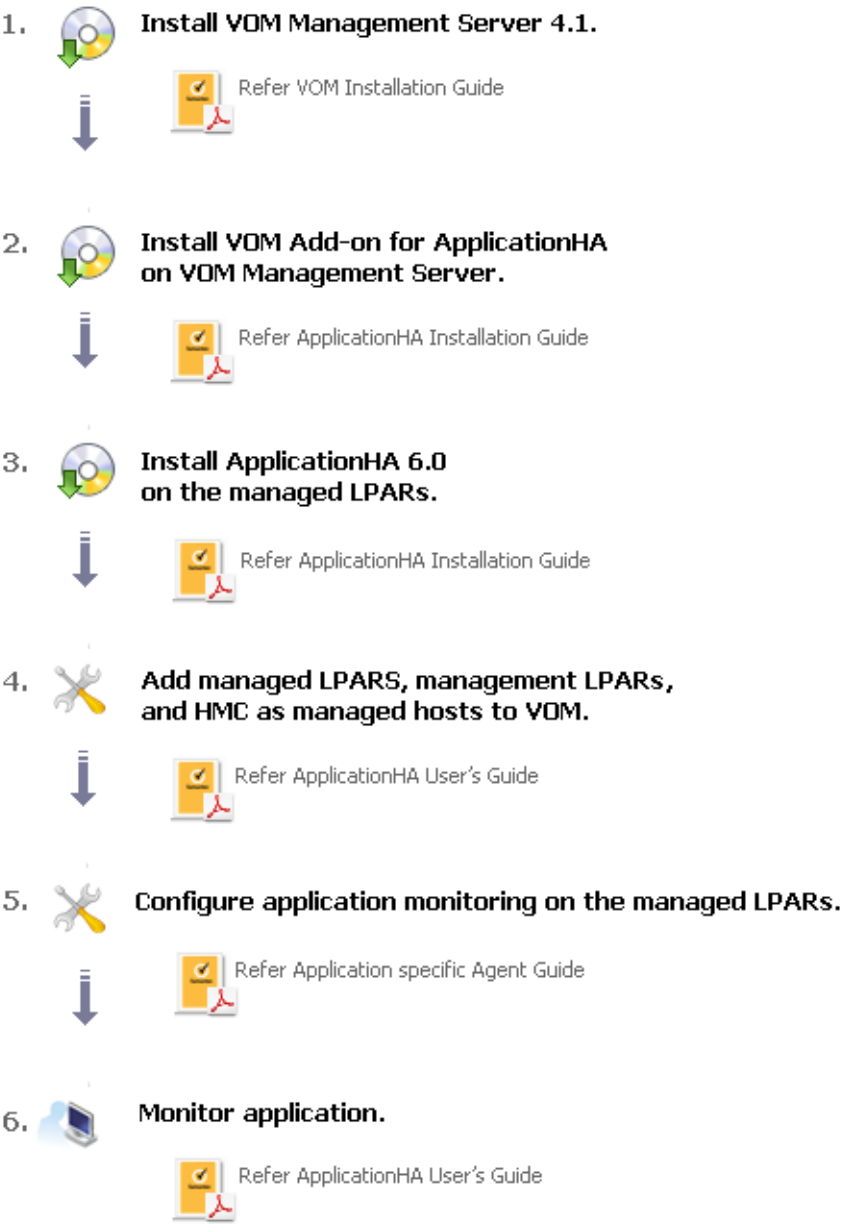
You can ensure high availability of applications running inside managed LPARs by using ApplicationHA. To provide high availability to the applications, perform the following steps:

- Install ApplicationHA on the managed LPAR

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

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

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


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

Ensuring high availability of virtualization infrastructure

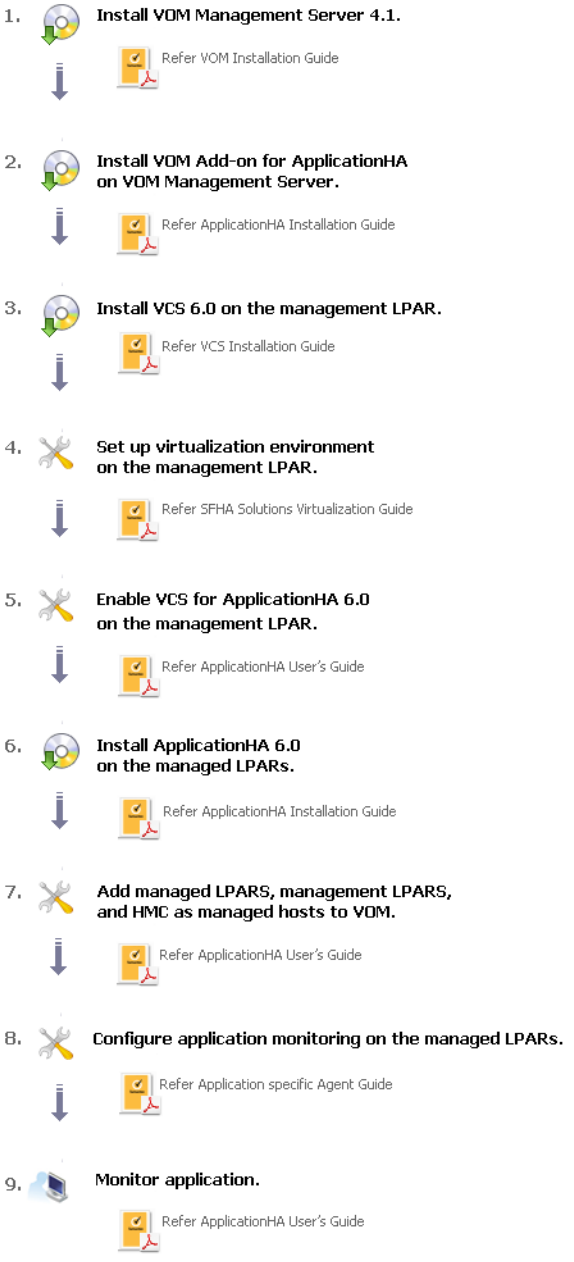
In addition to high availability of applications using ApplicationHA, you can also ensure high availability of the virtualization infrastructure with VCS. By using VCS, you can externally restart managed LPARs and fail over the managed LPARs in case of application failures or managed LPAR failures. To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

- Install VCS in the management LPAR.
- Enable ApplicationHA capabilities in underlying VCS in the management LPAR.
- Install ApplicationHA on the managed LPAR.
- Add managed LPAR and HMC as managed hosts to Veritas Operations Manager (VOM).

  Note: Ensure that Veritas Operations Manager 6.0 Managed Host (MH) 6.0 binaries are installed on the managed LPARs.

- Configure application monitoring on the managed LPAR.

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


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

Chapter 2

Planning to install Symantec ApplicationHA

This chapter includes the following topics:

About installing Symantec ApplicationHA

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

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

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

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

Task	Description
Add required managed LPARs to VOM as managed hosts	In the Home page of the VOM Management Server console, from the Settings menu, add the managed LPARs where you want to monitor applications, as managed hosts in VOM.
Configure application monitoring on the managed LPARs	In the Server perspective of the Management Server console, right-click the managed LPAR (managed host), and select **Manage ApplicationHA** to launch the ApplicationHA management window. In the window, click Configure Application Monitoring to launch the application monitoring configuration wizard.
Administer application monitoring on the managed LPARs	Click the appropriate links in the ApplicationHA management window, to perform administrative actions on configured applications.

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

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

Task	Description
Install VOM Management Server 6.0	Download the installer for VOM Management Server 6.0. The installer is available here: http://sort.symantec.com
Install VCS 6.1on the management LPAR	VCS 6.1 enables you to ensure high availability of the virtualization infrastructure in terms of restart and failover of failed managed LPARs.
Enable ApplicationHA capabilities for underlying VCS 6.1	Run the enable_applicationha script from /opt/VRTSvcs/bin/utils path on each management LPAR. The enable_applicationha script configures the infrastructure settings. It also enables communication between VCS in the management LPAR and ApplicationHA in the managed LPARs.

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

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

Support for centralized installations using the Deployment Server

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

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

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

- Version checking

- Release image management
- Install or upgrade systems
- Update metadata and preferences

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

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

Requirements for installing ApplicationHA on managed LPARs

You can install Symantec ApplicationHA Guest Components on managed LPARs running AIX. The managed LPAR where you want to install ApplicationHA Guest Components must meet the following requirements.

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

Supported virtualization environments

Symantec ApplicationHA can be installed and run inside managed LPARs in a IBM PowerVM virtualization environment, having:

- HMC 7.2.0.0 or later
- VIOS 2.1.3.10-FP-23 or later

Supported operating systems on managed LPARs

This section lists the supported operating systems for Symantec ApplicationHA 6.1.

Table 2-3 shows the supported operating systems for this release.

Table 2-3 Supported guest operating systems

Operating systems	Levels	Chipsets
AIX 7.1	TL0 or later	Any chipset that the operating system supports
AIX 6.1	TL5 or later	Power 7, Power 6, or earlier

Supported applications

Table 2-4 lists the applications that ApplicationHA Agent Pack currently supports on managed LPARs.

Table 2-4 ApplicationHA Agent Pack supported applications

Application	Version	Document
Oracle Database	10gR2, 11gR1, and 11gR2	*Symantec ApplicationHA Agent for Oracle Configuration Guide*
Apache HTTP server	1.3, 2.0, and 2.2. Also supports IBM HTTP Server 7.x.	*Symantec ApplicationHA Agent for Apache HTTP server Configuration Guide*
DB2	9.5 and 9.7	*Symantec ApplicationHA Agent for DB2 Configuration Guide*

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 managed LPARs:

- You must have root privileges on the managed LPAR where you install the guest components.
  In case of remote installation, you must also have root privileges on all the managed LPARs where you install the ApplicationHA guest components.

Ports and firewall settings for application high availability

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

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 (xprtld)	5634	Allow inbound and outbound	Used for communications between the VOM Console and the managed LPARs.
Veritas Operations Manager (VOM)	14161	Allow inbound and outbound	Used by the Tomcat server on VOM Console to receive Web service requests and for local administration.

Requirements for providing high availability of virtualization environment

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

- Install VCS on the management LPAR. For each physical server, you can have only one management LPAR running VCS.
  Refer to *Symantec Cluster Server Installation Guide - AIX*
- Review the settings of the virtualization environment for which you want to provide high availability
  Refer to *Symantec Storage Foundation and High Availability Solutions Virtualization Guide - AIX*
- Symantec recommends that you set the autorestart attribute of the managed LPARs to false, to allow VCS to control it.
- Ensure that SSH communication with management LPAR, is enabled on HMC
- Enable ApplicationHA capabilities for underlying VCS.
  Refer to *Symantec ApplicationHA User's Guide - AIX on IBM PowerVM*

Ports and firewall settings for virtualization infrastructure high availability

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

Table 2-6 displays the services and ports used by ApplicationHA for providing high availability of the virtualization environment.

Table 2-6 Services and ports used by Symantec ApplicationHA

Component Name	Port	Settings	Description
Veritas Storage Foundation Messaging Service (xprtld)	5634	Allow inbound and outbound	Used for communications between the VOM Console host machine and the managed LPARs.
Veritas Operations Manager (VOM)	14161	Allow inbound and outbound	Used by the Tomcat server on VOM Console to receive Web service requests and for local administration.
Internal communication component	14142	Allow inbound and outbound	Used for communication between, VCS in the management LPAR and ApplicationHA in the managed LPAR

Additional requirements

The following additional software requirements apply:

- Internet Explorer or Firefox Web browser is required on the systems where you access the Veritas Operations Manager console to manage the managed LPARs.
  Microsoft Internet Explorer 6.x, 7.x, 8.x, and 9.x are supported.
  Mozilla Firefox 3.x, 4.x, 5.x, and 6.x are supported.
- Adobe Flash Player
  Install Adobe Flash Player (version 9.0 or later) on the systems from where you access the Veritas Operations Manager console to manage the managed LPARs.
- 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 57.
- When installing Symantec ApplicationHA, ensure that there are no parallel installations in progress.

Chapter 3

Installing Symantec ApplicationHA Guest Components

This chapter includes the following topics:

About preparing to install Symantec ApplicationHA guest components

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

- See "Supported virtualization environments" on page 25.
- See "Supported operating systems on managed LPARs" on page 25.
- See "Supported applications" on page 26.
- See "Permissions requirements" on page 26.
- See "Ports and firewall settings for application high availability" on page 26.

- See "Additional requirements" on page 28.

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 30.
Set the PATH variable	See "Setting the PATH variable" on page 31.
Mount the product disc	See "Mounting the product disc" on page 31.
Verify the system before installation	See "Performing an automated preinstallation check" on page 32.

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 AIX operating system:

   ```
   # cd cdrom_root/applicationha
   ```

Performing an automated preinstallation check

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

To check the system

1 Navigate to the folder that contains the installation program.

See "Mounting the product disc" on page 31.

2 Start the preinstallation check:

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

The program proceeds in a non-interactive mode to examine the system for licenses, filesets, 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 managed LPARs running the AIX operating system:

Table 3-2 ApplicationHA installation methods

Method	Description
Interactive installation using the installation program	The install program asks you a few questions and installs ApplicationHA, based on the information you provide. One of the options is directly installing ApplicationHA using the install program, which internally uses the installapplicationha61 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 managed LPARs.
Manual installation using the AIX commands and utilities	You can install ApplicationHA using the operating system `installp -a` command.

Installing Symantec ApplicationHA using the install program

Note: The system from where you install ApplicationHA must run the same AIX distribution as the target managed LPARs.

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 31.

2. Navigate to the folder that contains the installation program for the AIX operating system:

   ```
   # cd cdrom_root/applicationha
   ```

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

   ```
   # ./installapplicationha61
   ```

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

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

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

   The install program does the following:

   - Checks that the local system that runs the install program can communicate with the remote system.
     If the install program finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
     If the default communication method ssh fails, the install program attempts to use rsh.
   - Makes sure the system uses one of the supported operating systems.
     See "Supported operating systems on managed LPARs" on page 25.
   - 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.
- 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 filesets already exist on a system.
  If the current version of any filesets exists, the install program removes the filesets from the installation list for the system.

6 Review the list of filesets that the install program would install on the managed LPAR.

The install program installs the ApplicationHA filesets 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 filesets 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 36.

Installing Symantec ApplicationHA using response files

When you install ApplicationHA on a managed LPAR using the install program, it generates a response file. You can use the response file to install ApplicationHA on other managed LPARs. 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 managed LPARs” on page 25.

2. Make sure the preinstallation tasks are completed.

   See “Performing preinstallation tasks” on page 30.

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 37.

   See “Sample response file for installing Symantec ApplicationHA” on page 39.

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 filesets. (Required)
CFG{systems}	List	Name of the systems on which the product is to be installed. (Required)

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

Variable	List or Scalar	Description
CFG{prod}	Scalar	Defines the product to be installed. The value is APPLICATIONHA61. (Required)
CFG{keys} {system}	Scalar	List of keys to be registered on the system. (Optional)
CFG{opt}{vxkeyless}	Scalar	Specifies whether you want to install a keyless license. CFG{opt}{vxkeyless} = 1 indicates that you want to install a keyless license. (Optional)
CFG{uploadlogs}	Scalar	Specifies whether the installer log files must be uploaded to the telemetrics server for troubleshooting. (Optional)
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of the ssh keyfile that is used to communicate with the remote system. (Optional)
CFG{opt}{pkgpath}	Scalar	Defines a location, typically an NFS mount, from which the remote system can install product filesets. The location must be accessible from the target system. (Optional)

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

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

Sample response file for installing Symantec ApplicationHA

Review the response file variables and their definitions.

See "Response file variables to install Symantec ApplicationHA" on page 37.

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;
```

Chapter 4

Performing post-installation tasks

This chapter includes the following topics:

Accessing the Symantec ApplicationHA documentation

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

To make the ApplicationHA documentation accessible from managed LPARs

1. Navigate to the folder that contains the PDF version of the documents for the AIX operating system:

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

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

   ```
   # cp -rp docs /opt/VRTS/docs
   ```

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

https://sort.symantec.com

Removing permissions for communication

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

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

Chapter 5

Upgrading Symantec ApplicationHA

This chapter includes the following topics:

About upgrading Symantec ApplicationHA

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

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

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

- Back up all your data.
- Ensure that you meet the required prerequisites.
  See “About installing Symantec ApplicationHA” on page 22.
- Review the licensing details.
  See “Licensing Symantec ApplicationHA ” on page 16.
- Review the supported upgrade matrix
  See “Upgrade matrix” on page 44.

Table 5-1 provides the details for upgrading ApplicationHA components.

Table 5-1 ApplicationHA upgrade details

Component	Upgrade details
Guest	You can upgrade the guest components by using any of the following methods: For upgrading by using the installer (interactive mode) See "Upgrading Symantec ApplicationHA using the install program" on page 44. For upgrading by using response files See "Upgrading Symantec ApplicationHA using response files" on page 47.

Upgrade matrix

Table 5-2 provides the supported scenarios for upgrading ApplicationHA Guest Components.

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

Upgrade from	Upgrade to	Operating system
ApplicationHA 6.0 Guest Components	ApplicationHA 6.1 Guest Components	AIX 6.1 and AIX 7.1

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

Upgrading Symantec ApplicationHA using the install program

Perform the following steps to upgrade ApplicationHA:

Note: The system from where you upgrade ApplicationHA must run the same AIX distribution as the target managed LPARs.

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 31.

2. Navigate to the folder that contains the installation program for the AIX operating system:

   ```
   # cd cdrom_root/applicationha
   ```

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

   ```
   # ./installapplicationha61
   ```

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

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

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

   The install program does the following:

   - Checks that the local system that runs the install program can communicate with the remote system.
     If the install program finds ssh binaries, it confirms that ssh can operate without requests for passwords or passphrases.
     If the default communication method ssh fails, the install program attempts to use rsh.
   - Makes sure the system uses one of the supported operating systems.
     See "Supported operating systems on managed LPARs" on page 25.
   - 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.
   - 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 filesets already exist on a system.
  If the current version of any filesets exists, the install program removes the filesets from the installation list for the system.

6 Review the list of filesets that the install program would upgrade on each managed LPAR.

The install program upgrades the ApplicationHA filesets 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 filesets 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 47.

Upgrading Symantec ApplicationHA using response files

When you upgrade ApplicationHA on a managed LPAR using the install program, it generates a response file. You can use the response file to upgrade ApplicationHA on other managed LPARs. 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 managed LPARs" on page 25.

2. Make sure the preinstallation tasks are completed.

   See "Performing preinstallation tasks" on page 30.

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 48.

   See "Sample response file for Upgrading Symantec ApplicationHA" on page 50.

   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 AIX disc, use the following command:

   ```
   # cd /cdrom_root/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 filesets. (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 *rsh* must be used instead of ssh as the communication method between systems. (Optional)
CFG{opt}{keyfile}	Scalar	Defines the location of the ssh keyfile that is used to communicate with the remote system. (Optional)
CFG{opt}{tmppath}	Scalar	Defines the location where a working directory is created to store temporary files and the depots that are needed during the install. The default location is /var/tmp. (Optional)

Table 5-3 Response file variables specific to upgrading 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 *logpath* location. (Optional)

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 48.

For permanent license:

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

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{prod}="APPLICATIONHA61";
$CFG{systems}=[ qw(system1) ];
$CFG{keys}{'systemname'}=["LICENSEKEY"];
$CFG{uploadlogs}=1;
```

For keyless license:

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

$CFG{accepteula}=1;
$CFG{opt}{upgrade}=1;
$CFG{opt}{installall pkgs}=1;
$CFG{prod}="APPLICATIONHA61";
$CFG{systems}=[ qw(system1) ];
```

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

Chapter 6

Uninstalling Symantec ApplicationHA Guest Components

This chapter includes the following topics:

Preparing to uninstall Symantec ApplicationHA

Before you uninstall ApplicationHA from any managed LPAR:

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

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

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

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

The uninstallapplicationha program removes all ApplicationHA filesets.

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

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 managed LPAR.
3. Enter the name of the systems from which you want to uninstall ApplicationHA.

   The program performs the following:

   - Verifies the communication between systems
   - Checks the installation on the system to determine the filesets 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 filesets.

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

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/applicationha/
```

For information on how to use the uninstallapplicationha program:

See "Uninstalling Symantec ApplicationHA using the uninstall program" on page 53.

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 managed LPAR.

To perform automated ApplicationHA uninstallation

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

   See "Preparing to uninstall Symantec ApplicationHA" on page 52.

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

   See "Sample response file for uninstalling Symantec ApplicationHA" on page 56.

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

   See "Response file variables to uninstall Symantec ApplicationHA" on page 55.

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 filesets. (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)
CFG{opt}{rsh}	Scalar	Defines that *rsh* must be used instead of ssh 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 /var/tmp. (Optional)
CFG{opt}{logpath}	Scalar	Mentions the location where the log files are to be copied. The default location is /opt/VRTS/install/logs. **Note:** The install program copies the response files and summary files also to the specified *logpath* location. (Optional)

Sample response file for uninstalling Symantec ApplicationHA

Review the response file variables and their definitions.

See "Response file variables to uninstall Symantec ApplicationHA" on page 55.

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

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

Chapter 7

Managing Symantec ApplicationHA licenses

This chapter includes the following topics:

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 a enable the keyless licensing feature from the command line.

See "Managing ApplicationHA licenses from the command line" on page 59.

- Connect to the Veritas Operations Manager console and in the Server perspective, in the left pane expand **Manage**, and in the related Organization or under Uncategorized Hosts, navigate to the managed LPAR where you want to update the licenses. Select the **Symantec High Availability** tab and click **Licenses**. Use this path to manage licenses for the local managed LPAR.

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

- You can also access the Symantec High Availability 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 Symantec High Availability tab

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

To manage the ApplicationHA licenses

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

Managing ApplicationHA licenses through Symantec High Availability view

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

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

To manage the ApplicationHA licenses

1. Connect to the Veritas Operations Manager Mangement Server (VOM MS).
2. In theVOM MS Console, select the Server perspective and expand **Manage** in the left pane.
3. Expand the Organization, or **Uncategorized Hosts** to navigate to the managed LPAR.
4. Right-click the required managed LPAR, and then click **Manage ApplicationHA**.

   The Symantec High Availability view appears.
5. In the Symantec High Availability view, click **Licenses**.
6. On the License Management panel, enter the permanent license key in the **Enter license key** text box and then click **Add**.
7. Click **Close**.

Managing ApplicationHA licenses from the command line

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

To view an existing license:

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

To install a valid license key:

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

To use keyless licensing

1 Navigate to the following directory:

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

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

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

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

```
# ./vxkeyless displayall
```

4 Enable ApplicationHA keyless licensing along with the other products.

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

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

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

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

To remove a keyless license

1 View the current setting for the product license level.

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

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

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

Appendix A

ApplicationHA installation packages

This appendix includes the following topics:

ApplicationHA installation filesets

Table A-1 shows the fileset name and contents for each Symantec Cluster Server fileset.

Table A-1 Symantec ApplicationHA filesets

fileset	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.
VRTSvcs	VRTSvcs contains the following components: ■ The binaries for Symantec Cluster Server. ■ The binaries for Symantec Cluster Server manual pages. ■ The binaries for Symantec Cluster Server English message catalogs. ■ The binaries for Symantec Cluster Server utilities. These utilities include security services.
VRTSvcsag	Contains the binaries for Symantec Cluster Server bundled agents by Symantec.

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

fileset	Contents
VRTSvcsvmw	Contains the ApplicationHA managed LPAR wizards for application monitoring configurations by Symantec.
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).
VRTSvbs	VRTSvbs contains the binaries for Virtual Business Services by Symantec.
VRTSsfcpi61	VRTSsfcpi61 contains the binaries for the Symantec Storage Foundation Common Product Installer. This mandatory fileset contains the scripts that perform the following: ■ Installation ■ Configuration ■ Upgrade ■ Uninstallation ■ Adds nodes ■ Removes nodes You can use this script to simplify the native operating system installations.

Appendix B

Troubleshooting Symantec ApplicationHA installation

This appendix includes the following topics:

Symantec ApplicationHA logging

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

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

ApplicationHA guest components logging

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

When installing ApplicationHA guest components by using the 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 managed LPAR

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

The agent log components are defined as follows:

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

The agent logs are located in the following location:

`/var/VRTSvcs/log/<agent name>_A.txt`

The format of the agent log is as follows:

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

A typical agent log resembles:

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

Veritas Operations Manager Management Server logging

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

The logs are located at the following location:

`/var/opt/VRTSsfmcs/logs`

To set the VOM log levels

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

   You can select one of the following levels:

   - Severe
   - Warning
   - Info
   - Debug
   - Fine

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

Index

U