Symantec™ ApplicationHA Installation and Configuration Guide

Windows Server 2003 (x64)
Windows Server 2008 (x64)

5.1 Service Pack 1

September 30, 2010

Symantec™ ApplicationHA Installation and Configuration 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: 5.1 SP1

Document version: 5.1.SP1.0

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice file accompanying this Symantec product for more information on the Third Party Programs.

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. 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 automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information

- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1 Introducing Symantec ApplicationHA

What is Symantec ApplicationHA? 12

- How Symantec ApplicationHA works with VMware vCenter Server 12
- How Symantec ApplicationHA detects application failures 14

Which applications can I monitor? 15

Components of Symantec ApplicationHA 16

- Symantec ApplicationHA Console 16
- Symantec ApplicationHA guest components for virtual machines 17

Symantec ApplicationHA user privileges 17

Symantec ApplicationHA agents 18

About Symantec ApplicationHA licensing 19

Chapter 2 Installing Symantec ApplicationHA

About installing Symantec ApplicationHA 22

Before installing Symantec ApplicationHA 22

- Disk space requirements 23
- ApplicationHA Console host requirements 23
- Virtual machine requirements 23
- Supported operating systems for virtual machines 24
- Supported VMware versions 25
- Supported applications 25
- Permissions requirements 25
- Ports and firewall settings 26
- Additional requirements 28

Installing Symantec ApplicationHA Console 29

About installing Symantec ApplicationHA guest components for virtual machines 32

- Installing ApplicationHA guest components using the installation wizard 33
- Installing ApplicationHA guest components using the command line interface 36
  - Example: ApplicationHA guest components command line installation 39

Configuring single sign-on between the virtual machine and the ApplicationHA Console 40
Configuring VMware HA settings 41
Configuring Symantec ApplicationHA access control 42
Configuring application monitoring for ApplicationHA Console 43

Chapter 3 Configuring application monitoring with Symantec ApplicationHA

About configuring application monitoring with Symantec ApplicationHA 46
Before configuring application monitoring 47
Configuring application monitoring for services, processes, and mount points 48
Configuring additional parameters for monitoring services 52
Configuring additional parameters for monitoring processes 53
Administering application monitoring from ApplicationHA view 56
To configure or unconfigure application monitoring 57
To view the status of configured applications 58
To start or stop applications 59
To enable or disable application heartbeat 59
To suspend or resume application monitoring 60
Administering application monitoring settings 61
Administering plugin registration using the PluginMgmt.bat utility 63
Considerations while administering virtual machines 65
Backing up ApplicationHA Console files and registry 66

Chapter 4 Uninstalling Symantec ApplicationHA

Uninstalling Symantec ApplicationHA guest components from the virtual machines 68
Uninstalling Symantec ApplicationHA Console 70

Appendix A Symantec ApplicationHA agents

About the Symantec ApplicationHA infrastructure agents 76
About the Heartbeat agent 77
Hearbeat agent function 77
Hearbeat agent state definitions 77
Hearbeat agent resource type definition 77
Hearbeat agent attribute 78
About the MountMonitor agent 79
MountMonitor agent function 79
MountMonitor agent state definitions 79

MountMonitor agent resource type definition 79
MountMonitor agent attributes 80
About the GenericService agent 81
GenericService agent functions 81
GenericService agent state definitions 81
GenericService agent resource type definition 81
GenericService agent attributes 82
About the Process agent 84
Process agent functions 84
Process agent state definitions 84
Process agent resource type definition 84
Process agent attributes 85
About the FileNone agent 89
FileNone agent function 89
FileNone agent state definitions 89
FileNone agent resource type definition 89
FileNone agent attribute 89
About the ElifNone agent 90
ElifNone agent function 90
ElifNone agent state definitions 90
ElifNone agent resource type definition 90
ElifNone agent attribute 90
About the FileOnOff agent 91
FileOnOff agent functions 91
FileOnOff state definitions 91
FileOnOff agent resource type definition 91
FileOnOff agent attribute 91
About the FileOnOnly agent 92
FileOnOnly agent functions 92
FileOnOnly state definitions 92
FileOnOnly agent resource type definition 92
FileOnOnly agent attribute 92

Appendix B Troubleshooting Symantec ApplicationHA installation and configuration

Symantec ApplicationHA logging 94
ApplicationHA installer logging 94
ApplicationHA Console logging 94
ApplicationHA view logging 95
Agent logging 96
Symantec ApplicationHA plugin registration error 97
Symantec ApplicationHA tab does not display the application monitoring status 98

Symantec ApplicationHA tab displays the “Unable to retrieve the status of this virtual machine.” error 98
Symantec ApplicationHA tab displays a “Failed to retrieve status.” popup message 99
Symantec ApplicationHA Configuration Wizard displays blank 100
ApplicationHA Console files become corrupt 100
ApplicationHA Console host becomes permanently unavailable 102
VMware vCenter Server becomes permanently unavailable 103

Appendix C Repairing Symantec ApplicationHA installation

Repairing the Symantec ApplicationHA Console installation 106
Repairing Symantec ApplicationHA guest component installation on a virtual machine 109
License management 111

Index 113

Chapter 1

Introducing Symantec ApplicationHA

This chapter includes the following topics:

- "What is Symantec ApplicationHA?" on page 12
- "Which applications can I monitor?" on page 15
- "Components of Symantec ApplicationHA" on page 16
- "Symantec ApplicationHA user privileges" on page 17
- "Symantec ApplicationHA agents" on page 18
- "About Symantec ApplicationHA licensing" on page 19

What is Symantec ApplicationHA?

Symantec ApplicationHA 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.

Symantec ApplicationHA is based on Veritas™ 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 Global Atomic Broadcast (GAB) and Low Latency Transport (LLT). Symantec ApplicationHA has a lightweight server footprint that allows faster installation and configuration.

Key benefits include:

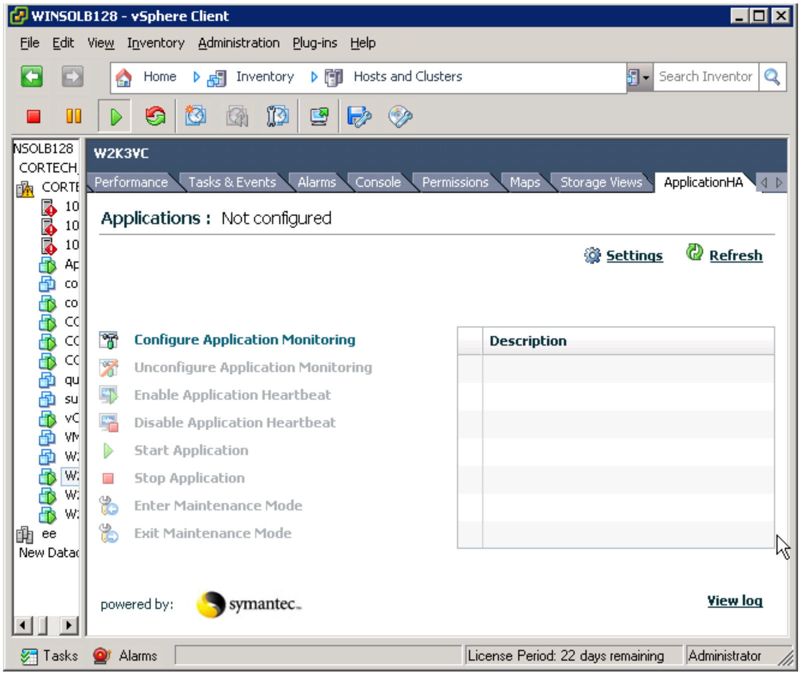
- Out of the box integration with the VMware vCenter Server HA
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside virtual machines
- Standardized way to manage applications using a single interface that is integrated with VMware vSphere Client

How Symantec ApplicationHA works with VMware vCenter Server

Symantec ApplicationHA communicates directly with VMware HA. ApplicationHA conveys the application health status in the form of an application heartbeat. This allows VMware HA to automatically reset or restart a virtual machine if the application heartbeat is not received within a specified interval.

Symantec ApplicationHA provides an interface for configuring application monitoring and administering the configured applications. A new tab named ApplicationHA appears in the vSphere Client after you install the ApplicationHA Console. The ApplicationHA tab is the primary interface for performing the application monitoring operations on a virtual machine.

The following figure displays the ApplicationHA tab.



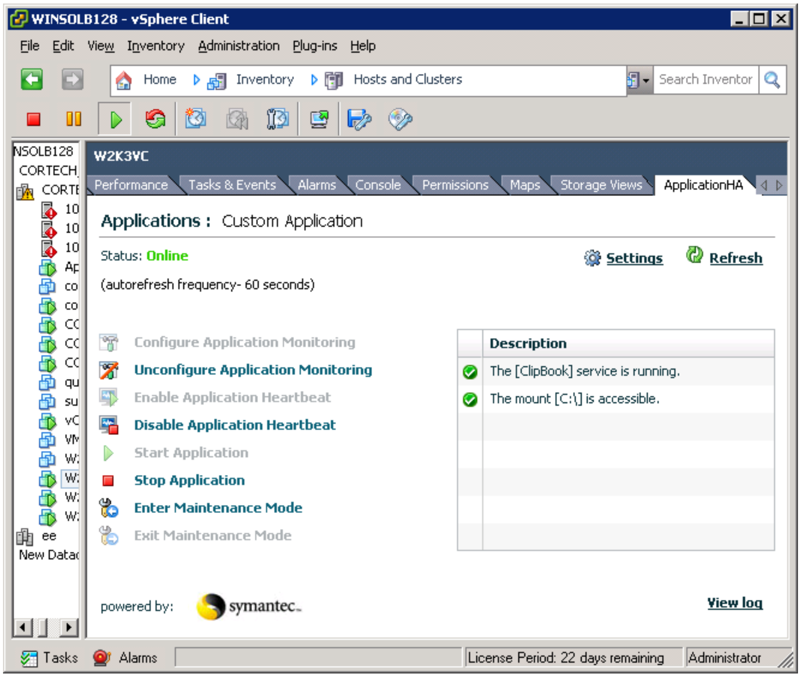
Applications : Not configured

License Period: 22 days remaining

Administrator

From this view you configure application monitoring and then monitor and control the configured application on the virtual machine. After configuring application monitoring, the Symantec ApplicationHA view displays the state of the application.

The following figure displays the ApplicationHA tab where a custom application is configured for monitoring.



Applications : Custom Application

Status: Online

(autorefresh frequency- 60 seconds)

	Description
✓	The [ClipBook] service is running.
✓	The mount [C:\] is accessible.

License Period: 22 days remaining

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 on the virtual machines. Symantec ApplicationHA detects failure of an application by issuing specific commands, tests, or scripts to monitor the overall health of an application. The Symantec ApplicationHA agents ensure that the configured applications are running on the virtual machine.

The ApplicationHA Heartbeat agent is configured when you configure application monitoring. The Heartbeat agent sends the application heartbeat to VMware HA. Symantec ApplicationHA uses the application heartbeat as the communication medium to convey the status of the application to VMware HA.

If an application fails, the agents attempt to restart the application for a configurable number of times. If the agents are unable to start the application, Symantec ApplicationHA stops sending the application heartbeat to VMware HA. Depending on the configuration, VMware HA takes the necessary corrective action. After the virtual machine is restarted, Symantec ApplicationHA agents attempt to start the application and its dependent components in a predefined order.

Which applications can I monitor?

Most applications can be placed under Symantec ApplicationHA control provided the following guidelines are met:

- Defined start, stop, and monitor procedures

  The application to be monitored must have defined procedures for starting, stopping, and monitoring.

Start procedure	The application must have a command to start it and all the dependent components and resources it may require. Symantec ApplicationHA brings up the required resources in a specific order, then brings up the application using the defined start procedure.
Stop procedure	The application must have a command to stop it and all the dependent components and resources. Symantec ApplicationHA stops the required resources in a specific order, then stops the application using the defined stop procedure.
Monitor procedure	The application must have a monitor procedure that determines if the specified application instance is healthy. The application must allow individual monitoring of unique instances. For example, in a database environment, the monitoring application can connect to the database server and perform SQL commands to verify read and write access to the database. The closer a test comes to matching what a user does, the better the test is in discovering problems. You should balance the level of monitoring between ensuring that the application is up and minimizing monitor overhead.

- Ability to restart the application in a known state

  When the application is stopped, it must close out all tasks, store data properly, and then exit. When Symantec ApplicationHA attempts to restart the application, it should be able to start from the last known state. In case of a server crash, the application must be able to recover gracefully.

  Commercial databases such as SQL Server and Oracle are good examples of well-written, crash-tolerant applications. On any client request, the client is responsible for holding the request until it receives acknowledgement from the server. When the server receives a request, it is placed in a special redo log file. The database confirms that the data is saved before it sends an acknowledgement to the client.

After a server crashes, the database recovers to the last-known committed state by mounting the data tables and applying the redo logs. This returns the database to the time of the crash. The client resubmits any outstanding client requests that are unacknowledged by the server, and all others are contained in the redo logs.

Components of Symantec ApplicationHA

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

- Symantec ApplicationHA Console
- Symantec ApplicationHA guest components for virtual machines

Symantec ApplicationHA Console

The ApplicationHA Console is installed separately in the Symantec ApplicationHA monitoring environment and resides on a separate virtual machine or a physical machine.

The ApplicationHA Console performs the following functions:

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

  This plugin is required to view the ApplicationHA tab in the vSphere Client. You can use the ApplicationHA tab to configure application monitoring, control application start and stop, and monitor the application status on a virtual machine.

- The ApplicationHA 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.

  For security reasons, the Console requires the virtual machine administrator account for establishing a trust relationship. It uses the administrator credentials to set up a permanent account that is used for performing various application monitoring operations on the virtual machine.

- 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 encyrpt 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.

Symantec ApplicationHA guest components for virtual machines

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

The guest components also include the Veritas Storage Foundation Messaging Service (xprtld). This service communicates the application monitoring status on the virtual machine and displays it in the ApplicationHA tab.

Symantec ApplicationHA user privileges

Symantec ApplicationHA provides a set of privileges that are available after you install the ApplicationHA Console. These privileges are the application monitoring operations that a user can perform on the virtual machine. You can create roles and then assign these privileges to them or assign these 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 configured for applications and components on a system. The agents are installed when you install Symantec ApplicationHA. These agents start, stop, and monitor the resources configured for the applications and report state changes. If an application and its components fail, these agents also restart the applications and its resources on the virtual machine.

Symantec ApplicationHA agents are classified as follows:

- Infrastructure agents

  Infrastructure agents are packaged (bundled) with the base software and include agents for mount points, generic services, and processes. These agents are immediately available for use after you install Symantec ApplicationHA.

  See "About the Symantec ApplicationHA infrastructure agents" on page 76.

- Application agents

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

  An agent pack is released on a quaterly 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 Veritas Operations Services (VOS) Web site for information on the latest agent pack availability.

  http://vos.symantec.com

This guide includes information about the infrastructure agents. See the agent-specific configuration guide for more details about the application agents.

About Symantec ApplicationHA licensing

Symantec ApplicationHA is a licensed product. Licensing for Symantec ApplicationHA is based on the server operating systems in use. A license is required for each system that runs any of the Symantec products.

An evaluation license key is embedded in the product. This license key is valid only for a limited evaluation period. You can use the embedded Symantec ApplicationHA license key or enter a key while installing the product.

The product installer lets you add and remove specific licenses. Use the Windows Add or Remove Programs to launch the Symantec ApplicationHA installer and then choose the License option.

Chapter 2

Installing Symantec ApplicationHA

This chapter includes the following topics:

- "About installing Symantec ApplicationHA" on page 22
- "Before installing Symantec ApplicationHA" on page 22
- "Installing Symantec ApplicationHA Console" on page 29
- "About installing Symantec ApplicationHA guest components for virtual machines" on page 32
- "Configuring single sign-on between the virtual machine and the ApplicationHA Console" on page 40
- "Configuring VMware HA settings" on page 41
- "Configuring Symantec ApplicationHA access control" on page 42
- "Configuring application monitoring for ApplicationHA Console" on page 43

About installing Symantec ApplicationHA

Installing and setting up Symantec ApplicationHA in a VMware virtualization environment involves the following tasks:

- **Installing Symantec ApplicationHA Console**
  Install the ApplicationHA Console on a separate physical or virtual machine. This installation registers the ApplicationHA plugin on the vCenter Server. After installation, the ApplicationHA tab is added to the vSphere Client. Use the ApplicationHA view to configure and control application monitoring on virtual machines that are managed from the VMware vCenter Server.
- **Installing Symantec ApplicationHA guest components for virtual machines**
  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.
- **Editing VMware VM monitoring settings to enable application monitoring**
  After installing Symantec ApplicationHA components, you must manually edit the VM monitoring settings to enable application monitoring.
  This involves the following tasks:
  - Editing the VM cluster settings from the vSphere Client
    You manually change these settings from the vSphere Client.
  - Editing the settings from each virtual machine.
    These settings are automatically modified by the Symantec ApplicationHA Configuration Wizard when you configure application monitoring for an application.

Before installing Symantec ApplicationHA

Review the following requirements before installing Symantec ApplicationHA in a VMware virtualization environment:

- Disk space requirements
- ApplicationHA Console host requirements
- Virtual machine requirements
- Supported operating systems for virtual machines
- Supported applications
- Permissions requirements
- Ports and firewall settings

- Additional requirements

Disk space requirements

Table 2-1 provides the minimum disk space requirements for the Symantec ApplicationHA components.

Table 2-1 Symantec ApplicationHA disk space requirements

Component	Disk space required
ApplicationHA Console components	350 MB
ApplicationHA guest components for virtual machine	300 MB

ApplicationHA Console host requirements

The following prerequisites apply to the machine that hosts the ApplicationHA Console:

- You can install the ApplicationHA Console on a physical or a virtual machine.
  If you wish to configure application monitoring for the ApplicationHA Console itself, the host must be a virtual machine.
- The ApplicationHA Console host must run Windows Server 2008 or Windows Server 2008 R2 (latest service packs supported).
  Windows Server 2003 is not supported for the ApplicationHA Console host.
- Memory must be a minimum 1 GB of RAM in addition to the recommended memory for the server operating system.
- Ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.
  See "Ports and firewall settings" on page 26.

Virtual machine requirements

The following prerequisites apply to the virtual machines where you install the Symantec ApplicationHA guest components:

- Memory must be a minimum 1 GB of RAM per server.
- Ensure that the Remote Registry and Windows Management Instrumentation (WMI) services are set to automatic and running (the default setting).

- For remote installations on Windows Server 2008 systems, ensure that the Computer Browser Service is set to automatic and running.
- Ensure that VMware Tools is installed. Install the version that is the similar to or later than that available with VMware ESX 4.1.
- Ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.
  See "Ports and firewall settings" on page 26.
- Ensure that ICMP, Windows Management Instrumentation (WMI) service, and Remote Registry service are included in the firewall exceptions list.

Supported operating systems for virtual machines

Table 2-2 lists the operating systems that Symantec ApplicationHA currently supports on virtual machines.

Table 2-2 Symantec ApplicationHA supported operating systems

Server	Architecture	Edition	Service Pack
Windows Server 2003	x64	Standard Edition, Enterprise Edition, Datacenter Edition	SP2 required
Windows Server 2003 R2	x64	Standard Edition, Enterprise Edition, Datacenter Edition	SP2 required
Windows Server 2003 R2	x64	Small Business Server	SP2 required
Windows Server 2008	x64	Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition, Small Business Server	SP1 required SP2 supported
Windows Server 2008 R2	x64	Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition	

Supported VMware versions

The following VMware Servers and management clients are currently supported:

- VMware ESX Server version 4.1
- VMware ESXi Server version 4.1
- VMware vCenter Server version 4.1
- VMware vSphere Client version 4.1

Supported applications

Table 2-3 lists the applications that Symantec ApplicationHA currently supports on virtual machines.

Table 2-3 Symantec ApplicationHA supported applications

Application	Architecture	Edition	Service Pack
Microsoft Exchange Server 2010 (Mailbox Server role required)	x64	Standard Edition, Enterprise Edition	
Microsoft SQL Server 2008 and SQL Server 2008 R2	x86, x64	Standard Edition, Enterprise Edition, Web Edition	
Internet Information Server (IIS) 6.0 and later versions			
Custom applications and generic services			

Permissions requirements

The following permissions are required for installing ApplicationHA Console:

- The logged-on user must have local administrator privileges on the system where you install ApplicationHA Console.
- During the installation the installer prompts for a user name and password. This user account must have the privileges to extend the vSphere Client. (Register extension and Unregister extension checkboxes under the Extension privilege in Edit Role box)
  The installer uses this account to register the ApplicationHA plugin on the specified vCenter Server.

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

- The logged-on user must have local administrator privileges on the virtual machine where you install the guest components.
  In case of remote installation, the user must also have local administrator privileges on all the virtual machines where you install the guest components.
- Depending on the selection, 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

Symantec 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.

Table 2-4 displays the services and ports used by Symantec ApplicationHA.

Table 2-4 Services and ports used by Symantec ApplicationHA

Component Name	Port/Protocol	Settings	Description
Services used by Symantec ApplicationHA installer			
File and Printer Sharing		Allow inbound and outbound	Used by the installer to copy the installation files to the machine.
Windows Management Instrumentation (WMI) service		Allow inbound and outbound	Used by the installer to discover virtual machines.
Ports and services used by Symantec ApplicationHA Console			
VMware Web Service	443 (Default port)	Allow inbound and outbound	Used by the installer to register ApplicationHA plugin and add ApplicationHA privileges to the vCenter Server.

Table 2-4 Services and ports used by Symantec ApplicationHA

Component Name	Port/Protocol	Settings	Description
Symantec ApplicationHA Service	14152	Allow inbound and outbound	Used by the ApplicationHA Console host to run Java Servlets that fetch the application monitoring status from the virtual machines and display the information on the ApplicationHA tab in the vSphere Client.
Symantec ApplicationHA Authentication Service	14153	Allow inbound and outbound	Used by the ApplicationHA Console to authenticate the single sign-on account configured for a virtual machine.
Ports and services used by Symantec ApplicationHA Console and guest components (virtual machines)			
Veritas Storage Foundation Messaging Service (xprtld)	5634 / https	Allow inbound and outbound	Used for communications between the ApplicationHA Console host machine and the virtual machines.

Additional requirements

The following additional software requirements apply:

- Microsoft Internet Explorer version 6.0 or later

  No other browsers are currently supported.

- To view the ApplicationHA tab in the vSphere Client, verify that the following settings in your Internet Explorer (IE) browser are enabled:

  Tools > Internet Options, Advanced tab

  - Use SSL 2.0
  - Use SSL 3.0
  - Use TLS 1.0

  Tools > Internet Options, Security tab

  - Active scripting
  - Run ActiveX controls and plug-ins
  - Script ActiveX controls marked safe for scripting

- Installation media and licenses for all products and third-party applications.

- Adobe Flash Player

  Install Adobe Flash on the systems from where you run the VMware vSphere Client to manage the virtual machines.

- Symantec ApplicationHA license

  An evaluation key is embedded in the product and is valid for two months. You can use all the product features during that period.

  To continue unrestricted usage, you must procure a valid license key.

- When installing Symantec ApplicationHA, ensure that there are no parallel installations, live updates, or Microsoft Windows updates in progress.

Installing Symantec ApplicationHA Console

Use the Symantec ApplicationHA installer to install Symantec ApplicationHA Console in your VMware virtualization environment.

Consider the following before you proceed:

- The installation must be run locally. Remote install is not supported.
- You can install the ApplicationHA Console on Windows Server 2008 or Windows Server 2008 R2 servers only.
- You can install the ApplicationHA Console on a dedicated physical host or a virtual machine or on the vCenter Server itself. If you wish to configure application monitoring for ApplicationHA Console, you must install on a virtual machine.
- The installer uses the logged-on user account context to perform the installation. Verify that the logged-on user has local administrator privileges on the machine where you want to install the server.
- As part of the server installation, the installer registers the Symantec ApplicationHA plugin for VMware vCenter Server.

  If the Symantec ApplicationHA plugin is already registered on a vCenter Server due to an earlier server installation, you must first uninstall the existing server and verify that the plugin is unregistered from the vCenter Server.
- Symantec ApplicationHA supports one ApplicationHA Console per vCenter Server. If you have multiple vCenter Servers in your virtualization environment, you must install and configure separate ApplicationHA Console instances for each of them.

Perform the following steps to install Symantec ApplicationHA Console using the installation wizard.

To install ApplicationHA Console using the installation wizard

1. From the machine identified to serve as the ApplicationHA Console, navigate to the Symantec ApplicationHA software package directory and run **Setup.exe** to launch the installer.
2. On the Symantec ApplicationHA Installer, click **Install** under ApplicationHA Console to launch the installation wizard.
3. Review the prerequisites on the Welcome panel and then click **Next**.
4. Read the Symantec Software License Agreement, click **I accept the terms of License Agreement**, and then click **Next**.

5 On the VMware vCenter Server Details panel, specify the vCenter Server details and then click **Next**.

Provide the following details:

ApplicationHA Console IP	Select the IP address of the local system from the drop-down list. This is the IP of the machine where you will install the ApplicationHA Console. The drop-down list may display several IPs if the system has multiple network adapters each with a unique IP address assigned. Select the host IP address that is accessible from the vCenter Server.
vCenter Server Name or IP	Specify the host name or IP address of the VMware vCenter Server. Ensure that the specified vCenter Server host name or IP address is accessible from the machine where you are installing ApplicationHA Console.
Web Service Https Port	Specify the https port used by the VMware Web Service. The default port number is 443.
User Name	Specify the name of the user account that has the privileges to extend the vSphere Client. The installer uses this account to register the ApplicationHA plugin on the vCenter Server.
Password	Specify the password for the user account specified in the User Name field.

6 On the System Validation panel, the installer automatically selects the local host for installation and begins verification.

After the status shows as *Ready for Install*, click **Next**.

The wizard uses `%Program Files%\Veritas` as the default installation directory. To change the directory, click the folder icon next to the system and then choose the installation directory.

The wizard performs validation checks such as the available disk space on the machine. If the machine does not meet the required criteria, the status is reflected as *Failed verification.* To view the cause of a validation failure, click the Information icon for the system. Rectify the issue and then click **Re-verify** to perform the validation checks on the rejected system again.

The wizard does not proceed unless the selected system has passed the validation checks.

7. On the Pre-install Summary panel, review the pre-installation summary and then click **Next**.

   Click **Save Report** if you wish to save the pre-installation summary report for reference.

8. The Installation panel displays the progress of the installation.

   After the panel indicates that the installation is complete, click **Next**.

9. On the Post-install Summary panel, review the installation results and then click **Next**.

   The wizard configures the required services and registers the Symantec ApplicationHA plugin on the specified vCenter Server.

   If the installation has failed on the system, review the post-install summary report and refer to the wizard log file for details.

   The log file is located at

   `%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>.`

   You may have to repeat the installation if the wizard indicates that the install itself has failed.

   If the logs indicate that the Symantec ApplicationHA plugin registration has failed, you may have to manually register the plugin on the vCenter Server. Use the PluginMgmt.bat utility to register the plugin.

   Refer to the configuration section for details about the PluginMgmt.bat utility.

10. On the Finish panel click **Finish**.

    This completes the installation of Symantec ApplicationHA Console.

11. This step is applicable only if you have re-installed Symantec ApplicationHA Console in your monitoring environment.

    After completing the installation, the ApplicationHA tab may fail to retrieve the application status. In such a case, you may have to close the ApplicationHA tab and open it again.

    In the vSphere Client, click another virtual machine, then click the original virtual machine again and then select the ApplicationHA tab, or exit the vSphere Client and launch it again.

    The ApplicationHA view then displays the status of the configured applications on the virtual machine.

About installing Symantec ApplicationHA guest components for virtual machines

Install the Symantec ApplicationHA guest components on the virtual machines where you wish to monitor applications.

Refer to the following procedures:

- For installing using the installation wizard

  See "Installing ApplicationHA guest components using the installation wizard" on page 33.

- For installing using the command line interface (CLI)

  See "Installing ApplicationHA guest components using the command line interface" on page 36.

Consider the following before you proceed:

- 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.
- The installer allows remote installation. You can launch the installer from any system in your network or directly on any of the virtual machines.

  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.
- The installer currently supports installation on up to 32 virtual machines at a time. If you wish to install on additional systems, you must first complete the installation on 32 systems, and then run the installer again and select the additional systems for installation.

  The installer generates a summary that contains the list of systems where the operation was performed. You can save that report as a reference.
- Remote installation is restricted to systems within a domain or a workgroup. You cannot select systems that are outside a domain. To install on multiple systems in a domain, run the installer from a system in that domain.
- 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.

- Symantec recommends that you first install the ApplicationHA Console before installing the guest components. The ApplicationHA plugin is registered during the ApplicationHA Console installation.

Installing ApplicationHA guest components using the installation wizard

Perform the following steps to use the installation wizard to install the Symantec ApplicationHA guest components on the virtual machines.

To install the ApplicationHA guest components using the installation wizard

1. From the Symantec ApplicationHA software package, run **Setup.exe** to launch the installer.
2. On the Symantec ApplicationHA Installer, click **Install** under Symantec ApplicationHA Guest Components to launch the installation wizard.
3. Review the prerequisites on the Welcome panel and then click **Next**.
4. Read the Symantec Software License Agreement, click **I accept the terms of License Agreement**, and then click **Next**.
5. On the License panel, specify the appropriate licensing details and then click **Next**:

   You can specify the licensing in the following ways:

   - Select **Use embedded 2-month evaluation key** to use the inbuilt license key. The evaluation license key supports all features and options and is valid for two months.

   or

   - Select **Enter license key**, specify the permanent license number in the field and then click **Add**.

     Select a key in the box to see the list of features and options that are available for use with the specified license key.

     To remove a specified key, select the key in the box and then click **Remove**.
6. On the vCenter Details panel, choose the way you want to specify virtual machines for the installation and then click **Next**.

   You can specify the virtual machines in the following ways:

- To add virtual machines names from the vCenter Server inventory, check the **Use virtual machine display names in the vCenter inventory** check box and provide the following vCenter Server details:

vCenter Server Name or IP	Specify the host name or IP address of the vCenter Server that is used to manage the virtual machines in your VMware environment.
Web Service Https Port	Specify the https port used by the VMware Web Service. The default port number is 443.
User Name	Specify the name of the user account that has the privileges to enumerate the virtual machines visible in the vSphere Client. The wizard uses this account to discover the virtual machines in the vCenter Server inventory.
Password	Specify the password for the user account specified in the User Name field.

  The wizard displays a prompt if the ApplicationHA plugin is not registered on the specified vCenter Server. Click **Yes** to proceed with the guest installation.
  The plugin registration is not required for guest components installation but is required for configuring application monitoring.

or

- To add systems using their host names or IP addresses, clear the **Use virtual machine display names in the vCenter inventory** check box.

7 On the System Selection panel, specify the systems for the installation and then click **Next**.
To add virtual machines from the vCenter Server inventory, do the following:

- To add a single system, in the VM Display Name field type the virtual machine name as it appears in the vCenter Server inventory and then click **Add**.
- To add multiple systems, click **Browse** to open the vCenter Server Browser. This dialog box displays the virtual machine names as they appear in the vCenter Server inventory.
  Expand Datacenters and then check the check boxes corresponding to the systems in the list and then click **OK**.

You cannot select systems that do not satisfy the installation prerequisites.

To add virtual machines using the hostnames or IP addresses, do the following:

- To add a single system, type the system name in the System Name or IP field and then click **Add**.
- To add multiple systems, click **Browse** to open the Select Systems dialog box.

  Select one or more systems from the Available Systems list and click the right arrow button to move them to the Selected Systems list and then click **OK**.

  The Available Systems list displays a list of systems in the domain where the current system resides.

The wizard uses `%Program Files%\Veritas` as the default installation directory. To change the directory, click the folder icon next to the system and then choose the installation directory.

The wizard performs the required validation checks on the selected systems. If a system passes the validation criteria, the status is reflected as *Ready for install*.

If a system does not meet the required criteria, the status is reflected as *Verification failed*. To view the cause of a validation failure, click the Information icon for the system.

Rectify the issue and then click **Re-verify** to perform the validation checks on the rejected system again.

The wizard does not proceed with the installation unless all the selected systems have passed the validation checks.

8. On the Pre-install Summary panel, review the pre-installation summary and then click **Next**.

   Click **Save Report** if you wish to save the pre-installation summary report for reference.

9. The Installation panel displays the progress of the installation on the selected systems.

   After the panel indicates that the installation is complete, click **Next**.

10. On the Post-install Summary panel, review the installation results and then click **Next**.

    If the installation has failed on any of the systems, review the post-install summary report and refer to the wizard log file for details.

    The log file is located at `%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>`.

    You may have to repeat the installation in case of failed installations.

11 On the Finish panel click **Finish**.

This completes the Symantec ApplicationHA guest components installation.

Installing ApplicationHA guest components using the command line interface

You can perform a silent installation of the ApplicationHA guest components using the Setup.exe command from the command prompt.

Perform the following steps to install the guest components on a virtual machine. Ensure that the Symantec ApplicationHA software package directory is accessible from the command prompt on the virtual machine.

Note: If User Access Control (UAC) is enabled on Windows Server 2008 or Windows Server 2008 R2 systems, you must launch the command prompt in the *Run as administrator* mode and then run the command mentioned in this procedure.

To install ApplicationHA guest components using the command line interface

1 From the virtual machine where you wish to install the guest components, click **Start > Run**, type `cmd`, and then click **OK** to open the command prompt.

For Windows Server 2008 or 2008 R2, launch the command prompt in the administrator mode. Right-click the command prompt shortcut from the Windows Start menu and click **Run as administrator** from the context menu.

2 In the command window, navigate to the Symantec ApplicationHA software package root directory.

3 Use the following command syntax to install:

```
Setup.exe /s solution=Solution
install_mode=Install_mode
installdir="Installdir" reboot=Reboot node="target"
licensekey="licensekey" options="options"
```

Here, the maximum length of the argument string is 2048 characters and the syntax is not case sensitive.

Table 2-4 describes the parameters applicable for Setup.exe command.

Table 2-5 ApplicationHA guest components command line install parameters

Parameter	Description
/s	Specifies the silent mode installation. If not set, this launches the product installation wizard.
solution	Specifies the type of installation. ■ **`1 = Symantec ApplicationHA`** Installs the Symantec ApplicationHA guest components for virtual machines. ■ **`2 = Symantec ApplicationHA Console`** Installs the Symantec ApplicationHA Console. This option is currently not supported by Symantec ApplicationHA. Use only the numerical value in the command. Example: solution=1
install_mode	Specifies install or uninstall operation. ■ **`1 = Install`** Installs the component specified by the solution parameter. ■ **`5 = Uninstall`** Removes the component specified by the solution parameter. Use only the numerical value in the command. Example: install_mode=1
installdir	Optional parameter. Specifies the installation directory. Enclose the path in double quotes. If you do not specify a path, the default installation directory is `%`*`ProgramFiles`*`%\Veritas`. Example: installdir=`"C:\Program Files\"`

Table 2-5 ApplicationHA guest components command line install parameters

Parameter	Description
reboot	Optional parameter. Specifies whether or not to reboot the system after the operation. ■ `0 = Do not reboot after the operation` ■ `1 = Reboot after the operation is complete` Default is 0 (Do not reboot after operation). Use only the numerical value in the command. Example: reboot=1 **Note:** A reboot is required if you are uninstalling Symantec ApplicationHA components using the command line. In case of uninstall, you must set this value to 1.
node	Optional parameter. Specifies the physical name of the system. Enclose the name in double quotes. Specify only one system at a time. If you do not specify a system name, the operation is performed on the local system by default. Example: node="SystemA"
licensekey	Optional parameter. Specifies the license key for the installation. ■ Enclose the license key in double quotes. ■ Enter multiple license keys separated by a comma. Do not put spaces around the comma. If you do not specify a license key, the embedded evaluation license key is installed by default. It is valid for two months. Example: "A2CU-PVEY-LKCJ-672C-G74O-ZNNO-PP6P-PPPP-PPP"
options	Optional parameter. This parameter is currently not applicable for Symantec ApplicationHA.

Example: ApplicationHA guest components command line installation

The following example installs ApplicationHA guest components on a virtual machine SystemA. The installation directory is `C:\Program Files`. The command also tells the system not to reboot after the installation is complete.

```
Setup.exe /s solution=1 install_mode=1 installdir="C:\Program Files"
reboot=0 node=SystemA
licensekey="A2CU-PVEY-LKCJ-672C-G74O-ZNNO-PP6P-PPPP-PPP"
```

Configuring single sign-on between the virtual machine and the ApplicationHA Console

After installing Symantec ApplicationHA (Console and guest components), you must configure single sign-on between the virtual machines and the ApplicationHA Console. This involves specifying the virtual machine administrator account to set up a permanent authentication for the virtual machine.

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

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

This 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.

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

To configure single sign-on for the virtual machines

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

   If you do not install the Symantec ApplicationHA Console certificate, this dialog pops up each time you log on to the vCenter Server using the vSphere Client.
3. Open the Hosts and Clusters view in the vSphere Client and then expand the Cluster to display the list of virtual machines.
4. From the left pane select a virtual machine where you installed ApplicationHA guest components and then in the right pane select the **ApplicationHA** tab.
5. Click **Yes** on the security certificate related dialog box, if displayed.

6 In the User Name and Password field, specify the credentials of a user that has administrative privileges on the virtual machine.

7 Click **Configure**.

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

After the authentication is successful, the ApplicationHA tab refreshes and displays the application configuration view.

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

Configuring VMware HA settings

Configuring VMware HA settings allows VMware HA to restart the virtual machine if the application heartbeat is not received within the specified time interval.

It involves the following tasks:

- Editing the VM monitoring settings in the Cluster Settings dialog box to enable VMware HA
- Setting the VM Monitoring option to **VM and Application Monitoring**
- Setting the monitoring sensitivity **Failure interval** for the VMware cluster to 30 seconds or more

  The monitoring sensitivity Failure interval field defines the time that VMware HA waits before attempting to restart the virtual machine. Symantec recommends that you set this value to the default 30 seconds or more.

These settings are available in the vSphere Client and are configurable on a per virtual machine basis in the VMware cluster. Refer to VMware documentation for more details.

To configure VMware HA settings

1 From the vSphere Client, display the cluster in the inventory.

2 Right-click the cluster and select **Edit Settings**.

3 In the left pane of the Cluster Settings dialog box, select **Cluster Features**.

4 In the right pane, check **Turn on VMware HA**.

5 In the left pane of the Cluster Settings dialog box, select **VM Monitoring**.

6 In VM Monitoring drop-down list, select **VM and Application Monitoring** to enable virtual machine monitoring and application monitoring.

7 Check the **Custom** check box in the Default Cluster Settings area.

8 In the **Failure interval** field, specify a value of 30 seconds or more.
If you have defined the failure interval on a per virtual machine basis, Symantec recommends that you apply this value for all the virtual machines where you wish to configure application monitoring.

9 Click **OK**.

Configuring Symantec ApplicationHA access control

After installing Symantec ApplicationHA you may want to configure access control for virtual machine users in your environment. Symantec ApplicationHA provides three levels of privileges, Admin, Operator, and Guest. Each of these privileges include a definite set of tasks that can be performed by a user. Using the available privileges you can segregate and distribute the application monitoring administration tasks. For example, a user with the Admin privilege can perform all the application monitoring tasks on a virtual machine. Similarly, a user with the Guest privilege can only view the application monitoring status on the virtual machine.

Use the vSphere Client to assign these privileges. You can either create additional roles or assign these privileges to existing roles directly.

To assign Symantec ApplicationHA user privileges

1 From the vSphere Client Home page click **Roles**.

2 In the Roles list, right-click the role to edit and click **Edit Role**.

3 In the Edit Role dialog box, expand **All Privileges**.
You should see the Symantec ApplicationHA privilege in the list.

4 Expand Symantec ApplicationHA and then check the check boxes of the privilege you want to enable for the role.

5 Click **OK**.

Refer to the VMware documentation for more details on roles, users, and groups.

Configuring application monitoring for ApplicationHA Console

Perform the following steps to configure application monitoring for ApplicationHA Console.

Note the following before you proceed:

- For configuring application monitoring, ApplicationHA Console must be installed on a virtual machine.
- This procedure is optional. The ApplicationHA Console functionality is not affected if you do not configure application monitoring for it.
- Symantec ApplicationHA considers the Console as a custom application. It can monitor ApplicationHA Console and its services running on the virtual machine. If any component fails, ApplicationHA attempts to start the component on the machine.
- During the time ApplicationHA attempts to restart the ApplicationHA Console components, the ApplicationHA tab may not display the current status of the applications being monitored on the virtual machines.
- After configuring application monitoring for ApplicationHA Console, the ApplicationHA tab in the vSphere Client displays the status of the application.

  You can perform all the operations from the ApplicationHA tab to control application monitoring for ApplicationHA Console. However, the Stop Application functionality is blocked. You cannot stop the application as that would result in Symantec ApplicationHA stopping the ApplicationHA Console. If the Console services are stopped, the ApplicationHA tab does not display the status of the applications configured on the virtual machines.
- To remove the application monitoring configuration, you can click **Unconfigure Application Monitoring** in the ApplicationHA tab. However, if you wish to configure monitoring again, you must perform the steps mentioned in this procedure.

  Do not use the Symantec ApplicationHA Configuration Wizard to configure application monitoring for ApplicationHA Console.

To configure application monitoring for ApplicationHA Console

1. Install the ApplicationHA guest components on the virtual machine where you installed ApplicationHA Console.

   See “About installing Symantec ApplicationHA guest components for virtual machines” on page 32.

2 After completing the guest components installation, launch the command prompt in the administrator mode. Right-click the command prompt shortcut from the Windows Start menu and click **Run as administrator** from the context menu.

3 Navigate to the following directory in the command window:

```
<installdirectory>\VRTSsfmh\bin
```

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

4 Run the Config_AppServer_HA perl script. Type the following command in the command window and then press **Enter**:

```
perl "<installdirectory>\cluster
server\portal\admin\Config_AppServer_HA.pl”
```

The perl script configures the required application monitoring resources. Different messages indicate the status of the operation.

This completes the application monitoring configuration for ApplicationHA Console. To verify the configuration, launch the vSphere Client, select the virtual machine where the Console is installed and then click the ApplicationHA tab. The status of the the application appears as configured and running on the virtual machine. The Description box displays the details of the configured components.

Chapter 3

Configuring application monitoring with Symantec ApplicationHA

This chapter includes the following topics:

- "About configuring application monitoring with Symantec ApplicationHA" on page 46
- "Before configuring application monitoring" on page 47
- "Configuring application monitoring for services, processes, and mount points" on page 48
- "Administering application monitoring from ApplicationHA view" on page 56
- "Administering application monitoring settings" on page 61
- "Administering plugin registration using the PluginMgmt.bat utility" on page 63
- "Considerations while administering virtual machines" on page 65
- "Backing up ApplicationHA Console files and registry" on page 66

About configuring application monitoring with Symantec ApplicationHA

This chapter describes the steps to configure application monitoring for services, processes, and mount points with Symantec ApplicationHA in a VMware virtualization environment.

For information on configuring applications such as Microsoft SQL Server 2008, Microsoft Exchange 2010 and Microsoft IIS, refer to the respective agent configuration guide.

Consider the following before you proceed:

- You configure application monitoring on a virtual machine using the Symantec ApplicationHA Configuration Wizard. The wizard is launched when you click **Configure Application Monitoring** on the ApplicationHA tab in VMware vSphere Client.
- Apart from the application monitoring configuration, the configuration wizard also sets up the other components required for Symantec ApplicationHA to successfully monitor the applications.

  You must first configure application monitoring using the configuration wizard before using VCS commands to add additional components or modify the existing configuration.
- You can use the wizard to configure monitoring for only one application per virtual machine.

  For example, if you have configured monitoring for SQL Server, you cannot run the wizard again to configure another application on that virtual machine.

  To configure another application using the wizard, you must first unconfigure the existing application monitoring configuration.
- You can configure multiple services, processes, and mount points in a single wizard workflow. After configuring a set of components, if you wish to add another component to the configuration, you cannot use the wizard.

  In this case, you can either use the VCS commands to add the components to the configuration, or unconfigure the existing configuration and then run the wizard again to select all the desired components for the monitoring.

  Note: When you configure or unconfigure application monitoring, it does not affect the state of the application. The application runs unaffected on the virtual machine. This also does not require any additional steps on the vCenter Server.

- If a configured service, process, or mount point fails, Symantec ApplicationHA attempts to start the component on the machine. If the component does not start, Symantec ApplicationHA communicates with VMware HA to take corrective action. Symantec ApplicationHA then stops the other configured components in a predefined order. This avoids the other components from getting corrupted due to a machine reboot.

  Thus, a single failed component can bring down other healthy components running on the virtual machine. You must take this behavior into consideration while configuring application monitoring on a virtual machine.

Before configuring application monitoring

Note the following prerequisites before configuring application monitoring for services, processes, and mount points on a virtual machine:

- Verify that you have installed Symantec ApplicationHA Console and guest components in your VMware environment.

  See “About installing Symantec ApplicationHA” on page 22.

- Verify that VMware Tools is installed on the virtual machine.

  Install the version that is the similar to or later than that available with VMware ESX 4.1.

- Verify that you have installed VMware vSphere Client. The vSphere Client is used to configure and control application monitoring.

  You can also perform the application monitoring operations directly from a browser window using the following URL:

  ```
  https://<virtualmachineNameorIPaddress>:5634/vcs/admin/
  application_health.html?priv=ADMIN
  ```

- Verify that the logged-on user has administrative privileges on the virtual machine where you wish to configure application monitoring.

- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.

  See “Ports and firewall settings” on page 26.

- If you wish to monitor storage managed using Storage Foundation for Windows (SFW), ensure that the volumes and mount points are created on dynamic disk groups.

  Symantec ApplicationHA does not support monitoring for volumes and mount points created on cluster disk groups.

Configuring application monitoring for services, processes, and mount points

Perform the following steps to configure monitoring for services, processes, and mount points on a virtual machine.

Note: You can configure monitoring for multiple services and processes in a single wizard workflow. However, you cannot configure multiple applications simultaneously.

To configure application monitoring for services, processes, and mount points

1. Launch the vSphere Client and connect to the vCenter Server that manages the virtual machine.
2. From the vSphere Client's Inventory view in the left pane, select the virtual machine where you want to configure application monitoring, and then in the right pane select the **ApplicationHA** tab.
3. Skip this step if you have already configured the single sign-on for the virtual machine.

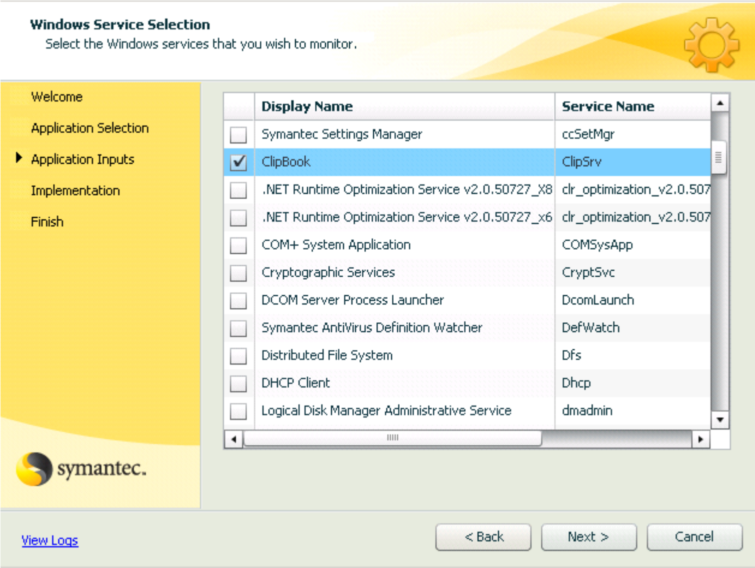
   In the User Name and Password field, specify the credentials of a user that has administrative privileges on the virtual machine and then click **Configure**.

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

   See "Configuring single sign-on between the virtual machine and the ApplicationHA Console" on page 40.

   After the authentication is successful, the ApplicationHA tab refreshes and displays the application health view.
4. Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard.
5. Review the information on the Welcome panel and then click **Next**.
6. On the Application Selection page, click **Custom Application** in the Supported Applications list and then click **Next**.
7. On the Windows Service Selection panel, select the services that you wish to monitor and then click **Next**.

The wizard automatically discovers the services on the virtual machine.



Windows Service Selection

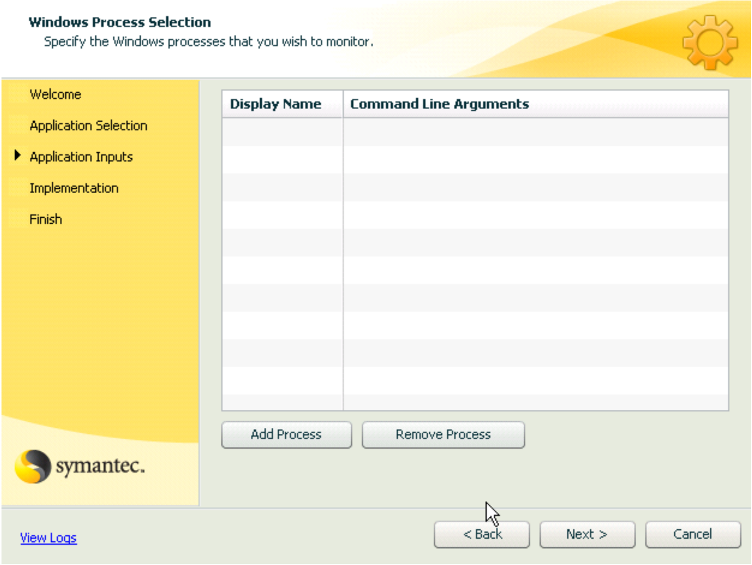
Select the Windows services that you wish to monitor.

	Display Name	Service Name
□	Symantec Settings Manager	ccSetMgr
☑	ClipBook	ClipSrv
□	.NET Runtime Optimization Service v2.0.50727_X8	clr_optimization_v2.0.507
□	.NET Runtime Optimization Service v2.0.50727_x6	clr_optimization_v2.0.507
□	COM+ System Application	COMSysApp
□	Cryptographic Services	CryptSvc
□	DCOM Server Process Launcher	DcomLaunch
□	Symantec AntiVirus Definition Watcher	DefWatch
□	Distributed File System	Dfs
□	DHCP Client	Dhcp
□	Logical Disk Manager Administrative Service	dmadmin

If a selected service depends on some other services, you must also select those services. You can define the dependencies between those services on the Start-Stop panel later.

If you do not want to configure any services, click **Next**.

8 On the Windows Process Selection panel, specify the processes that you wish to monitor and then click **Next**.



Windows Process Selection

Specify the Windows processes that you wish to monitor.

Display Name	Command Line Arguments

Perform the following steps to add a process:

- Click **Add Process** to display the Process Parameters dialog box.
- In the Process Full Path field type the complete path of the process executable file including its extension.

  If you define the process as a script (a perl script, or a vbs script), specify the full path of the program that interprets the script (perl.exe, or cscript.exe) in the Process Full Path field and specify the full path of the script itself in the Arguments field.

  For example, to specify Perl.exe, type the path as follows:

  `C:\Program Files\Perl\Perl.exe`.

  This presumes that Perl is installed at the mentioned path.
- In the Arguments field, type the command line arguments for the process, if any.
- The specified process runs in the context of the local system account by default. To run the process in a different user's context, check the **Run process using specified credentials** check box and then specify the user name and password in the respective fields.

  The user name must be in the format *user@domain.com* or *domain.com\username*.
- Click **OK**.

The process that you add is displayed on the wizard page.

Repeat these steps for all the processes that you wish to configure for monitoring.

If you do not want to configure any processes, click **Next**.

9 On the Mount Point Selection panel, select the mount points that you wish to monitor and then click **Next**.

If you do not want to monitor any mount points, click **Next**.

10 On the Define Start-Stop Order panel, specify the order in which you want the configured services, processes, and mount points to be started or stopped and then click **Configure**.

Perform the following steps to define the dependency between the components:

- Click on an application component name in the Parent Component box on the left.
- Then check the component check box in the Resources box on the right.

  While starting the service or process, the components are brought online in the defined order. For example, if a service is dependent on a mount point, then while starting the service the mount point is first brought online and then the service itself.

11 The wizard performs the application monitoring configuration tasks. The wizard creates the required resources and enables the application heartbeat that communicates with VMware HA.

The panel displays the status of each task. After all the tasks are complete, click **Next**.

If the configuration tasks fail, click **View Logs** to check the details of the failure. Rectify the cause of the failure and run the wizard again to configure the application monitoring.

12 On the Finish panel, click **Finish** to complete the wizard.

This completes the application monitoring configuration. You can view the application status in the ApplicationHA tab.

The view then displays the application as configured and running on the virtual machine. The Description box displays the details of the configured components.

If the application status shows as not running, click **Start Application** to start the configured service or process on the machine.

Configuring additional parameters for monitoring services

The configuration wizard uses the Symantec ApplicationHA GenericService agent resources to monitor services. When you configure application monitoring for a service, the wizard adds the service name to the agent's ServiceName attribute.

You can configure the other agent attributes to customize the monitoring configuration, if required. You can monitor a service in a user-context by configuring the GenericService agent attributes UserAccount, Password, and Domain from the command line.

Refer to the Appendix for details about the GenericService agent attributes.

Note: This procedure is optional. It is not essential for the functioning of application monitoring for the service.

To monitor a configured service in a user-context

1 From the ApplicationHA tab in the vSphere Client, click **Stop Application**.
This stops the configured service on the virtual machine. This is required for the attribute changes to take effect.

1 On the virtual machine where you have configured the service, type the following on the command prompt and then press **Enter**:

```
haconf -makerw
```

This command sets the configuration mode to read/write.

2 To set the UserAccount attribute, type the following on the command prompt and then press **Enter**:

```
hares -modify <resourcename> UserAccount
<user@domain.com or domain.com\username>
```

Here, <resourcename> is the name of the resource configured for the service. The resource name is of the format Service_<*servicename*>_res.
You can also retrieve the service resource name using the following command:

```
hares -state
```

The output of this command displays the resources configured on the virtual machine.

3 You must now encrypt the password for the user that you specified in the earlier step.
Perform the following steps to encrypt the password:

- Type the following on the command prompt and press **Enter**:

```
vcsencrypt -agent
```

- Type the password when prompted.
- Type the same password again when prompted.
- The output then displays some characters. These represent the password in an encrypted form.
- Copy the encrypted password. This is required in the next step.

The password is encrypted using the VCSEncrypt utility. Refer to the *Veritas Cluster Server Administrator's Guide* for more details.

4 To set the Password attribute, type the following on the command prompt and then press **Enter**:

```
hares -modify <resourcename> Password <password>
```

Here, <resourcename> is the name of the resource configured for the service and <password> is the encrypted password that you created in the earlier step.

5 To set the Domain attribute, type the following on the command prompt and then press **Enter**:

```
hares -modify <resourcename> Domain <domain>
```

Here, <resourcename> is the name of the resource configured for the service and <domain> is the domain to which the specified user belongs.

6 Use the `hares` command to modify other GenericService agent attributes, as desired.

7 Use the `hares -display` command to see the changes made to the resource attributes.

8 Save and close the configuration. Type the following on the command prompt and press **Enter**:

```
haconf -dump -makero
```

This command also sets the configuration mode to read only.

The specified attributes take effect and Symantec ApplicationHA monitors the service using the configured parameters.

The UserAccount attribute takes effect when you restart the service.

9 From the ApplicationHA tab in the vSphere Client, click **Start Application**.

The specified attributes take effect and Symantec ApplicationHA monitors the service using the configured parameters.

Configuring additional parameters for monitoring processes

The configuration wizard uses the Symantec ApplicationHA Process agent resources to monitor processes. When you configure application monitoring for a process, the wizard adds the process name to the agent's StartProgram attribute.

You can configure the other Process agent attributes to customize the monitoring configuration, if required. For example, you can use the attributes MonitorProgram, StopProgram, and CleanProgram to specify additional scripts for customizing the monitoring and stopping of the configured process.

Refer to the Appendix for details about the Process agent attributes.

Note: This procedure is optional. It is not essential for the functioning of application monitoring for the process.

Note the following before you proceed:

- When defining the StartProgram, StopProgram, or MonitorProgram attributes from the command line, enclose the path of the executable file in double quotes.

  For example, specify the StartProgram attribute in the following format:

  StartProgram = "executable_pathname" “arguments”

This procedure describes how to configure application monitoring for a set of perl scripts. The following components are used as a reference in the procedure:

- Start program: Perl.exe
- Perl scripts: start.pl, stop.pl, monitor.pl, and clean.pl

To configure additional parameters for monitoring a process

1 From the ApplicationHA tab in the vSphere Client, click **Stop Application**.

  This stops the configured process on the virtual machine. This is required for the attribute changes to take effect.

1 On the virtual machine where you have configured the service, type the following on the command prompt and then press **Enter**:

  ```
  haconf -makerw
  ```

  This command sets the configuration mode to read/write.

2 To get the Process agent resource name, type the following on the command prompt and then press **Enter**:

  ```
  hares -state
  ```

  The output of this command displays the resources configured on the virtual machine.

  The Process resource name is of the format Process_<*processname*>_res.

  Make a note of the process name. This is required in the subsequent steps.

3 To set the StartProgram attribute of the process resource, type the following on the command prompt and then press **Enter**:

  ```
  hares -modify <resourcename> StartProgram
  “\“<processpath>” \“<arguments>”
  ```

Here, <resourcename> is the name of the process resource. <processpath> is the complete path of the executable used to run the scripts. <arguments> is the script itself. Enclose <processpath> and <arguments> in doublequotes.

For example,

```
hares -modify Process_Perl_res StartProgram
“\“C:\\Program Files\\Perl\\perl.exe”
\”C:\\Processes\\scripts\\start.pl”
```

4 To set the StopProgram attribute of the process resource, type the following on the command prompt and then press **Enter**:

```
hares -modify <resourcename> StopProgram “\“<processpath>”
\“<arguments>”
```

For example,

```
hares -modify Process_Perl_res StopProgram
“\“C:\\Program Files\\Perl\\perl.exe”
\”C:\\Processes\\scripts\\stop.pl”
```

5 To set the MonitorProgram attribute of the process resource, type the following on the command prompt and then press **Enter**:

```
hares -modify <resourcename> MonitorProgram
“\“<processpath>” \“<arguments>”
```

For example,

```
hares -modify Process_Perl_res MonitorProgram
“\“C:\\Program Files\\Perl\\perl.exe”
\”C:\\Processes\\scripts\\monitor.pl”
```

6 Use the hares command to modify other Process agent attributes, as desired.

7 Save and close the configuration. Type the following on the command prompt and press **Enter**:

```
haconf -dump -makero
```

This command also sets the configuration mode to read only.

8 From the ApplicationHA tab in the vSphere Client, click **Start Application**.

The specified attributes take effect and Symantec ApplicationHA monitors the process using the configured parameters.

Administering application monitoring from ApplicationHA view

Symantec ApplicationHA provides an interface, the Symantec ApplicationHA tab, to configure and control application monitoring. The Symantec ApplicationHA tab is integrated with the VMware vSphere Client.

Use the Symantec ApplicationHA view to perform the following tasks:

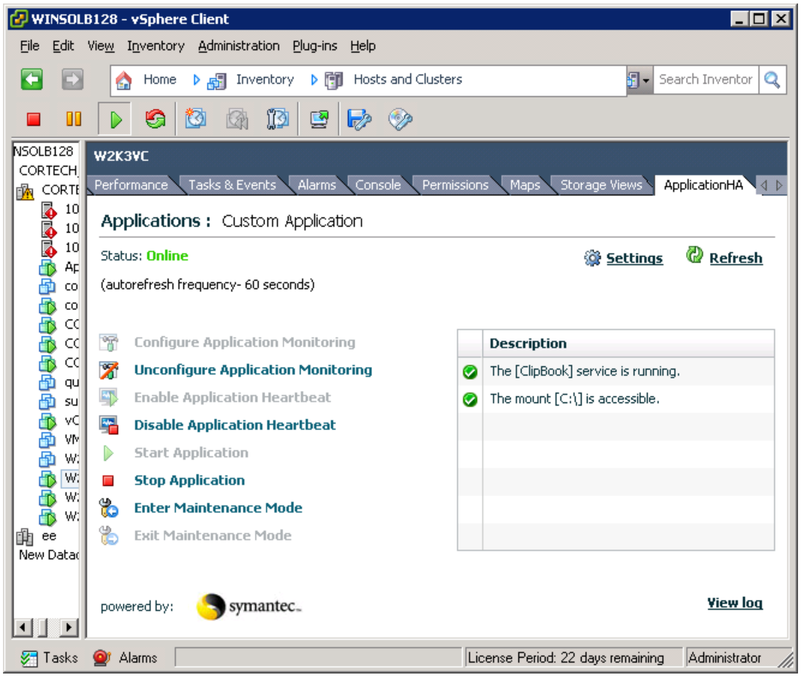
- configure and unconfigure application monitoring
- start and stop configured applications
- enable and disable application heartbeat
- enter and exit maintenance mode

To view the Symantec ApplicationHA view, launch the VMware vSphere Client, select a virtual machine from the Inventory pane, and in the Management pane on the right, click the **ApplicationHA** tab.

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

Note: You can also perform the application monitoring operations directly from a browser window using the following URL: https://<virtualmachineNameorIPaddress>:5634/vcs/admin/application_health.html?priv=ADMIN

After you configure an application on a virtual machine, the ApplicationHA view displays as follows:



Applications : Custom Application

Status: Online

(autorefresh frequency- 60 seconds)

	Description
✓	The [ClipBook] service is running.
✓	The mount [C:\] is accessible.

To configure or unconfigure application monitoring

Use the ApplicationHA view to configure or delete an application monitoring configuration from the virtual machine. This may be required in case you wish to re-create the configuration or configure another application using the wizard.

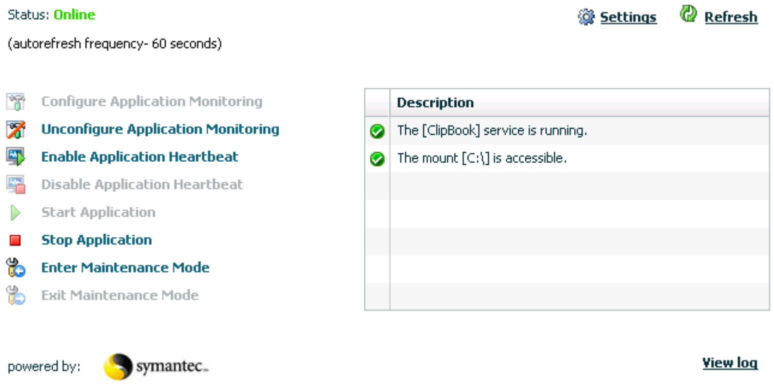
- Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard. Use the wizard to configure application monitoring.
- Click **Unconfigure Application Monitoring** to delete the application monitoring configuration from the virtual machine.

  Symantec ApplicationHA removes all the configured resources for the application and its services.

  Note that this does not uninstall Symantec ApplicationHA from the virtual machine. This only removes the configuration. The unconfigure option removes all the application monitoring configuration resources from the virtual machine. To monitor the applications, you have to configure them again.

To view the status of configured applications

The Description box in the ApplicationHA view displays the status of the configured services, processes, and mount points.



Status: Online

(autorefresh frequency- 60 seconds)

Description

✓ The [ClipBook] service is running.

✓ The mount [C:\] is accessible.

Settings
Refresh
Configure Application Monitoring
Unconfigure Application Monitoring
Enable Application Heartbeat
Disable Application Heartbeat
Start Application
Stop Application
Enter Maintenance Mode
Exit Maintenance Mode
powered by: symantec.
View log

For example, if you have configured monitoring for services and mount points, the Description box displays the following information:

```
The mount [mountpoint] is accessible.
The [servicename] service is running.
```

Here mountpoint and servicename are the names of the mount point and service configured on the virtual machine.

The Status field displays the state of the configured application and its components.

The following states are displayed:

- **online**
  Indicates that the services and processes are running on the virtual machine.
- **offline**
  Indicates that the services and processes are not running on the virtual machine.
- **partial**
  Indicates that either the services and processes are being started on the virtual machine or ApplicationHA was unable to start one or more of the configured services or processes.
- **faulted**
  Indicates that the configured services or components have unexpectedly stopped running

Click **Refresh** to see the most current status of the applications and its associated services. The status is refreshed every 60 seconds by default.

To start or stop applications

Use the ApplicationHA view to control the status of the configured application and the associated services.

The ApplicationHA view provides the following options:

- Click **Start Application** to start a configured application.
  Symantec ApplicationHA attempts to start the configured application and its components in the required order. The configured resources are also brought online in the appropriate heirarchy.
- Click **Stop Application** to stop a configured application that is running on the virtual machine.
  Symantec ApplicationHA begins to stop the configured application and its components gracefully. The configured resources are also taken offline in the pre-defined order.

To enable or disable application heartbeat

The VMware virtual machine monitoring feature uses the heartbeat information that VMware Tools captures as a proxy for guest operating system availability. This allows VMware HA to automatically restart individual virtual machines that have lost their ability to send the heartbeat. You must select VM and Application Monitoring if you want to enable application monitoring.

ApplicationHA view allows you to control the application heartbeat on the virtual machines.

Use the following options on the ApplicationHA tab to control the status of the configured application heartbeat:

- Click **Enable Application Hearbeat** to enable the heartbeat communication between the configured applications running on the virtual machine and VMware HA.
  The application heartbeat is enabled by default when an application is configured for monitoring.
- Click **Disable Application Hearbeat** to disable the heartbeat communication between the configured applications running on the virtual machine and VMware HA.
  When the application heartbeat is disabled, Symantec ApplicationHA does not send the application heartbeat to VMware HA. VMware HA will not reboot the machine if an application or its component faults.

However, Symantec ApplicationHA continues to monitor the configured application on the virtual machine. You can perform all the other application monitoring operations as usual.

This option disables the application monitoring feature in the VMware virtual machine monitoring settings.

To suspend or resume application monitoring

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

If stopping the application is not an option, you can suspend application monitoring and create a window for performing such maintenance tasks. When application monitoring is suspended, ApplicationHA freezes the application configuration, disables the application heartbeat, and stops sending the heartbeat to VMware HA.

The ApplicationHA view provides the following options:

- Click **Enter Maintenance Mode** to suspend the application monitoring for the applications that are configured on the virtual machine. During the time the monitoring is suspended, Symantec ApplicationHA does not monitor the state of the application and its dependent components. The ApplicationHA view does not display the current status of the application. If there is any failure in the application or its components, ApplicationHA takes no action.

- Click **Exit Maintenance Mode** to resume the application monitoring for the applications configured on the virtual machine. You may have to click the **Refresh** link in the ApplicationHA view to see the current status of the application.

  When application monitoring is restarted from a suspended state, ApplicationHA does not enable the application heartbeat. Click **Enable Application Heartbeat** to enable it.

  If you have made changes that include database addition or change in the underlying storage mount point that was being monitored, then those changes may not reflect in the application monitoring configuration. In such cases, you may have to unconfigure and reconfigure the application monitoring.

Administering application monitoring settings

The ApplicationHA view provides a set of options that you can use to control the way Symantec ApplicationHA handles application monitoring, application and dependent component faults, and application recovery on the virtual machine. These configuration settings are applicable on a per virtual machine basis. The settings apply to all the applications that Symantec ApplicationHA monitors on the virtual machine.

The following settings are available:

- AppStartStopTimeout

  When you click the **Start Application** or **Stop Application** links in the ApplicationHA view, Symantec ApplicationHA initiates an orderly start or stop of the application and its dependent components. This option defines the number of seconds Symantec ApplicationHA must wait for the application to start or stop. If the application does not respond in the stipulated time, an error is displayed in the ApplicationHA view.

  A delay in the application response does not indicate that the application or its dependent component has faulted. Parameters such as workload, system performance, and network bandwidth may affect the application response. Symantec ApplicationHA continues to wait for the application response even after the timeout interval is over. If the application fails to start or stop, ApplicationHA takes the necessary action depending on the other configuration settings.

  AppStartStopTimeout value can vary between 0 to 600. The default is 300 seconds.

- AppRestartAttempts

  This option defines the number of times Symantec ApplicationHA should try to restart a failed application or its dependent component. If an application fails to start in the specified number of attempts, Symantec ApplicationHA stops the application heartbeat and communicates the fault to VMware HA.

  AppRestartAttempts value can vary between 1 to 6. The default is 1.

- AppShutdownGraceTime

  This option defines the number of seconds Symantec ApplicationHA should wait before communicating the application fault to VMware HA.

  If a configured application or its dependent component fails, Symantec ApplicationHA tries to restart the component for the configured number of times. If the component fails to start, Symantec ApplicationHA stops the application heartbeat and communicates the fault to VMware HA. VMware HA may then restart the virtual machine depending on the configuration settings.

An abrupt shutdown may affect the other healthy application components running on the machine. If those components require more time to stop, Symantec ApplicationHA may not be able to stop them gracefully in time before the reboot is initiated. For such cases, you can use AppShutdownGraceTime to delay the virtual machine reboot so that Symantec ApplicationHA stops all the application components gracefully.

When an application fails to start, Symantec ApplicationHA initiates a graceful shutdown of all the healthy applications being monitored on the virtual machine and waits for time specified in this option. A virtual machine reboot takes place only after all the application components are shut down gracefully or at the end of the grace time, whichever is earlier.

This setting is applicable to the heartbeat service group that is created when you configure application monitoring using the Symantec ApplicationHA Configuration Wizard. Internally, it sets the *DelayBeforeAppFault* attribute of the Heartbeat agent resource (VMWAppMonHB) in the configuration.

AppShutDownGraceTime value can vary between 0 to 600. The default is 300 seconds.

To modify the application monitoring configuration settings

1. Launch the vSphere Client and from the inventory pane on the left, select the virtual machine where you have configured application monitoring.
2. Select the **ApplicationHA** tab and then click the **Settings** link to display the Settings dialog box.
3. Specify the values for the available options displayed in the Settings box and then click **OK**.

   The specified values are updated in the configuration and they take effect immediately.

Administering plugin registration using the PluginMgmt.bat utility

The PluginMgmt.bat utility helps you manage the Symantec ApplicationHA plugin registration in your VMware environment. The utility provides options to register, unregister, and verify the registration of the plugin on the vCenter Server.

Plugin registration is handled by the ApplicationHA installer during the ApplicationHA Console installation. Symantec recommends that you use this utility if the installer fails to register or unregister the plugin. You may need to unregister and register the plugin in cases where you wish to change the existing ApplicationHA Console host, or if there is a change in the vCenter Web Service port.

After you install the ApplicationHA Console the PluginMgmt.bat 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`.

To administer the plugin registration using PluginMgmt.bat

1. From the ApplicationHA Console host, launch the command prompt in the *Run as Administrator* mode and then navigate to the following directory in the command window:

   <*installdirectory*>`\ApplicationHA\bin`

2. Type the following command to run the pluginmgmt.bat in desired mode:

   ```
   PluginMgmt <register|unregister|verify>
   <ApplicationHAConsole_IP> <vCenterServer_IP>
   <vCenterServerSDK_Port> <vCenterServer_Username>
   <vCenterServer_Password>
   ```

   The following inputs are required:

register | unregister | verify	Specify register to register the plugin. Specify unregister to unregister the plugin. Specify verify to validate the plugin registration. The PluginMgmt.bat utility performs these operations on the vCenter Server specified for vCenterServer_IP value.

ApplicationHAConsole_IP

If you wish to register the plugin, specify the IP address of the system where you installed the ApplicationHA Console.

If you wish to unregister or verify the plugin, specify the IP address of the system that is currently running the ApplicationHA Console.

vCenterServer_IP

Specify the IP address of the vCenter Server used to manage the virtual machines.

vCenterServerSDK_Port

If you wish to register or verify the plugin, specify the port used by the VMware Web Service.

If you wish to unregister the plugin, then specify the port that was used while registering the plugin.

The default port is 443.

vCenterServer_Username

Specify a user account that has the vCenter Extension privileges on the vCenter Server specified for vCenterServer_IP value.

vCenterServer_Password

Specify the password of the user account specified for vCenterServer_Username value.

The output of the command confirms the status of the requested operation.

Considerations while administering virtual machines

In a VMware environment you may perform various virtual machines administration tasks that include suspending or stopping virtual machines, taking snapshots, reverting to snapshots, migrating virtual machines to alternate hosts, and creating virtual machine templates. VMware provides a host of features to perform these administrative tasks on the virtual machines. Symantec ApplicationHA supports these features.

ApplicationHA support includes but is not limited to the following features:

- VMware vMotion
- VMware Distributed Resource Scheduler (VMware DRS)
- VMware Storage vMotion
- VMware Snapshots
- VMware High Availability (VMware HA)

You can perform the administrative tasks on virtual machines where you have configured application monitoring. Symantec ApplicationHA supports these administrative operations while it is actively monitoring applications on the virtual machines. These operations do not affect the ApplicationHA functionality.

Symantec recommends that while working with virtual machine snapshots or migrating virtual machines to alternate hosts, you either disable the application heartbeat (Disable Application Heartbeat button on the ApplicationHA tab) or suspend application monitoring (Enter Maintenance Mode button on the ApplicationHA tab) on the virtual machine.

You can create templates of virtual machines that have Symantec ApplicationHA installed. You make a template after installing Symantec ApplicationHA and configuring a secure trust relationship between the virtual machine and the Console.

You must not make a template of a virtual machine where application monitoring is configured. Symantec ApplicationHA may fail to discover the application monitoring configuration on the virtual machine created from such templates. You have to unconfigure the application monitoring first and then configure it again on the virtual machine.

Symantec recommends that you create virtual machine templates after installing Symantec ApplicationHA and setting up the trusted communication between the virtual machine and the Console.

Refer to the VMware documentation for prerequisites and recommendations for performing these virtual machine administration tasks.

Backing up ApplicationHA Console files and registry

After configuring application monitoring on the virtual machines, you can take a backup of ApplicationHA Console files and registry keys. The backed up files can be used to restore the configuration data in cases where the Console files become corrupt.

Perform the following steps on the ApplicationHA Console host:

1. Back up the following directory from the ApplicationHA Console host:

   <*installdirectory*>`\Veritas Shared`

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

2. Click **Start > Run**, type **regedit** and then click **OK** to open the Windows Registry Editor and then navigate to the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veritas\VPI`

3. Take a back up of the VPI key.

   Right-click **VPI**, then click **Export** and then specify the file name and a location for saving the VPI registry branch.

4. Back up the following directories on the ApplicationHA Console host:

   `%AllUsersProfile%\Symantec\ApplicationHA\sec`

   `%AllUsersProfile%\Symantec\ApplicationHA\conf`

   Here %AllUsersProfile% typically expands to C:\ProgramData.

Store the backup files at a location from where you can retreive them, if required. See the troubleshooting section for information on how to restore these files in case of a file corruption on the Console host.

Chapter 4

Uninstalling Symantec ApplicationHA

This chapter includes the following topics:

- "Uninstalling Symantec ApplicationHA guest components from the virtual machines" on page 68
- "Uninstalling Symantec ApplicationHA Console" on page 70

Uninstalling Symantec ApplicationHA guest components from the virtual machines

Use the Symantec ApplicationHA installer to uninstall the Symantec ApplicationHA components from the virtual machines in your VMware virtualization environment.

Consider the following points before you proceed:

- If application monitoring is configured on the virtual machines, you must first remove the configuration. This is required for a clean uninstall of Symantec ApplicationHA components.

  Also, if you uninstall without removing the application monitoring configuration, the virtual machine may go in to a reboot mode.
- The installer uses the logged-on user account context for uninstallation. Verify that the logged-on user has local Administrator privileges on the system where you want to uninstall.
- The installer currently supports uninstallation on up to 32 virtual machines at a time. If you wish to uninstall on additional systems, you must first complete the operation on 32 systems, and then run the installer again and select the additional systems for the uninstallation.

  The installer generates a summary that contains the list of systems where the operation was performed. You can save that report as a reference.
- A reboot is required post uninstallation. The installer can automatically reboot the systems after the uninstallation is complete. If you wish to reboot the systems later, uncheck the automatic reboot option on the wizard's Pre-uninstall Summary panel.
- The installer allows remote uninstallation. You can launch the installer from any virtual machine in your network that has Symantec ApplicationHA installed.

  In case of remote uninstallations, ensure that the logged-on user has local Administrator privileges on all the remote systems.
- For uninstallation on Windows Server 2008 systems, ensure that the Application Information service is running on all the systems.

  To start the service type the following on the command prompt:

  ```
  net start appinfo
  ```

Perform the following steps to remove the Symantec ApplicationHA components from the virtual machines.

To remove the Symantec ApplicationHA components from the virtual machines

1. On a virtual machine launch Windows Add or Remove Programs from the Windows start menu.

   Click **Start > Settings > Control Panel** and then double-click **Add or Remove Programs**.

   In case of Windows Server 2008, click **Start > Settings > Control Panel** and then double-click **Programs and Features**.

2. In the Add or Remove Programs window, select **Symantec ApplicationHA** and then click **Remove**. In case of Windows Server 2008, click **Uninstall**.

   This launches the Symantec ApplicationHA installer.

3. Review the prerequisites on the Welcome panel and then click **Next**.

4. On the System Selection panel, add the systems where you want to uninstall the Symantec ApplicationHA components and then click **Next**.

   Note that the wizard automatically adds the local system name to the list.

   You can add systems in the following ways:

   - To add a single system at a time, type the system name in the System Name field and then click **Add**.
   - To add multiple systems at a time, click **Browse** to open the Select Systems dialog box.

     The wizard discovers the systems in the domain where the current system resides and displays them in the Available Systems list.

     Select one or more systems from the Available Systems list and click the right arrow button to move them to the Selected Systems list and then click **OK**.

   The wizard performs validation checks on the selected systems. If a system passes the validation criteria, the status is reflected as *Ready for uninstall*.

   If a system does not meet the required criteria, the status is reflected as *Failed verification*. To view the cause of a validation failure, click the Information icon for the system.

   Rectify the issue and then click **Re-verify** to perform the validation checks on the rejected system again.

   The wizard does not proceed with the uninstallation unless all the selected systems have passed the validation checks.

5. On the Pre-uninstall Summary panel, review the pre-uninstallation summary and then click **Next**.

   Click **Save Report** if you wish to save the summary report for reference.

   If you do not want the installer to reboot the systems after the uninstallation, clear the **Automatically reboot systems after installer completes the operation** check box.

You must manually reboot all the systems later.

6 The Un-installation panel displays the progress of the uninstallation on the selected systems. After the panel indicates that the tasks are complete, click **Next**.

7 On the Post-uninstall Summary panel, review the results and then click **Next**.

Click **Save Report** if you wish to save the summary report for reference.

If the uninstallation has failed on any of the systems, review the post-uninstall summary report and refer to the wizard log file for details.

The log file is located at `%AllUsersProfile%\ApplicationData\Veritas\VPI\log\<date_timestamp>`.

On Windows Server 2008 and 2008 R2, the path is `%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>`.

You may have to repeat the uninstallation in case of failed uninstallations.

8 On the Finish panel click **Finish**.

9 Click **Yes** on the dialog box that prompts for the systems reboot. The installer automatically reboots the systems.

Click **No** if you wish to reboot the systems later.

The uninstallation requires a reboot of the systems. If you did not select the automatic reboot option, you must manually reboot the systems.

This completes the Symantec ApplicationHA virtual machine component uninstallation.

Uninstalling Symantec ApplicationHA Console

Use the Symantec ApplicationHA installer to uninstall the Symantec ApplicationHA Console from your VMware virtualization environment.

Consider the following points before you proceed:

- As part of the server uninstallation, the installer also unregisters the Symantec ApplicationHA plugin for vCenter Server.
- If the purpose of the uninstall is to replace the existing server with another ApplicationHA Console, then the application monitoring may not be visible in the vSphere Client until the new server is installed and configured.

  The ApplicationHA view in the vSphere Client may not display the most current status of the applications configured on the virtual machines.
- A reboot is required post uninstallation. The installer can automatically reboot the system after the uninstallation is complete. If you wish to reboot

the system later, uncheck the automatic reboot option on the wizard's Pre-uninstall Summary panel.

- The uninstallation must run locally. Remote uninstall is not supported.
- The installer uses the logged-on user account context to perform the uninstallation. Verify that the logged-on user has local administrator privileges on the system where you want to uninstall.

Perform the following steps to uninstall the Symantec ApplicationHA Console.

To uninstall the Symantec ApplicationHA Console

1. On the ApplicationHA Console host open Windows Add or Remove Programs.

   Click **Start > Settings > Control Panel** and then double-click **Add or Remove Programs**.

   In case of Windows Server 2008, click **Start > Settings > Control Panel** and then double-click **Programs and Features**.

2. In the Add or Remove Programs window, select **Symantec ApplicationHA Console** and then click **Remove**. In case of Windows Server 2008, click **Uninstall**.

   This launches the Symantec ApplicationHA installer.

3. Review the prerequisites on the Welcome panel and then click **Next**.

4. On the VMware vCenter Server Details panel, specify the vCenter Server details and then click **Next**.

   Provide the following details:

ApplicationHA Console IP	Select the IP address of the local system from the drop-down list. This is the IP of the machine where ApplicationHA Console is installed. The drop-down list may display several IPs if the system has multiple network adapters each with a unique IP address assigned. Select the host IP address that is accessible from the vCenter Server.
vCenter Server Name or IP	Specify the host name or IP address of the VMware vCenter Server. Ensure that the specified vCenter Server host name or IP address is accessible from the ApplicationHA Console host.

Web Service Https Port	Specify the https port used by the VMware Web Service. The default port number is 443.
User Name	Specify the name of the user account that has the privileges to extend the vSphere Client. The installer uses this account to unregister the ApplicationHA plugin on the vCenter Server.
Password	Specify the password for the user account specified in the User Name field.

5 On the System Selection panel, the installer automatically selects the local host for uninstallation and begins verification. After the status shows as *Ready for uninstall*, click **Next**.

The wizard performs validation checks on the specified system. If the system does not meet the required criteria, the status is reflected as *Verification failed*. To view the cause of a validation failure, click the Information icon for the system. Rectify the issue and then click **Re-verify** to perform the validation checks on the rejected system again.

The wizard does not proceed unless the selected system has passed the validation checks.

6 On the Pre-uninstall Summary panel, review the summary and then click **Next**.

Click **Save Report** if you wish to save the pre-uninstallation summary report for reference.

If you do not want the installer to reboot the systems after the uninstallation, clear the **Automatically reboot systems after installer completes the operation** check box.

You must manually reboot the system later.

7 Click **OK** on the dialog box that confirms about the system reboot. To change the reboot option click **Cancel**.

The Pre-uninstall Tasks pane displays the status of the pre-install tasks. The installer stops the required services and unregisters the Symantec ApplicationHA plugin on the vCenter Server.

If the pre-uninstall tasks fail on the system, rectify the issue and then click **Retry** to run the tasks on the system again.

8 The Symantec ApplicationHA Console Un-installation panel displays the progress of the uninstallation.

After the panel indicates that the uninstallation is complete, click **Next**.

9 On the Post-uninstall Summary panel, review the results and then click **Next**.

If the uninstallation has failed on the system, review the post-uninstall summary report and refer to the wizard log file for details.

The log file is located at `%AllUsersProfile%\ApplicationData\Veritas\VPI\log\<date_timestamp>`.

On Windows Server 2008 or 2008 R2, the path is `%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>`.

You may have to repeat the uninstallation if the wizard indicates that the installation itself has failed.

If the logs indicate that the Symantec ApplicationHA plugin uninstallation has failed, you may have to manually unregister the plugin on the vCenter Server. Use the PluginMgmt.bat utility to register the plugin. Refer to the configuration section for details about the PluginMgmt.bat utility.

10 On the Finish panel click **Finish**.

11 Click **Yes** on the dialog box that prompts for a system reboot. The installer automatically reboots the system.

Click **No** if you wish to reboot the system later.

The uninstallation requires a reboot of the system. If you did not select the automatic reboot option, you must manually reboot the system.

This completes the Symantec ApplicationHA Console uninstallation.

Symantec ApplicationHA agents

This appendix includes the following topics:

- "About the Symantec ApplicationHA infrastructure agents" on page 76
- "About the Heartbeat agent" on page 77
- "About the MountMonitor agent" on page 79
- "About the GenericService agent" on page 81
- "About the Process agent" on page 84
- "About the FileNone agent" on page 89
- "About the ElifNone agent" on page 90
- "About the FileOnOff agent" on page 91
- "About the FileOnOnly agent" on page 92

About the Symantec ApplicationHA infrastructure agents

Agents are processes that manage applications and resources of predefined resource types on a system. The agents are installed when you install Symantec ApplicationHA. A system has one agent per resource type that monitors all resources of that type. For example, a single GenericService agent manages all services that are configured using the GenericService resources. When the agent starts, it obtains the necessary configuration information from the resources and then monitors the configured applications. The agents then periodically update Symantec ApplicationHA with the resource and application status.

Agents perform the following operations:

- Bring resources online
- Take resources offline
- Monitor resources and report state changes

Symantec ApplicationHA agents are classified as Infrastructure agents and Application agents.

Infrastructure agents are packaged (bundled) with the base software and include agents for mount points, generic services and processes. These agents are immediately available for use after you install Symantec ApplicationHA.

Application agents are used to monitor third party applications such as Microsoft SQL Server, Oracle, and Microsoft Exchange. These agents are packaged separately and are available in the form of an agent pack that can be installed after you have installed Symantec ApplicationHA.

An agent pack is released on a quaterly 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 Veritas Operations Services (VOS) Web site for information on the latest agent pack availability.

http://vos.symantec.com

The following sections provide details about the infrastructure agents. For more details about an application agent, refer to the application-specific configuration guide.

About the Heartbeat agent

The Heartbeat agent monitors the configured application service group. When you configure application monitoring using the Symantec ApplicationHA Configuration Wizard, the wizard also creates a separate service group containing a resource for this agent. This resource verifies the status of the configured application service group. A single resource is used for monitoring all the application service group created on the virtual machine.

The heartbeat agent is represented by the VMAppMonHB resource type.

Hearbeat agent function

Monitor	Verifies that the specified service group is online.

Hearbeat agent state definitions

ONLINE	Indicates that the configured resource is online.
OFFLINE	Indicates that the service group specified in the resource has faulted.
UNKNOWN	Indicatest that the agent encountered errors while monitoring the VMAppMonHB resource.

Hearbeat agent resource type definition

```
type VMWAppMonHB (
    static str ArgList[] = { ServiceGroupName, DelayBeforeAppFault}
    static int MonitorInterval = 10
    static int OfflineMonitorInterval = 10
    static int NumThreads = 1
    static str Operations = None
    str ServiceGroupName[]
    int DelayBeforeAppFault = 300
    )
```

Hearbeat agent attribute

Table A-1 Heartbeat agent attributes

Required attribute	Description
ServiceGroupName	The name of the service group that is being monitored. This attribute contains the name of the service group created when you run the Symantec ApplicationHA Configuration Wizard. If you configure additional application service groups using the command line, this attribute contains the names of all those service groups.
DelayBeforeAppFault	The number of seconds the agent must wait for the healthy application service groups on the machine to go offline, before communicating application fault to VMware HA. This attribute can take a value between 0 to 600 seconds. Default is 300 seconds.

About the MountMonitor agent

The MountMonitor agent monitors the mount path of the configured storage. It is independent of how the underlying storage is managed (whether SFW disk groups or LDM disks or any other storage management software). The mount path can be a drive letter or a folder mount.

When configuring a directory to host the mount, verify the following conditions:

- The configured path exists.
- The directory is empty.
- The volume on which the directory resides is NTFS-formatted.

This agent is represented by the MountMonitor resource type.

MountMonitor agent function

Online	Mounts the configured mount path (drive letter or folder) on the system.
Monitor	Verifies that the specified mouth path (drive letter or folder) is mounted.

MountMonitor agent state definitions

ONLINE	Indicates the system can access the configured mount path.
OFFLINE	Indicates the system cannot access the configured mount path.
UNKNOWN	Indicates the agent could not determine the status of the resource.

MountMonitor agent resource type definition

```
type MountMonitor (
    static i18nstr ArgList[] = { MountPath, VolumeName }
    static str Operations = OnOnly
    str MountPath
    str VolumeName
    )
```

MountMonitor agent attributes

Table A-2 MountMonitor agent required attributes

Required attributes	Description
MountPath	The drive letter or path to an empty NTFS folder where a partition is mounted. The attribute can be specified as X, X:, X:\, X:\Directory, X:\Directory\. When configuring a directory to host the mount, verify the following conditions: ■ The configured path exists. ■ The directory is empty. ■ The volume on which the directory resides is NTFS-formatted. Type and dimension: string-scalar
VolumeName	The GUID of the volume to be mounted.

About the GenericService agent

The GenericService agent brings services online, takes them offline, and monitors their status. A service is an application type that is supported by Windows, and conforms to the interface rules of the Service Control Manager (SCM).

Services are configured as resources of type GenericService. You can configure the GenericService agent to monitor multiple services by defining a resource for each service to be monitored. You can monitor a service in a user-context by specifying the user name, password, and domain.

Note: The service to be configured using the GenericService agent must not be in a disabled state.

This agent is represented by the GenericService resource type.

GenericService agent functions

Online	Starts the configured service.
Offline	Stops the configured service.
Monitor	Retrieves the current state of the configured service. It also verifies the user context, if applicable.

GenericService agent state definitions

ONLINE	Indicates that the service being monitored is running.
OFFLINE	Indicates that the service being monitored is stopped.
UNKNOWN	Indicates the service operation is in a pending state, or that the agent could not determine the state of the resource.

GenericService agent resource type definition

```
type GenericService (
    static i18nstr ArgList[] = { ServiceName, DelayAfterOnline,
    DelayAfterOffline, UserAccount, Password, Domain, service_arg }
    i18nstr ServiceName
    int DelayAfterOnline = 10
int DelayAfterOffline = 10
i18nstr UserAccount
str Password
i18nstr Domain
str service_arg[]
)
```

GenericService agent attributes

Table A-3 GenericService agent required attributes

Required attribute	Description
ServiceName	Name of the service to be monitored. The service name can be the Service Display Name or the Service Key Name. Type and dimension: string-scalar

Table A-4 GenericService agent optional attributes

Optional attributes	Description
DelayAfterOffline	Number of seconds the offline routine waits for the service to go offline. Default is 10 seconds. Type and dimension: integer-scalar
DelayAfterOnline	Number of seconds the online routine waits for the service to go online. Default is 10 seconds. Type and dimension: integer-scalar
Domain	The domain name to which the user specified in the UserAccount attribute belongs. If the UserAccount attribute is empty or contains a built-in service account, this attribute is ignored. Type and dimension: string-scalar

Table A-4 GenericService agent optional attributes

Optional attributes	Description
Password	The password of the user, in whose context, the service would be started. Encrypt the password using the VCSEncrypt utility. If the UserAccount attribute is empty or contains a built-in service account, this attribute is ignored. Type and dimension: string-scalar
service_arg	An array of arguments passed to the service. Type and dimension: string-vector
UserAccount	A valid user account in whose context the service will be monitored. The user name can be of the form *username@domain.com* or *domain.com\username*. If the startup type of the configured service is set to Automatic, then the user account you specify here must be the same as that specified in the Windows Service Control Manager (SCM). If you do not specify a value for this attribute, then the user account of the service in the SCM is ignored. To monitor service under built-in accounts, you must provide explicit values. For example: On Windows 2003: UserAccount='LocalSystem', 'Local Service', or 'Network Service'. Domain='NT Authority'. The 'NT Authority' domain is not applicable for the 'LocalSystem' account. Type and dimension: string-scalar

About the Process agent

The Process agent brings processes online, takes them offline, and monitors their status. You can specify different executables for each process routine. The processes are monitored in the context of the LocalSystem account by default. You can run a process with user privileges by specifying the user name, password, and domain.

This agent is represented by the Process resource type.

Process agent functions

Online	Starts the process configured as the start program.
Offline	Terminates the process, or starts the process configured as the stop program.
Monitor	Verifies the status of the process, or starts the process configured as the monitor program.

Process agent state definitions

ONLINE	Indicates the process being monitored is running properly.
OFFLINE	Indicates the process being monitored is not running properly.
UNKNOWN	Indicates the agent could not determine the status of the resource.

Process agent resource type definition

```
type Process (
    static i18nstr ArgList[] = { StartProgram, StopProgram,
    MonitorProgram, UserName, Password, Domain,
    MonitorProgramTimeout,InteractWithDesktop, CleanProgram,
    StartupDirectory, StopProgramTimeout, CleanProgramTimeout }
    i18nstr StartProgram
    i18nstr StartupDirectory
    i18nstr StopProgram
    i18nstr CleanProgram
    i18nstr MonitorProgram
    i18nstr UserName
    str Password
    i18nstr Domain
    int MonitorProgramTimeout = 30
    boolean InteractWithDesktop = 0
    int StopProgramTimeout = 30
    int CleanProgramTimeout = 30
)
```

Process agent attributes

Table A-5 Process agent required attributes

Required Attribute	Description
StartProgram	The process to be monitored by the agent. You must specify the complete path of the executable, its file extension, and command-line arguments, if any. If you define the start program as a batch file or a script to launch another program, you must specify the monitor program in the configuration file. If you define the start program as a script (a batch file, a perl script, or a vbs script), the start program should be the program that interprets the script (cmd.exe, or perl.exe, or cscript.exe) and the script itself should be passed as an argument. Type and dimension: string-scalar

Table A-6

Optional Attributes	Description
CleanProgram	The full path of the clean process that is launched when the resource needs a forceful offline. If no value is specified for this attribute, for a clean operation the agent kills the process indicated by the StartProgram attribute. Type and dimension: string-scalar
CleanProgramTimeout	The maximum time, in seconds, that the agent must wait before killing the process specified in the CleanProgram attribute. This attribute is ignored if the clean program is not specified. The default value is 30 seconds. Type and dimension: integer-scalar

Table A-6

Optional Attributes	Description
Domain	The domain in which the user specified by the attribute UserName exists. This attribute is ignored if the user name is not specified. Type and dimension: string-scalar
InteractWithDesktop	Defines whether the configured process interacts with the desktop. Enabling desktop interaction enables user intervention for the process. The value 1 indicates the process will interact with the desktop. The value 0 indicates it will not. Default is 0. Type and dimension: boolean-scalar
MonitorProgram	A program that monitors the process specified as the start program. You must specify the complete path of the executable, its file extension, and command-line arguments, if any. If you do not specify a value for this attribute, Symantec ApplicationHA monitors the start program. However, if the start program is a batch file or a script to launch another program, you must specify a monitor program. Type and dimension: string-scalar **Note:** The monitor program is spawned every monitor cycle and must return before the program specified in MonitorProgram times out. The return values for the monitor program must conform to Symantec ApplicationHA conventions: 110 for ONLINE and 100 for OFFLINE. For exit values outside the range 100-110, the status is considered UNKNOWN. Refer to the *VCS Agent Developers Guide* for more information.
MonitorProgramTimeout	The maximum wait time, in seconds, for the agent to receive a return value from the monitor routine. This attribute is ignored if the monitor program is not specified. Default is 30 seconds. Type and dimension: integer-scalar

Table A-6

Optional Attributes	Description
Password	The encrypted password of the user specified by the UserName. Note that the password must be encrypted using the VCSEncrypt utility. This attribute is ignored if the user name is not specified. Type and dimension: string-scalar Refer to the *VCS Administrator's Guide* for more information about the VCSEncrypt utility.
StartupDirectory	The startup directory for the process indicated by the StartProgram attribute. Type and dimension: string-scalar
StopProgram	A program that stops the process specified as the start program. You must specify the complete path of the program, its file extension, and command-line arguments, if any. If you do not specify a value for this attribute, Symantec ApplicationHA stops the start program. Type and dimension: string-scalar **Note:** If successful, the StopProgram returns a positive value. The Monitor routine is called after those many seconds, as returned by StopProgram. Also, while writing a stop program, make sure to stop all the processes launched by the start program.
StopProgramTimeout	The maximum time, in seconds, that the agent must wait before killing the process specified in the StopProgram attribute. The default value is 30 seconds. Type and dimension: integer-scalar
UserName	The user name with whose privileges the configured process executes. User name can be of the form *username@domain.com* or *domain.com\username*. If a user name is not specified, the configured process runs in the context of the local system account. Type and dimension: string-scalar

Note: When defining the StartProgram, StopProgram, or MonitorProgram attributes, enclose the path of the executable file and its arguments in double quotes.

About the FileNone agent

The FileNone agent monitors a file. The monitor routine returns ONLINE if the specified file exists.

This agent is represented by the FileNone resource type.

FileNone agent function

Monitor	Verifies that the specified file exists.

FileNone agent state definitions

ONLINE	Indicates the specified file exists.
OFFLINE	Indicates the specified file does not exist.
UNKNOWN	Indicates that the value of the PathName attribute does not contain a valid file name.

FileNone agent resource type definition

```
type FileNone (
    static i18nstr ArgList[] = { PathName }
    static int OfflineMonitorInterval = 60
    static str Operations = None
    i18nstr PathName
    )
```

FileNone agent attribute

Table A-7 FileNone agent required attribute

Required Attributes	Description
PathName	The complete path of the file to be monitored. Type and dimension: string-scalar

About the ElifNone agent

The ElifNone agent monitors a file. The monitor routine returns ONLINE if the specified file does not exist.

This agent is represented by the ElifNone resource type.

ElifNone agent function

Monitor	Verifies that the specified file exists.

ElifNone agent state definitions

ONLINE	Indicates the specified file does not exist.
OFFLINE	Indicates the specified file exists.
UNKNOWN	Indicates that the value of the PathName attribute does not contain a valid file name.

ElifNone agent resource type definition

```
type ElifNone (
    static i18nstr ArgList[] = { PathName }
    static int OfflineMonitorInterval = 60
    static str Operations = None
    i18nstr PathName
    )
```

ElifNone agent attribute

Table A-8 ElifNone agent required attribute

Required Attributes	Description
PathName	The complete path of the file to be monitored. Type and dimension: string-scalar

About the FileOnOff agent

The FileOnOff agent creates, removes, and monitors files.

This agent is represented by the FileOnOff resource type.

FileOnOff agent functions

Online	Creates an empty file with the specified name, if the file does not already exist.
Offline	Removes the specified file.
Monitor	Verifies that the specified file exists.

FileOnOff state definitions

ONLINE	Indicates the specified file exists.
OFFLINE	Indicates the specified file does not exist.
UNKNOWN	Indicates that the value of the PathName attribute does not contain a valid file name.

FileOnOff agent resource type definition

```
type FileOnOff (
    static i18nstr ArgList[] = { PathName }
    i18nstr PathName
    )
```

FileOnOff agent attribute

Table A-9 FileOnOff agent required attribute

Required Attributes	Description
PathName	The complete path of the file to be monitored. Type and dimension: string-scalar

About the FileOnOnly agent

The FileOnOnly agent creates and monitors a file.

This agent is represented by the FileOnOnly resource type.

FileOnOnly agent functions

Online	Creates the specified file.
Monitor	Verifies that the specified file exists.

FileOnOnly state definitions

ONLINE	Indicates the specified file exists.
OFFLINE	Indicates the specified file does not exist.
UNKNOWN	Indicates that the value of the PathName attribute does not contain a valid file name.

FileOnOnly agent resource type definition

```
type FileOnOnly (
    static i18nstr ArgList[] = { PathName }
    static str Operations = OnOnly
    i18nstr PathName
    )
```

FileOnOnly agent attribute

Table A-10 FileOnOnly agent required attribute

Required Attributes	Description
PathName	The complete path of the file to be monitored. Type and dimension: string-scalar

Appendix B

Troubleshooting Symantec ApplicationHA installation and configuration

This appendix includes the following topics:

- "Symantec ApplicationHA logging" on page 94
- "Symantec ApplicationHA plugin registration error" on page 97
- "Symantec ApplicationHA tab does not display the application monitoring status" on page 98
- "Symantec ApplicationHA tab displays the "Unable to retrieve the status of this virtual machine." error" on page 98
- "Symantec ApplicationHA tab displays a "Failed to retrieve status." popup message" on page 99
- "Symantec ApplicationHA Configuration Wizard displays blank" on page 100
- "ApplicationHA Console files become corrupt" on page 100
- "ApplicationHA Console host becomes permanently unavailable" on page 102
- "VMware vCenter Server becomes permanently unavailable" on page 103

Symantec ApplicationHA logging

This chapter describes how to troubleshoot common problems that may occur while installing and configuring 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 installer logging

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

The installer creates the log directory as soon as you launch the wizard.

The log file is located at `%AllUsersProfile%\ApplicationData\Veritas\VPI\log\<date_timestamp>\AppControl_Installer_A.txt`.

On Windows Server 2008 and 2008 R2, the path is

`%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>\AppControl_Installer_A.txt`.

Here, *%AllUsersProfile%* is the Windows variable that typically expands to `C:\Documents and Settings\All Users`.

On Windows 2008 and 2008 R2, it typically expands to `C:\ProgramData`.

ApplicationHA Console logging

Use the hagetcf utility to collect the ApplicationHA 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 ApplicationHA 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 ApplicationHA Console logs:

1 On the ApplicationHA 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 view logging

The ApplicationHA view generates log files that are appended by letters. The log files are segregated based on operations and configuation settings.

- Operations and wizard logging

  Operations logs include the Symantec ApplicationHA Configuration Wizard logs and logs related to the various operations performed from the ApplicationHA view.

  Operations logs are located at `<%vcs_home%>log\AppControlOperations_A.log.`

  Here, `<%vcs_home%>` is set during ApplicationHA guest component installation is typically, `C:\Program Files\Veritas\Cluster Server`.

  The Symantec ApplicationHA Configuration Wizard also maintains in-memory logs that are available only during the time the wizard is running. These logs are maintained on a per session basis. The in-memory logs are purged after the wizard is closed. These logs are not stored in any file or directory.

- Configuration settings logging

  Application monitoring configuration settings related changes are logged separately and are available at `<%vcs_home%>log\AppControlSettings_A.log.`

  Here, `<%vcs_home%>` is set during ApplicationHA guest component installation is typically, `C:\Program Files\Veritas\Cluster Server`.

  These settings are accessible from the Settings link on the ApplicationHA view.

- ApplicationHA view logging

  The ApplicationHA view also maintains in-memory logs of the operations performed from the view. These logs are available only until the time the logs window is open. To view the current logs, click the **View Logs** link available on the right hand side in the ApplicationHA view. A window appears within the view. This window displays the details of the operations performed.

Agent logging

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 at `<%vcs_home%>log\agent_A.txt`.

Here, `<%vcs_home%>` is set during ApplicationHA guest component installation is typically, `C:\Program Files\Veritas\Cluster Server`.

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.

Symantec ApplicationHA plugin registration error

The Symantec ApplicationHA plugin unregistration may fail during ApplicationHA Console uninstallation.

Resolution

Use the PluginMgmt.bat utility to unregister the plugin.

See "Administering plugin registration using the PluginMgmt.bat utility" on page 63.

If the PluginMgmt.bat utility fails to unregister the plugin, then perform the following steps to manually remove the plugin from the vCenter Server:

1. Open a Web browser and log on to the vCenter Server Managed Object Browser (MOB) using the following URL:

   `https://`*vCenter Server IP or host name*`/mob`

   Here, <vCenter Server IP or host name> is the IP address or system name of the vCenter Server where the ApplicationHA plugin is registered.

   If the VMware Web Service does not use the default port 443, then specify the following URL:

   `https://`*vCenter Server IP or host name*`:`*PortNumber*`/mob`

2. When prompted specify the credentials of a user that has the Unregister extension privilege on the vCenter Server.

3. After successful authentication, type the following URL in the browser address bar:

   ```
   https://<vCenter Server IP or host name>/mob/
   ?moid=ExtensionManager
   ```

   This opens the vCenter Server Extension Manager.

   If the ApplicationHA plugin is registered, the following entry is displayed in the Properties table:

   extensionList["com.symantec.applicationha"]

4. In the Methods table click **UnregisterExtension**.

   This launches the UnregisterExtension method in a separate browser window.

5. In the UnregisterExtension window, type the following in the extensionKey value field:

   `com.symantec.applicationha`

6. Click **Invoke Method**.

   This unregisters the ApplicationHA plugin from the vCenter Server.

   Verify that the ApplicationHA plugin entry is cleared from the Properties table in the vCenter Server Extension Manager.

Symantec ApplicationHA tab does not display the application monitoring status

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

Resolution

Verify the following conditions and then refresh the ApplicationHA tab in the vSphere Client console:

- Verify that the ApplicationHA Console host is running and is accessible over the network.
- Verify the VMware Web Service is running on the vCenter Server.
- Verify that the Veritas Storage Foundation Messaging Service is running on the ApplicationHA Console and the virtual machine.
  If it is stopped, type the following on the command prompt:
  ```
  net start xprtld
  ```
- Verify that ports 14152, 14153, and 5634 are not blocked by a firewall.
- Log out of the vSphere Client and then login again. Then, verify that the Symantec ApplicationHA plugin is installed and enabled.

Symantec ApplicationHA tab displays the “Unable to retrieve the status of this virtual machine.” error

The Symantec ApplicationHA tab in the vSphere Client console may display the following error:

```
Unable to retrieve the status of this virtual machine.
Please verify the following:
```

- `VMware Tools is installed`
- `Symantec ApplicationHA is installed and the required services are running`
- `The machine is switched on, has a valid IP address, and is accessible over the network`
- `The required ports are not blocked by a firewall`

Resolution

Verify the following conditions and then refresh the ApplicationHA tab in the vSphere Client console:

- Verify that the ApplicationHA Console host is running and is accessible over the network.
- Verify that the Symantec ApplicationHA Service is running on the ApplicationHA Console host.
- Verify that the vCenter Server is running and accessible over the network.
- Verify that the Veritas Storage Foundation Messaging Service is running on the vCenter Server.

  If it is stopped, type the following on the command prompt:

  ```
  net start xprtld
  ```
- Verify the VMware Web Service is running on the vCenter Server.
- Verify that ports 14152, 14153, and 5634 are not blocked by a firewall.
- Verify that the VMware Web Service port that was configured before registering the ApplicationHA plugin is still being used.

  If the Web Service port has changed, unregister the ApplicationHA plugin on the vCenter Server and register it again.

  See "Administering plugin registration using the PluginMgmt.bat utility" on page 63.

Symantec ApplicationHA tab displays a "Failed to retrieve status." popup message

The Symantec ApplicationHA tab in the vSphere Client console may display the following error in a popup window:

```
Failed to retrieve status.

Please ensure the machine is powered on and required
services are running.
```

Resolution

This error may occur if you reinstall or repair Symantec ApplicationHA Console in your application monitoring environment.

Perform the following actions:

- Verify that the virtual machine is powered on and accessible over the network.
- Verify that the Veritas Storage Foundation Messaging Service (xprtld) is running on the virtual machine.
- Close the ApplicationHA tab and open it again.

In the vSphere Client, click another virtual machine, then click the original virtual machine again and then select the ApplicationHA tab, or exit the vSphere Client and launch it again.
The ApplicationHA view then displays the status of the configured applications on the virtual machine.

Symantec ApplicationHA Configuration Wizard displays blank

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

Resolution

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

ApplicationHA Console files become corrupt

If the Symantec ApplicationHA Console files and registry becomes corrupt and the Console fails to respond, perform the following to restore and get the ApplicationHA Console up and running.

These steps presume that you had backed up the following directories and registry from the ApplicationHA Console host, after configuring application monitoring on the virtual machines:

- <*installdirectory*>`\Veritas Shared`
  Here, <*`installdirectory`*> is the directory where you installed the Console, typically, `C:\Program Files\Veritas`.
- `%AllUsersProfile%\Symantec\ApplicationHA\sec`
  `%AllUsersProfile%\Symantec\ApplicationHA\conf`
  Here %AllUsersProfile% typically expands to C:\ProgramData.
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veritas\VPI`

Perform the following steps on the ApplicationHA Console host:

1 Restore the veritas shared directory that you backed up to the following location:
<*installdirectory*>`\`
Here, <*`installdirectory`*> is the directory where you installed the Console, typically, `C:\Program Files\Veritas`.

2 From the Windows registry editor, restore the following VPI registry key that you had backed up earlier:
Perform the following:

- Click **Start > Run**, type **regedit** and then click **OK** to open the Windows Registry Editor.
- Navigate to the following location:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veritas`
- Click **File > Import** and then specify the VPI registry key that you had backed up earlier and then click **Open**.
- After the import is successful, save and close the registry editor.

3 From Windows Add or Remove Programs, repair the Veritas Operations Manager (Host Component).
Refer to the VOM documentation for instructions.

4 From the Windows Add or Remove Programs, repair ApplicationHA Console.
See "Repairing the Symantec ApplicationHA Console installation" on page 106.

5 After the Console repair completes, stop the following services:

- Symantec ApplicationHA Authentication Service
- Symantec ApplicationHA Service
- Veritas Storage Foundation Messaging Service

6 Restore the sec and conf directories that you backed up earlier at the following location:
`%AllUsersProfile%\Symantec\ApplicationHA\`
`%AllUsersProfile%\Symantec\ApplicationHA\`
Here %AllUsersProfile% typically expands to C:\ProgramData.

7 Start the services that you stopped in step 5 earlier.

8 Exit the vSphere client, launch it again and then log on to the vCenter Server that manages the virtual machines where you have configured application monitoring.

9 In the vSphere client Inventory pane, click on a virtual machine where you have configured application monitoring, and then select the ApplicationHA tab to view the status of the applications configured.

ApplicationHA Console host becomes permanently unavailable

If the Symantec ApplicationHA Console host becomes unavailable either due to a server crash or because you want to set up the Console on a new server altogether, there are series of steps that you must perform before you get the new ApplicationHA Console host up and running.

Perform the following steps:

1. Unregister the ApplicationHA plugin for the vCenter Server.
   - If your existing ApplicationHA Console host is still available, use the pluginmgmt.bat utility for the operation.
     See "Administering plugin registration using the PluginMgmt.bat utility" on page 63.
   - If you have lost the existing ApplicationHA Console host, perform the operation manually.
     Refer to the steps mentioned in the topic "Symantec ApplicationHA plugin registration error" on page 97.
2. Install ApplicationHA Console on the new server.
   See "Installing Symantec ApplicationHA Console" on page 29.
3. Exit the vSphere client, launch it again and then log on to the vCenter Server that manages the virtual machines where you have configured application monitoring.
4. From the vSphere client Inventory pane, click on a virtual machine where you have configured application monitoring, select the ApplicationHA tab, and then configure the virtual machine administrator account on the new Console host.
   See "Configuring single sign-on between the virtual machine and the ApplicationHA Console" on page 40.
5. Repeat step 4 for all the virtual machines where you have configured application monitoring.
   The ApplicationHA tab then displays the status of the configured applications on the virtual machines.
6. Configure Symantec ApplicationHA user privileges for the vCenter Server users, if required.
   See "Configuring Symantec ApplicationHA access control" on page 42.

VMware vCenter Server becomes permanently unavailable

If the VMware vCenter Server becomes unavailable either due to a server crash or because you want to set up a new server altogether, perform the following steps to set up the new server in the application monitoring environment:

1. Create a new vCenter Server. Refer to VMware documentation for instructions.
   Symantec ApplicationHA supports VMware vCenter version 4.1 or later.
2. Move all the VMware ESX systems to the new vCenter Server you just created.
   Refer to the VMware documentation for instructions.
3. Register the ApplicationHA plugin for the vCenter Server.
   See "Administering plugin registration using the PluginMgmt.bat utility" on page 63.
4. Exit the vSphere client, launch it again and then log on to the new vCenter Server where you moved all the ESX systems.
5. In the vSphere client Inventory pane, click on a virtual machine where you have configured application monitoring, and then select the ApplicationHA tab to view the status of the applications configured.
6. Configure Symantec ApplicationHA user privileges for the vCenter Server users, if required.
   See "Configuring Symantec ApplicationHA access control" on page 42.

Appendix C

Repairing Symantec ApplicationHA installation

This chapter includes the following topics:

- "Repairing the Symantec ApplicationHA Console installation" on page 106
- "Repairing Symantec ApplicationHA guest component installation on a virtual machine" on page 109
- "License management" on page 111

Repairing the Symantec ApplicationHA Console installation

Use the Symantec ApplicationHA installer to repair the Symantec ApplicationHA Console installation in your VMware virtualization environment.

Repairing the installation restores the server installation to its original state. Repairing fixes missing or corrupt files, shortcuts, and registry entries on the local system.

Note: You can repair the Symantec ApplicationHA Console installation on the local system only. Repairing an installation remotely is not supported.

Consider the following points before you proceed:

- Before repairing the Symantec ApplicationHA guest components, you must first repair the Veritas Operations Manager (Host Component) on the system.

  The installer prompts you to run the VOM host component repair.
- While the installer is repairing the server installation, application monitoring may be temporarily suspended.

  If you have configured application monitoring, then the ApplicationHA view in the vSphere Client may not display the most current status of the applications configured on the virtual machines.
- The installer uses the logged-on user account context to perform the repair. Verify that the logged-on user has local administrator privileges on the system where you want to repair the installation.
- After the repair completes successfully, you may have to register the Symantec ApplicationHA plugin on the VMware vCenter Server again.

To repair the ApplicationHA Console installation

1. On the Symantec ApplicationHA Console host open Windows Add or Remove Programs.

   Click **Start > Settings > Control Panel** and then double-click **Add or Remove Programs**.

   In case of Windows Server 2008, click **Start > Settings > Control Panel** and then double-click **Programs and Features**.
2. In the Add or Remove Programs window, select **Symantec ApplicationHA Console** in the programs list and then click **Change** to launch the Symantec ApplicationHA installer.

3. On the Mode Selection panel, click **Repair** and then click **Next**.

4. Click **OK** on the dialog box that prompts you to repair the Veritas Operations Manager (Host Component).

   You must repair the VOM host component before you proceed.

   From Windows Add or Remove Programs, select **Veritas Operations Manager (Host Component)** and click **Change** to launch the installer. Then follow the installer steps to complete the repair.

   Refer to VOM documentation for more information.

5. On the System Selection panel the installer automatically selects the local system for repair and begins verification. After the status shows as *Ready for repair*, click **Next**.

   You can repair the installation on the local system only.

   The wizard performs the required validation checks on the local system. If the system does not meet the required criteria, the status is reflected as *Verification failed*. To view the cause of a validation failure, click the Information icon for the system. Rectify the issue and then click **Re-verify** to perform the validation checks on the rejected system again.

   The wizard does not proceed with the repair unless the system has passed the validation checks.

6. On the Pre-install Summary panel, review the pre-update summary and then click **Next**.

   Click **Save Report** if you wish to save the summary report for reference.

7. The Installation panel displays the progress of the installation on the selected system. After the panel indicates that the installation is complete, click **Next**.

8. On the Post-install Summary panel, review the installation results and then click **Next**.

   If the installation has failed, review the post-install summary report and refer to the wizard log file for details.

   The log file is located at

   `%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>`.

   You may have to repeat the installation repair in case the installation fails.

9. On the Finish panel click **Finish**.

   This completes the Symantec ApplicationHA Console installation repair.

10. If you have configured application monitoring for ApplicationHA Console, start the Veritas High Availability Engine service on the ApplicationHA Console host.

    Type the following on the command prompt:

    ```
    hastart
    ```

11 After performing the repair, the ApplicationHA tab may fail to retrieve the application status. In such a case, you may have to close the ApplicationHA tab and open it again.

In the vSphere Client, click another virtual machine, then click the original virtual machine again and then select the ApplicationHA tab, or exit the vSphere Client and launch it again. The ApplicationHA view then displays the status of the configured applications on the virtual machine.

Repairing Symantec ApplicationHA guest component installation on a virtual machine

Use the Symantec ApplicationHA installer to repair the Symantec ApplicationHA guest components installation on the virtual machines in your VMware virtualization environment.

Repairing the installation on a virtual machine restores the installation to its original state. Repairing fixes missing or corrupt files, shortcuts, and registry entries on the local system.

Note: You can repair the virtual machine component installation on the local system only. Repairing an installation remotely is not supported.

Consider the following points before you proceed:

- Before repairing the Symantec ApplicationHA guest components, you must first repair the Veritas Operations Manager (Host Component) on the system.
  The installer prompts you to run the VOM host component repair.
- While the installer is repairing the installation on the virtual machine, application monitoring may be temporarily suspended.
  If you have configured application monitoring, then the ApplicationHA view in the vSphere Client may not display the most current status of the applications and services on the virtual machine.
- The installer uses the logged-on user account context to perform the repair. Verify that the logged-on user has local administrator privileges on the system where you want to repair the installation.

To repair the virtual machine component installation

1. On the virtual machine open Windows Add or Remove Programs.
   Click **Start > Settings > Control Panel** and then double-click **Add or Remove Programs**.
   In case of Windows Server 2008, click **Start > Settings > Control Panel** and then double-click **Programs and Features**.
2. In the Add or Remove Programs window, select **Symantec ApplicationHA Guest** in the programs list and then click **Change** to launch the Symantec ApplicationHA installer.
3. On the Mode Selection panel, click **Repair** and then click **Next**.
4. Click **OK** on the dialog box that prompts you to repair the Veritas Operations Manager (Host Component).

You must repair the VOM host component before you proceed.

From Windows Add or Remove Programs, select **Veritas Operations Manager (Host Component)** and click **Change** to launch the installer. Then follow the installer steps to complete the repair.

Refer to VOM documentation for more information.

5 On the Virtual Machine Selection panel the installer automatically selects the local system for repair and begins verification. After the status shows as *Ready for repair*, click **Next**.

You can repair the installation on the local system only.

The wizard performs the required validation checks on the local system. If the system does not meet the required criteria, the status is reflected as *Verification failed* . To view the cause of a validation failure, click the Information icon for the system. Rectify the issue and then click **Re-verify** to perform the validation checks on the rejected system again.

The wizard does not proceed with the repair unless the system has passed the validation checks.

6 On the Pre-install Summary panel, review the pre-update summary and then click **Next**.

Click **Save Report** if you wish to save the summary report for reference.

7 The Installation panel displays the progress of the installation on the selected system. After the panel indicates that the installation is complete, click **Next**.

8 On the Post-install Summary panel, review the installation results and then click **Next**.

If the installation has failed, review the post-install summary report and refer to the wizard log file for details.

The log file is located at `%AllUsersProfile%\ApplicationData\Veritas\VPI\log\<date_timestamp>`.

On Windows Server 2008 and 2008 R2, the path is `%AllUsersProfile%\Veritas\VPI\log\<date_timestamp>`.

You may have to repeat the installation repair in case the installation fails.

9 On the Finish panel click **Finish**.

This completes the Symantec ApplicationHA virtual machine component installation repair.

License management

The product installer lets you add or remove license keys for Symantec ApplicationHA components. You may want to add a license if the embedded two-month evaluation key has expired.

You can change the license keys from any virtual machine that has Symantec ApplicationHA components installed. You cannot change the license key from the Symantec ApplicationHA Console.

Perform the following steps to manage Symantec ApplicationHA license keys.

To manage the Symantec ApplicationHA license keys

1 Launch Windows Add or Remove Programs from the Windows start menu.

Click **Start > Settings > Control Panel** and then double-click **Add or Remove Programs**.

For Windows Server 2008, click **Start > Settings > Control Panel** and then double-click **Programs and Features**.

2 Select **Symantec ApplicationHA** and then click **Change** to launch the Symantec ApplicationHA installer.

3 On the Mode Selection panel, select **License Management** and then click **Next**.

4 On the License panel, select **Enter license key** and then enter the license key that you want to add.

5 Click Show Details to view what features and components are available for use with the specified license key.

6 Click **Finish**.

The specified license takes effect immediately.

Index

A

agent functions
- ElifNone 90
- FileNone 89
- FileOnOff 91
- FileOnOnly 92
- Process 84

agents
- ElifNone 90
- FileNone 89
- FileOnOff 91
- FileOnOnly 92
- Process 84

AppFaultGraceTime 61

ApplicationHA guest components
- install using command line 36
- install using wizard 33

AppRestartLimit 61

AppStartStopTimeout 61

attribute definitions
- Process agent 85

attributes
- ElifNone agent 90
- FileNone agent 89
- FileOnOff agent 91
- FileOnOnly agent 92

C

client license 19

E

ElifNone agent
- agent functions 90
- attributes 90
- description 90
- state definitions 90

F

FileNone agent
- agent functions 89
- attributes 89
- description 89
- state definitions 89

FileOnOff agent
- agent functions 91
- attributes 91
- description 91
- state definitions 91

FileOnOnly agent
- agent functions 92
- attributes 92
- description 92
- state definitions 92

I

infrastructure agents
- Process agent 84

infrastructure and support agents
- ElifNone agent 90
- FileNone agent 89
- FileOnOff 91
- FileOnOnly 92

install
- ApplicationHA guest components, command line 36
- ApplicationHA guest components, installation wizard 33

L

license key 19

License management 111

licensing 19

Logs
- Agents 96
- Application monitoring configuration settings 95
- ApplicationHA Console 94
- ApplicationHA view 95
- installer 94

Symantec ApplicationHA Configuration Wizard 95

P

Process agent
- agent functions 84
- attribute definitions 85
- description 84
- state definitions 84

product licensing 19

R

repair
- ApplicationHA Console installation 106
- virtual machine component installation 109

S

settings 61

state definitions
- ElifNone agent 90
- FileNone agent 89
- FileOnOff agent 91
- FileOnOnly agent 92
- Process agent 84

Symantec ApplicationHA
- license 19

U

uninstalling Symantec ApplicationHA 67