Symantec™ ApplicationHA User's Guide

Windows Server 2003 and 2003 R2, Windows Server 2008 and 2008 R2

6.0

October 2011

Symantec

Symantec™ ApplicationHA User's Guide

Product_version: 6.0

Document_version: 6.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Contents

Chapter 1

Introducing Symantec ApplicationHA

This chapter includes the following topics:

What is Symantec ApplicationHA

Symantec ApplicationHA provides monitoring capabilities for applications running inside 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 Group Membership and Atomic Broadcast (GAB) and Low Latency Transport (LLT). Symantec ApplicationHA has a lightweight server footprint that allows faster installation and configuration.

Key benefits include the following:

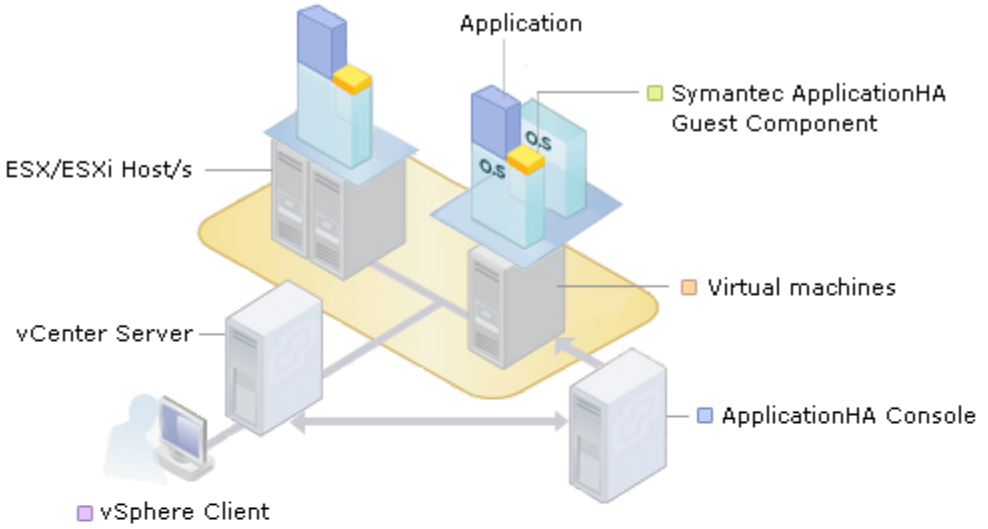
- Out of the box integration with the VMware vCenter Server HA
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside virtual machines.

- Standardized way to manage applications using a single interface that is integrated with VMware vSphere Client
- Specialized Application Maintenance mode, in which ApplicationHA allows you to intentionally take an application out of its purview for maintenance or troubleshooting
- Integration with VMware SRM Server that provides the capability to resume application monitoring after the virtual machines are started on the recovery site.

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.

The following figure displays the sample deployment of Symantec ApplicationHA.



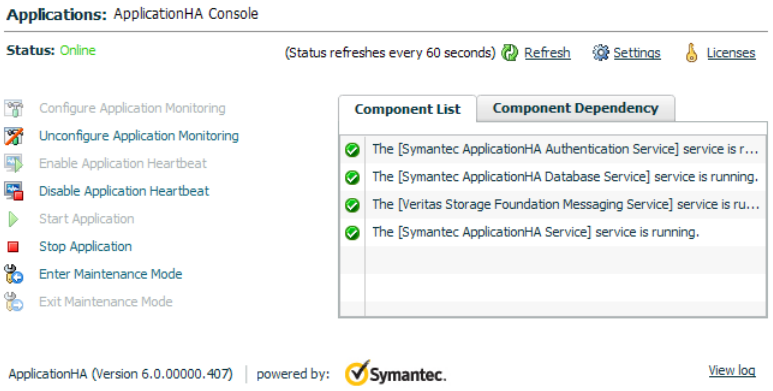
- Symantec ApplicationHA Guest Component
  - Include Heartbeat components integrated with VMware HA
  - Include other components for monitoring application status
- Virtual machines
  - Running Windows OS or Linux OS
- ApplicationHA Console
  - Integrates with vSphere Client
  - Has vCentre privileges to provide discretionary access control (DAC)
  - Offers single sign-on to virtual machines under ApplicationHA control
  - Can be installed on a virtual machine or a physical machine
- vSphere Client
  - Integrates with Symantec ApplicationHA View

ApplicationHA provides a vCenter plug-in for integration with VMware vSphere Client and adds the following interfaces for performing application monitoring tasks. These interfaces appear in the vSphere Client after you install the ApplicationHA Console.

- ApplicationHA tab: The ApplicationHA tab is the primary interface for performing the application monitoring operations on a virtual machine.

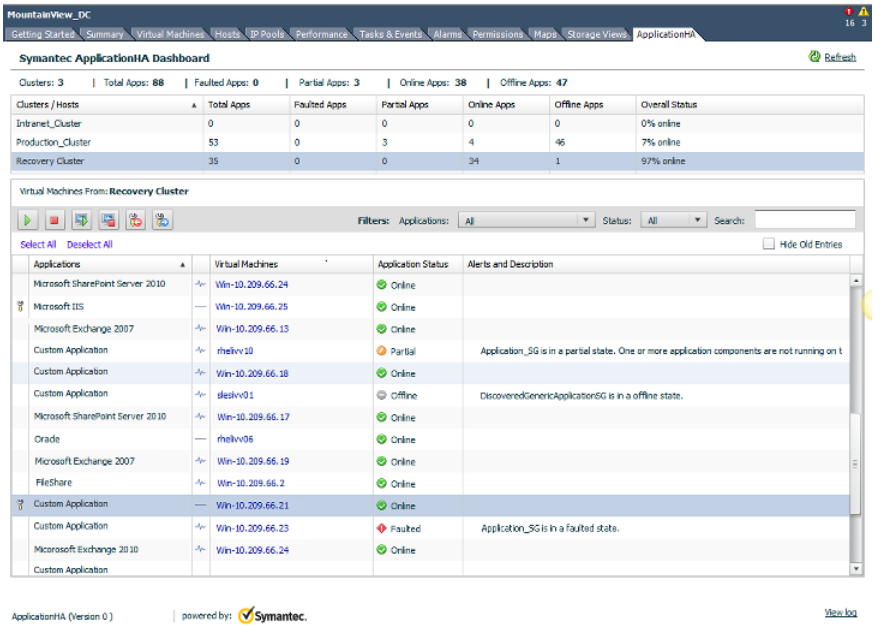
From this view you configure application monitoring and then monitor and control the configured application on the virtual machine. After configuring application monitoring, the Symantec ApplicationHA view displays the state of the application and the component dependencies.

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



- ApplicationHA dashboard: The ApplicationHA dashboard is the primary interface for administering the configured applications on a VMware cluster or datacenter. After configuring application monitoring, the ApplicationHA dashboard displays the state of the application.

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



How ApplicationHA works

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 agents monitor the overall health of the configured applications by running specific commands, tests, or scripts. For more details, see the agent functions section of the application-specific agent guides or the generic agent guide distributed with ApplicationHA.

The ApplicationHA Heartbeat agent is 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, ApplicationHA performs the following actions in the specified sequence.

1. The ApplicationHA agents attempt to restart the application for a configurable number of times.
2. ApplicationHA gracefully restarts the virtual machine. This action is performed only if you have configured ApplicationHA-initiated virtual machine restart. This action is not performed if you have not configured ApplicationHA-initiated virtual machine restart.

3. If the agents are unable to start the application, Symantec ApplicationHA stops sending the application heartbeat to VMware HA.
4. Depending on the configuration, VMware HA takes the necessary corrective action.
5. After the virtual machine is restarted, Symantec ApplicationHA agents attempt to start the application and its dependent components in a predefined order.
6. If the application fails to start after the configurable number of VMware HA attempts and if the virtual machine Auto Recovery is configured, ApplicationHA triggers the request to Backup Exec for restoring the latest successful backup of the virtual machine.

The auto-restore capability is available only in a local VMware cluster environment. This capability is not available for virtual machines configured under ApplicationHA, in a VMware SRM environment.

For details on configuring application monitoring in a VMware SRM environment, refer to, *Symantec™ ApplicationHA User's Guide*.

How ApplicationHA integrates with Symantec Backup Exec

A typical Backup Exec configuration in a VMware environment comprises a Media Server installed on a separate physical or virtual machine and a Plug-in installed on the VMware vSphere client.

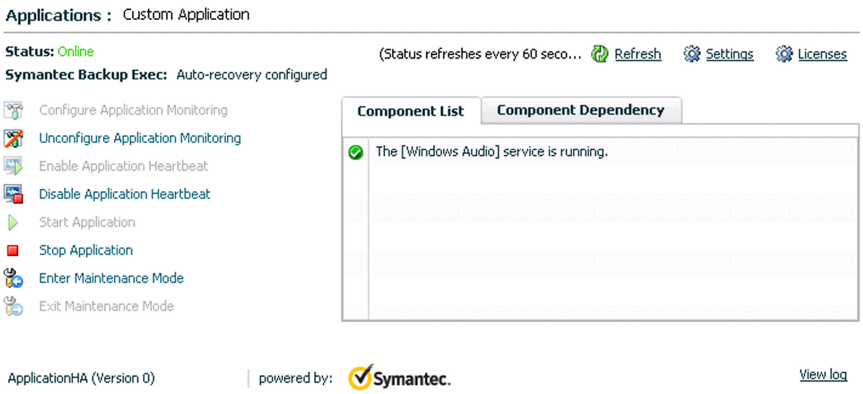
The Media Server serves as a management console for various backup specific administrative jobs to be performed.

The Plug-in registration adds a “Symantec Backup Exec” tab in the vSphere Client. This tab is the primary interface that enables you to configure "Virtual Machine Auto Recovery". To configure "Virtual Machine Auto Recovery" for virtual machines under ApplicationHA control, you are required to set up a link between the ApplicationHA Console and the Media Server. Setting up the link between the ApplicationHA Console and the Media Server, authenticates the ApplicationHA Console Server user account.

After you authenticate the ApplicationHA Console Server user account and configure "Virtual Machine Auto Recovery", the Backup Exec High Availability (BE HA) service transfers the virtual machine details such as hostname, virtual machine ID, and the MAC address to the ApplicationHA Console Server. ApplicationHA Console Server then registers the specified virtual machine for auto-restore and adds the entries to the Console Server database.

After the ApplicationHA Console Server registers the virtual machine for auto-restore, the ApplicationHA tab displays that the "Virtual Machine Auto

Recovery" is configured. The following figure of ApplicationHA tab represents "Virtual Machine Auto Recovery" is configured.



The Backup Exec Virtual Machine Auto-Recovery database and the ApplicationHA Console Server database are synchronized once everyday. If you perform any changes to the "Virtual Machine Auto Recovery" settings or reconfigure the ApplicationHA Console Server, the "Virtual Machine Auto Recovery" settings are updated in the ApplicationHA Console Server database during the next synchronization cycle.

Note: If you need to update the ApplicationHA Console Server database before the next synchronization cycle, you must re-configure Virtual Machine Auto Recovery settings for the virtual machines.

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 restarts the virtual machine. If the application fails to start even after virtual machine reboot, the ApplicationHA Heartbeat agent triggers the request for restoring the virtual machine backup. The Console Server receives and redirects this request to the Media Server.

Note: If you have configured ApplicationHA-initiated virtual machine restart, ApplicationHA gracefully restarts the virtual machine before it stops sending the application heartbeat for VMware HA.

The Media Server then verifies if "Virtual Machine Auto Recovery" is configured. After the verification check is successful a user confirmation prompt is displayed.

This prompt is displayed only if you have configured the setting for user confirmation. After the user approves the request, the Media Server restores the virtual machine using the latest available backup.

Note: If the request for virtual machine restore fails, refer to the AutoRestoreTriggerStatus_A.log file at %Programdata%\Symantec\ApplicationHA\Logs on the ApplicationHA Console Server.

ApplicationHA tab displays the following conditions and respective status messages when "Virtual Machine Auto Recovery" is configured.

Condition	Status
Request for virtual machine restore is triggered but user consent is not yet received	Awaiting user consent for virtual machine restore
User consent for virtual machine restore is received and the virtual machine restore job is in queue	Queued for virtual machine restore

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, as follows:

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 and 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, and 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 and adds the ApplicationHA tab and the ApplicationHA dashboard to the VMware vSphere Client.
  This plugin is required to view the ApplicationHA tab and the ApplicationHA dashboard 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.
  You can use the ApplicationHA dashboard to administer application monitoring on a VMware cluster or datacenter.
- 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.
- The Console uses Symantec ApplicationHA Authentication service to provide secure communication between the virtual machine and the vSphere Client. It uses digital certificates for authentication and uses SSL to encrypt communications. Symantec ApplicationHA uses platform-based authentication; it does not store user passwords.
- The Console adds the Symantec ApplicationHA privileges to the vSphere Client environment. You can use the privileges to configure access control for vCenter Server users and groups.

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 privileges to them or assign privileges to the existing roles that are available in the vSphere environment. Application monitoring operations are enabled or disabled depending on the privileges that are assigned to the vCenter user account. For example, the Admin privilege is required for configuring application monitoring on a virtual machine.

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

Symantec ApplicationHA provides the following privileges:

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

Symantec ApplicationHA agents

Agents are application-specific modules that plug into the ApplicationHA framework that manages applications and resources of predefined resource types configured for applications and components on a system. The agents are installed when you install Symantec ApplicationHA guest components. These agents start, stop, and monitor the resources configured for the applications and report state changes. If an application or its components fail, 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.
Refer to the *Symantec™ ApplicationHA Generic Agents Guide* for more details about the infrastructure agents.

- 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 guest components.
  The ApplicationHA agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing ApplicationHA guest components installation.
  Refer to the Symantec Operations Readiness Tools (SORT) Web site for information on the latest agent pack availability.
  https://sort.symantec.com
  Refer to the agent-specific configuration guide for more details about the application agents.

Chapter 2

Configuring Symantec ApplicationHA in a local VMware cluster environment

This chapter includes the following topics:

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

SSO configuration involves specifying the virtual machine administrator account to set up a permanent authentication for the virtual machine.

Use the ApplicationHA tab to manually configure the single sign-on between the virtual machine and the Console host. You are required to manually configure the single sign-on during the following cases:

- SSO configuration has failed during the guest installation or upgrade
- You have not configured SSO during the guest installation or upgrade

- You have installed or upgraded the guest components using the CLI

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 encrypt 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 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**.

Disabling VMware HA at a cluster level

You can disable VMware HA if you do not want VMware HA to restart the virtual machine in case of a heartbeat failure. In some cases, VMware HA restarts the virtual machine even if VMware HA is disabled at the VMware cluster level. This may occur if the VMware HA settings are set incorrectly. Use the following steps to correctly disable VMware HA.

To disable VMware HA

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 **VM Monitoring**.

If VM Monitoring does not appear, select **Cluster Features** and then in the right pane, check **Turn on VMware HA**.

4 In VM Monitoring drop-down list, select **Disabled** to disable virtual machine monitoring and application monitoring.

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

6 In the right pane, clear the **Turn on VMware HA** check box.

7 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 includes 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.

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

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**.

Configuring Virtual Machine Auto Recovery

You must perform this task only if you want to configure the virtual machine for auto recovery.

To configure "Virtual Machine Auto Recovery" for virtual machines under ApplicationHA control, ensure that the ApplicationHA Console is powered on and accessible from the Backup Exec Media Server.

Perform the following tasks from the BackUp Exec tab available in the vSphere Client:

- Review the list of virtual machines for which the backup is taken on the Media Server.
- Authenticate the user account of ApplicationHA Console and thus set up a link with the Media Server.
- Configure "Virtual Machine Auto Recovery" for virtual machines under ApplicationHA control.
  You can configure "Virtual Machine Auto Recovery" only in a local VMware cluster environment. Configuring "Virtual Machine Auto Recovery", in a VMware SRM environment is not supported.

Note: You cannot configure "Virtual Machine Auto Recovery" for a virtual machine on which ApplicationHA Console is installed.

- To define the time interval, in minutes, for which the heartbeat agent must wait for VMware HA to reset the virtual machine, modify the "vmrestoretimeout" attribute configuration settings.
  See “Administering vmrestoretimeout” on page 57.

  Note: The default value for vmrestoretimeout is 5 minutes. The vmrestoretimeout value must always be greater than the VMware HA configuration settings.

  For more details on vmrestoretimeout attribute, refer to *Symantec™ ApplicationHA Generic Agents Guide*

For more details on configuring "Virtual Machine Auto Recovery", refer to *Symantec Backup Exec™ Management Plug-in for VMware® User's Guide*.

Best practices for configuring Virtual Machine Auto Recovery

Review the following best practices that you must follow while configuring Virtual Machine Auto Recovery.

- Ensure that the latest backup is available for a virtual machine. You must take a backup of the virtual machine if you update the configuration settings for an application configured on the virtual machine.
- If you plan to move the Media Server or the ApplicationHA Console server to a different domain, you must ensure that the older FQHN of a virtual machine points to the same virtual machine in the DNS sever of the new domain. Failing this, you must re-configure "Virtual Machine Auto Recovery" for all the virtual machines, after moving the servers to a new domain.
- If you plan to change the hostname of a virtual machine, you must ensure that the older hostname points to the same machine, in the DNS server. Failing this, you must re-configure "Virtual Machine Auto Recovery" for that virtual machine.
  For details on re-configuring Virtual Machine Auto Recovery, refer to, *Symantec Backup Exec™ Management Plug-in for VMware® User's Guide*.
- The ApplicationHA Console server must be powered-on and accessible over the network, before and after the request for virtual machine auto-restore is triggered. Failing this, the virtual machine is not restored.
- If you plan to clone a virtual machine, you must disable "Virtual Machine Auto Recovery" for that virtual machine. After you clone the virtual machine, you must perform the following tasks:

- For the cloned virtual machine: Re-configure Application monitoring and then configure "Virtual Machine Auto Recovery".
- For the original virtual machine: Re-configure "Virtual Machine Auto Recovery".

- If you update the "Virtual Machine Auto Recovery" settings, it is recommended that you must take the complete virtual machine backup again. This ensures to save the changed settings.

Chapter 3

Configuring Symantec ApplicationHA in a VMware site recovery environment

This chapter includes the following topics:

About Site Recovery Manager (SRM)

VMware vCenter Site Recovery Manager (SRM) is a disaster recovery solution for your virtual machines. SRM supports array-based replication of the virtual machines configured at the primary or protected site, to the recovery site and helps to manage synchronization of data between the protected and the recovery site.

In case of any disaster, migration of the virtual machines from the protected site to the recovery site is defined by a recovery plan that specifies the recovery tasks to be performed. By integrating seamlessly with VMware Infrastructure and vCenter server, SRM helps to automate and accelerate the recovery process.

For more details on SRM, refer to, VMware product documentation.

How does Symantec ApplicationHA integrate with VMware SRM Server

In a local application monitoring configuration, Symantec ApplicationHA communicates with VMware HA and conveys the application health status in 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. However, these configurations do not provide monitoring capability if an outage affects the entire local site.

To configure application monitoring in a site recovery environment, Symantec ApplicationHA provides components that must be installed on the SRM Server at the recovery site. These components perform the following functions and help to initiate the application monitoring capability after the virtual machines are started on the recovery site.

- Deploys the recovery site ApplicationHA Console credentials on to the SRM Server at the recovery site.
- Enables you to configure single sign-on between the recovery site ApplicationHA Console and the virtual machines at the protected site. This SSO configuration enables communication between the protected site virtual machines and the ApplicationHA Console and SRM Server at the recovery site.
- Provides the recovery step result in the VMware history status report.

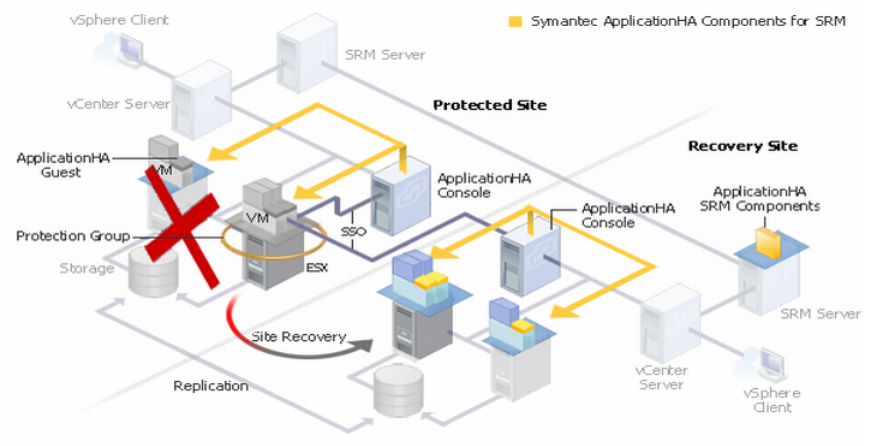
When a disaster strikes, the virtual machines at the protected site are failed over and started on the recovery site. The ApplicationHA guest components then resume application monitoring.

Typical ApplicationHA configuration in a VMware site recovery setup

A typical VMware site recovery setup involves the VMware cluster configuration on both, the protected site and the recovery site. The VMware cluster at the protected site provides high availability of virtual machines during the normal operations and that at the recovery site provides high availability of virtual if the protected site fails.

Figure 3-1 represents the typical disaster recovery VMware cluster configuration with Symantec ApplicationHA enabled for application monitoring continuity.

Figure 3-1 Typical site recovery configuration



Consider that the protected site consists of virtual machines VM1, VM2 and VM3. Similarly the recovery site may have some virtual machine, say VM4. Array-based replication is set up across the storage on protected site and the recovery site. Each site has a clustered setup with SRM Server configured on a separate physical or virtual machine and both the sites are paired to exchange authentication information and discover replicated storage arrays and supported devices.

Additionally,

- The folders, networks, and resource pools on the protected site to which the virtual machines are assigned are mapped on the recovery site.
- The protection group is created based on the datastore group they use. Say, a protection group is created for VM1 and VM2.
- A recovery plan is configured specifying the failover priority order and the recovery steps to be performed.

Along with the SRM Server each site also has a separate vCenter server and Symantec ApplicationHA Console configured on a separate physical or a virtual machine. The Symantec ApplicationHA guest components are installed on the virtual machines where you want to configure application monitoring. A single sign-on mechanism is configured between the s and the ApplicationHA Console on the protected site.

Note: You must ensure that the ApplicationHA Console installed at the recovery site is powered on and accessible from the guest virtual machines at the protected site, before and after the failover.

After this VMware cluster setup is ready, the ApplicationHA components for SRM Server are installed on the SRM server at the recovery site. During installation these components register the IP address or hostname of the recovery site ApplicationHA Console on to the SRM Server.

After installation, a single sign-on mechanism is configured for the virtual machines on the protected site with the ApplicationHA Console on the recovery site. This enables communication between the recovery site ApplicationHA Console, SRM Server and the protected site virtual machines. The SRM recovery plan is then edited to define the action for application monitoring continuity. This action is defined in the form of an ApplicationHA recovery command that must be added to the SRM recovery steps in an appropriate sequence.

When a disaster occurs at the protected site, the VMware disaster recovery plan fails over the virtual machines (VM1 and VM2) to the recovery site. VM1 and VM2 are started on the recovery site as per the configured recovery plan. The ApplicationHA guest components then resume application monitoring and the ApplicationHA recovery command provides the application health status in the SRM history status report.

The highlighted step in the following figure represents a sample application recovery status displayed in the SRM history status report. This sample represents the "Online" application state.

1.3. Shutdown High Priority Protected Virtual Machines		
2. Prepare Storage	Success	00:01:17
2.1. Attach Disks for Protection Group "protection group 1"	Success	00:01:17
3. Suspend Non-critical Virtual Machines	Success	00:00:00
4. Command: c:\windows\system32\cmd.exe /c "C:\Program Files\Symantec\ApplicationHA\SRM\bin\getappstatus.bat" 10.217.56.223	Success: " [10.217.56.223] [Custom Application] => Application is running 1 "	00:00:09
5. Recover High Priority Virtual Machines	Success	00:00:00

If the application is not online, the Application recovery command displays an error. You can view the error details in the ApplicationHA log file.

Following are the application states and its status displayed in the log file.

Application State	**Status displayed**
Online	Application is running
Partially online	Application is partially running
Faulted	Some of the application components are faulted
Offline	Application is not running

If these states are observed while the application is starting, the status is appended by "[Starting Application ...]". However, if the states are observed while the application is stopping, the status is appended by "[Stopping Application ...]".

About application monitoring in VMware SRM environment with customized specifications

In most cases the VMware site recovery clusters may have customized specifications such that after a failover,

- the computer name of a virtual machine on the protected site changes at the recovery site.
- the network settings at the protected site provide an IP address different from that at the recovery site.

If you have configured ApplicationHA in a VMware cluster where the computer name of a virtual machine changes at the recovery site, the ApplicationHA tab at the recovery site displays the cluster state as "Unknown" and the application fails to come online.

Similarly, if the configured application uses the virtual machine IP address, then the application may fail to come online or may not be accessible over the network after a site recovery. You must re-configure the application at the recovery site with the new IP address, using the ApplicationHA tab.

Configuring single sign-on between the recovery and protected site

After installing Symantec ApplicationHA Components for VMware SRM, you must configure single sign-on between the virtual machines at the protected site and the ApplicationHA Console at the recovery site.

Use the Symantec ApplicationHA SRM Components Configuration Wizard to configure the single sign-on for the virtual machines. You must launch this configuration wizard from the ApplicationHA Console at the recovery site.

Before you begin to configure SSO, ensure that you meet the following points:

- ApplicationHA guest components are installed and SSO is configured between the ApplicationHA Console and the virtual machines on the protected site.
- The vCenter logged-on user has ApplicationHA administrator privileges on the virtual machines at the protected site.
- The https port used by the VMware Web Service is enabled for inbound and outbound communication. The default port is 443.

- The https port used by Veritas Storage Foundation Messaging Service (xprtld) is enabled for inbound and outbound communication. The default port is 5634.
- ApplicationHA Console host at the recovery site can access the vCenter Server and the Console host at the protected site.
- The virtual machines can access the Console host at both the sites.
- The virtual machines can access the Console host at recovery site using the fully qualified host name.
- The clock times on the protected site virtual machines and the recovery site ApplicationHA Console are within 30 minutes of one another.
- The following services are running on the Console hosts at both the sites
  - Symantec ApplicationHA Service (ApplicationHA Console)
  - Veritas Storage Foundation Messaging Service (xprtld)
  - Symantec Authentication Service
- Ports 5634, 14152, and 14153 are not blocked by a firewall on the Console hosts and the virtual machines.

To configure single sign-on for the virtual machines

1. On the recovery site, using the vSphere Client, connect to the vCenter Server and navigate to **Home** > **Solutions and Applications** > **Symantec ApplicationHA**
2. On the Symantec ApplicationHA home page, click the **Disaster Recovery** tab.
3. On the Disaster Recovery tab, click **Configure Single Sign-on**.

   This launches the Symantec ApplicationHA SRM components configuration wizard.
4. Review the prerequisites on the Welcome panel and then click **Next**.
5. On the ApplicationHA Inputs panel, specify the required details of the ApplicationHA Console and the vCenter Server at the protected site.

   The installer uses these details to set up a link with the protected site vCenter Server and the ApplicationHA Console. This link enables communication with the guest virtual machines at the protected site.
6. On the System Selection panel, select the virtual machines for configuring single sign-on.

   All the vCenter virtual machines are listed.
7. The Implementation panel displays the SSO configuration progress for each virtual machine. After the configuration process is complete, click **Next**.

If the configuration has failed on any of the machine, refer to the log files for details.

The log file is located on the protected site ApplicationHA Console at the following location:

- For virtual machines running Windows Server 2008 or 2008 R2 operating system
  %AllUsersProfile%\Symantec\ApplicationHA\Logs
- For virtual machines running Windows Server 2003 operating system
  %AllUsersProfile%\Application Data\Symantec\ApplicationHA\Logs

You may have to rectify the cause and repeat the configuration on the failed machines.

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

This completes the SSO configuration between the virtual machines at the protected site and the ApplicationHA Console at the recovery site.

During a disaster, to ensure application monitoring continuity at the recovery site, proceed to update the VMware SRM recovery plan.

See "Modifying the SRM recovery plan" on page 37.

Modifying the SRM recovery plan

After you have configured SSO between the recovery site ApplicationHA Console and the protected site virtual machines, you must modify the SRM recovery plan to define the action for application monitoring continuity. This action is defined in a form of an ApplicationHA recovery command that must be added to the SRM recovery steps, in an appropriate sequence.

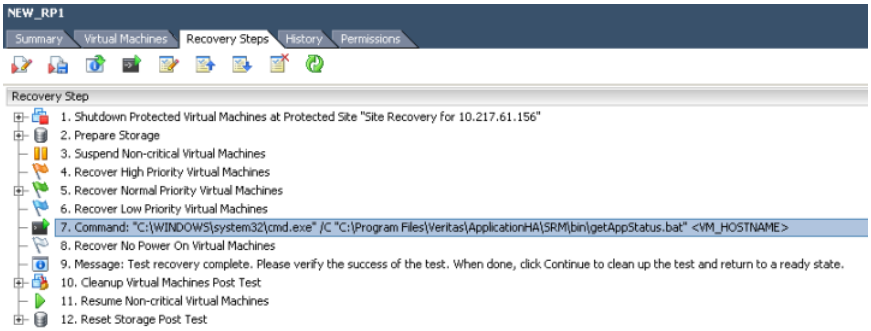
Following is a sample ApplicationHA recovery command that defines the action for application monitoring continuity. You can define this command for a set of priority based virtual machines, or you can define the command per virtual machine.

Note: From the set of priority based virtual machines even if a single virtual machine fails to come online the ApplicationHA recovery command displays an error in the SRM history status report. Symantec thus recommends you to define the ApplicationHA recovery command per virtual machine.

```
C:\Windows\system32\cmd.exe /c c:\Program
Files\Veritas\ApplicationHA\SRM\bin\getappstatus.bat
<VirtualMachine1_HostName> <VirtualMachine2_HostName>
```

A single command defined for a set of priority based virtual machines takes in to account the application monitoring continuity for a maximum of 32 virtual machines. You must add another command for additional virtual machines, if any.

Following is a sample recovery plan with the ApplicationHA recovery command added. This command is defined for a set of priority based virtual machines and thus the application monitoring would resume after all the "High Priority", "Normal Priority" and "Low Priority" virtual machines fail over to the recovery site.



To add the ApplicationHA recovery command for a set of priority based virtual machines

1. On the recovery site, using the vSphere client connect to the vCenter Server and navigate to **Home** > **Solutions and Applications** > **Site Recovery**.
2. From the tree view, select the desired recovery plan and select the **Recovery Steps** tab.
3. Right click on the step that is one below the step that defines the recovery for the desired priority level virtual machines. Select **Add Command**.
4. On the Add Command Step panel, specify the command for ApplicationHA recovery. Click **Ok**.

   The command is added before the selected step.

To add the ApplicationHA recovery command for a single virtual machine

1. On the recovery site, using the vSphere client connect to the vCenter Server and navigate to **Home** > **Solutions and Applications** > **Site Recovery**.
2. From the tree view, select the desired recovery plan and select the **Virtual Machines** tab.
3. On the desired virtual machine, right click and select **Configure**.

4 Follow the wizard steps and on the Edit Post Power on Steps for this VM panel, click **Add Command**.

5 On the Add Command Step panel, specify the ApplicationHA recovery command and click **Ok**.

6 Follow the wizard steps till you reach the Finish panel. Click **Finish**.

About application monitoring in VMware test recovery environment

After you have configured the sites for disaster recovery, you can test the recovery plan to verify the fault-readiness by mimicking a failover from the protected site to the recovery site. This procedure is done without affecting services at either site.

When you run a test recovery plan, the virtual machines specified in the plan appear in the isolated network at the recovery site.

For details, refer to, VMware product documentation.

For test recovery, Symantec recommends you to modify your network settings such that,

- A copy of the replicated storage is created on the recovery site. When you run the test recovery plan, you must use this copy of the replicated data.
- The recovery site SRM Server and ApplicationHA Console is able to communicate with the test virtual machines.

Note: If you configure "Auto" test network for running the test recovery, the virtual machines in the test recovery plan create and fail over in a new isolated network environment at the recovery site. Since the virtual machines start in an isolated network, the recovery site SRM Server and the ApplicationHA Console fail to communicate with the virtual machines and the recovery step for application monitoring continuity fails to provide the application status. Also, the ApplicationHA tab and the dashboard do not provide any status for the configured application.

If you configure a test network same as that of your protected and recovery site, then after a test failover the virtual machines in the test recovery plan communicate with the ApplicationHA Console at both the sites. This reflects the application status on the dashboard at both the sites.

When you initiate a test recovery, copy of the test virtual machines is failed over to the recovery site and the application monitoring recovery status is displayed in the VMware history status report.

Executing the application monitoring fail back

After the original protected site is recovered, VMware SRM does not provide an automated option to fail back the virtual machines to the original protected site.

If you intend to restore the virtual machines and services to the original protected site, you must first configure it to be a recovery site and then run a failback recovery plan. The failback recovery plan migrates the virtual machines from the recovery site to the original protected site. You must run this recovery plan on the original protected site.

Verify the following points to avail the application monitoring continuity after you fail back the virtual machines to the original protected site:

- ApplicationHA SRM components are installed on the protected site SRM Server.
- Single sign-on is configured between the protected site ApplicationHA Console and the virtual machines to be failed back.
- The ApplicationHA recovery command is added to failback recovery plan.

Chapter 4

Configuring application monitoring with Symantec ApplicationHA

This chapter includes the following topics:

About configuring application monitoring with Symantec ApplicationHA

ApplicationHA enables you to configure application monitoring for services, processes, mount points, file share, ApplicationHA Console, and the third party applications, in a VMware virtualization environment.

For details refer to the respective agent configuration guide.

Consider the following before you proceed:

- You configure application monitoring on a virtual machine virtual machine using the Symantec ApplicationHA Configuration Wizard. The wizard is launched when you click **Configure Application Monitoring** on the ApplicationHA tab.

- 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.
  To configure another application using the wizard, you must first unconfigure the existing application monitoring configuration.

  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.

- After you have configured monitoring for an application using the wizard, you can configure monitoring for additional applications from the command line. Use the Veritas Cluster Server commands to configure additional applications. Refer to the following technote for additional information:
  http://www.symantec.com/docs/TECH159846
- If you clone a virtual machine on which you have configured application monitoring, you must reconfigure application monitoring on the cloned virtual machine.
- If a configured application fails, Symantec ApplicationHA attempts to start the component on the virtual 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 on a virtual machine:

- 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 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 Symantec ApplicationHA (Console and guest components) in your VMware environment.
  Refer to the *Symantec ApplicationHA Installation and Upgrade Guide* for instructions.
- Verify that the logged-on user has administrative privileges on the virtual machine where you wish to configure application monitoring.
- 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.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.
  Refer to the for a list of ports and services used.

About configuring application monitoring for the ApplicationHA Console

Consider the following before you configure application monitoring for ApplicationHA Console:

- Symantec ApplicationHA considers the Console as a custom application. It can monitor ApplicationHA Console services running on the virtual machine. If any component fails, ApplicationHA attempts to restart 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 its status. 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 perform the stop function 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.
- Verify that the ApplicationHA Console and the ApplicationHA guest components are installed on the same virtual machine. This is required for configuring application monitoring for the ApplicationHA Console.

Configuring application monitoring for ApplicationHA Console

Perform the following steps to configure application monitoring for ApplicationHA Console on a virtual machine.

Note: After you have configured application monitoring for ApplicationHA Console, you can administer application monitoring by using either the ApplicationHA tab or the ApplicationHA dashboard.

See "Administering application monitoring using the ApplicationHA tab" on page 49.

See "Administering application monitoring using ApplicationHA dashboard" on page 58.

To configure application monitoring for ApplicationHA Console

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 have installed ApplicationHA Console, and then click the **ApplicationHA** tab on the right pane.
3. On the ApplicationHA tab, provide the administrator account's credentials for the virtual machine. Then, ApplicationHA Console sets up a permanent account for performing various operations on the virtual machine.
4. Click **Configure Application Monitoring** to launch the ApplicationHA Configuration Wizard.
5. On the Welcome panel, review the information, and then click **Next**.

6 On the Application Selection panel, select **ApplicationHA Console** to configure application monitoring for ApplicationHA Console services on the virtual machine, and then click **Next**.

7 On the ApplicationHA Console Services panel, the wizard lists the ApplicationHA Console services that will be configured. Click **Configure** to configure these services for application monitoring.

8 On the ApplicationHA Configuration panel, the wizard initializes Symantec ApplicationHA, configures ApplicationHA Console services for application monitoring, and enables application heartbeat. When these tasks are completed, click **Next**.

9 On the Finish panel, click **Finish** to exit the wizard.

This completes the application monitoring configuration for ApplicationHA Console. On the ApplicationHA tab, the Description box displays the list of services configured for application monitoring. The status of the application appears as configured and running on the virtual machine.

Chapter 5

Administering application monitoring

This chapter includes the following topics:

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)
- VMware Fault Tolerance

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.

Administering application monitoring using the ApplicationHA tab

Note: You can administer application monitoring in two ways. One, using the ApplicationHA tab as described below and two, using the Symantec ApplicationHA Dashboard. Using the ApplicationHA dashboard, you can administer application monitoring for multiple applications on multiple virtual machines in a data center. For more information about the latter,

See "Administering application monitoring using ApplicationHA dashboard" on page 58.

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

Use the ApplicationHA tab 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 ApplicationHA tab, 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://<*VMNameorIP*>:5634/vcs/admin/application_health.html?priv=ADMIN
where *<VMNameorIP>* is the virtual host name or the IP address.

To configure or unconfigure application monitoring

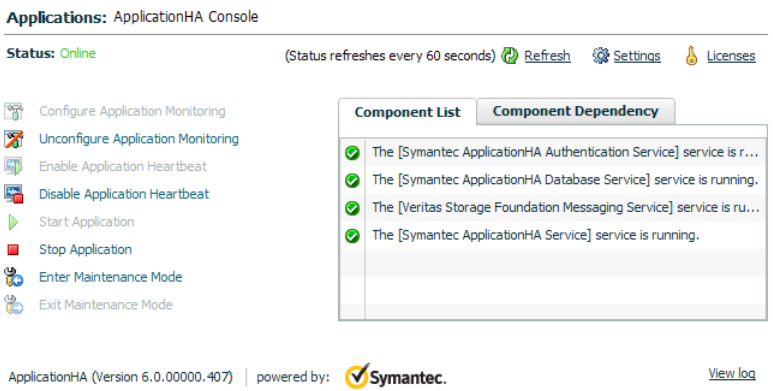
Use the ApplicationHA tab to configure or delete an application monitoring configuration from the virtual machine. This may be required in case you wish to re-create the configuration or configure another application using the wizard.

You can use the following buttons:

- 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 application, you have to configure them again.

To view the status of configured applications

Under the Component List tab, the Description box in the ApplicationHA displays the status of the configured application and the associated services.



For example, if you have configured monitoring for Application Console, the Description displays the following information:

```
The [service] service is running.
```

Where, *service* is the name of the service configured on the virtual machine.

The Description box also 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 configured components. The status is refreshed every 60 seconds by default.

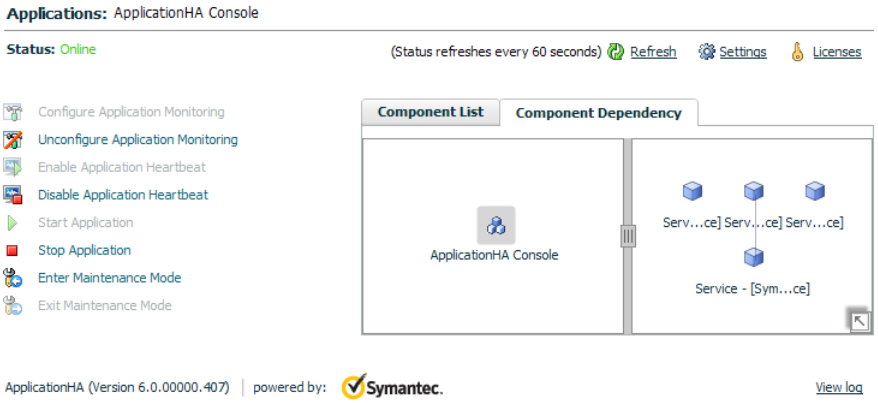
To view component dependency

ApplicationHA monitors a configured application for high availability by monitoring the status of its components. Inter-related components form a component group. The status of the application depends on the component groups.

The Component Dependency tab of the VMware vSphere client GUI illustrates this dependency between the application and its components.

To access the Component Dependency tab perform the following step:

- In the ApplicationHA tab of the vSphere client GUI, click **Component Dependency**.
  A component dependency graph appears. The graph indicates which component depends on which other component to be up and running.



The above figure illustrates the component dependency for the Internet Information Server (IIS) application.

The left pane indicates the component groups, while the right pane indicates the components of the selected component group. A vertical line joining two components indicates that for the component at the higher level to be running, the component at the lower level must be running.

The track pad, at the left-bottom corner helps you navigate through complex component dependency graphs.

The Component Dependency graph also uses various icons to indicate component groups and components as well as their status. If you roll the mouse over a component, a tooltip highlights the name and the state of the component.

For example, in the above figure, the Internet Information Services component group is selected in the left pane and the components, IIS site and Storage mount point, appear in the right pane. For IIS to be up, the Internet Information Services component group must be online. For the Internet Information Services component group to be online, the Storage mount point component must come up first, followed by the IIS site resource.

To start or stop applications

Use the following options on the ApplicationHA tab to control the status of the configured application and the associated components:

- 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 hierarchy.
- 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 reset or restart individual virtual machines that have lost their ability to heartbeat. You can select VM and Application Monitoring if you also want to enable application monitoring.

The ApplicationHA tab 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 Heartbeat** 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 Heartbeat** to disable the heartbeat communication between the configured applications running on the virtual machine and VMware HA.
  Disabling the application heartbeat does not instruct VMware HA to restart the virtual machine. 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 tab 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 tab 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 tab 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. The view also provides a set of options that you can use to configure ApplicationHA to restart 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:

- App.StartStopTimeout

  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 and 600. The default is 30 seconds.

- App.RestartAttempts

  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 and 6. The default is 1.

- App.ShutdownGraceTime
  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 and 600. The default is 300 seconds.

- VM.GracefulRebootPolicy
  Use this option to enable or disable ApplicationHA-initiated virtual machine restart policy. This option defines whether or not ApplicationHA restarts the virtual machine in response to application and component failures. When a configured application or component fails, ApplicationHA attempts to restart the failed components. If the component fails to start, ApplicationHA then takes the next corrective action.
  If this policy is disabled, and an application or component fails, then ApplicationHA stops sending the heartbeat to VMware HA. As a result VMware HA can then restart the virtual machine.
  If this policy is enabled, ApplicationHA itself invokes a native operating system command to restart the virtual machine.
  VM.GracefulRebootPolicy value can be Enabled (1) or Disabled (0). The default value is Disabled.

- VM.GracefulRebootAttempts

This option defines the number of times ApplicationHA attempts to restart the virtual machine gracefully if the configured application or component becomes unresponsive. The number of restart attempts is time bound and is defined by the option VM.GracefulRebootTimeSpan. The restart attempts count is reset after the reboot time span elapses.

For example, if the reboot attempts value is 4, the time span value is 1 hour, and ApplicationHA has restarted the virtual machine once, then the restart attempt count is 3 (initial set value of 4 minus one reboot) for the remaining period of the 1-hour interval. The restart attempts count is reset to 4 at the beginning of the next 60-minute span.

If the restart attempts are exhausted and the application or component fails within the reboot time span again, ApplicationHA stops the application heartbeat and communicates the fault to VMware HA. Depending on the configuration, VMware HA may then restart the virtual machine.

VM.GracefulRebootAttempts value can vary between 1 and 10. The default value is 1.

- VM.GracefulRebootTimeSpan

  This option defines the time interval, in hours, during which ApplicationHA can gracefully restart the virtual machine for the number of times defined by the option VM.GracefulRebootAttempts.

  VM.GracefulRebootTimeSpan value can vary between 1 and 24. The default value is 1 hour.

Note: These attribute values are not affected due to a hard restart by VMware HA. The configuration remains in effect even after VMware HA reboots the virtual machine.

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 vmrestoretimeout

vmrestoretimeout defines the time interval, in minutes, for which the heartbeat agent must wait for VMware HA to reset the virtual machine. If the VMware HA does not reset the virtual machine within this time, heartbeat agent triggers a request for backup restore.

Note: In case of VMware ESX Server version 4.0 the request for virtual machine restore is triggered after the graceful reboot attempt.

The default value for vmrestoretimeout is 5 minutes.

You can administer the vmrestoretimeout value through command line. 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.

Note: These attribute values are not affected due to a hard restart by VMware HA. The configuration remains in effect even after VMware HA reboots the virtual machine.

To modify the vmrestoretimeout configuration settings

1. On the virtual machine, open the command prompt.
2. Set the cluster configuration mode to read/write by typing the following command.

   ```
   haconf -makerw
   ```

3. Modify the vmrestoretimeout value.

   ```
   hares -modify VCSAppMonHBRes vmrestoretimeout time in minutes
   ```

   Note: The vmrestoretimeout value must always be greater than the VMware HA configuration settings. Failing this, the request for virtual machine backup will be triggered before the VMware HA action.

4. Save these changes. Then set the cluster configuration mode to read-only by typing the following command.

   ```
   haconf -dump -makero
   ```

Administering application monitoring using ApplicationHA dashboard

The ApplicationHA dashboard is the consolidated graphic user interface of ApplicationHA that lets you administer configured applications on virtual machines in a VMware vCenter-administered datacenter.

The dashboard is fully integrated with the VMware vSphere Client GUI. The dashboard appears in the ApplicationHA tab of the VMware vSphere Client GUI. To view the dashboard, in the inventory view of the vSphere Client, you must click a datacenter or a VMware cluster, and then click the ApplicationHA tab in the right pane.

On the dashboard, you can view the aggregate health of the configured applications across a datacenter. You can also drill down to a VMware cluster and view the aggregate health of configured applications in that cluster. You can further drill down to an individual application, on an individual virtual machine, and view or change the state of the application.

You can start or stop the application. You can enable or disable the heartbeat mechanism for the application. You can also take the application offline for maintenance (without raising any high availability alert), or bring back the application online after maintenance.

For more information on the components of the dashboard:

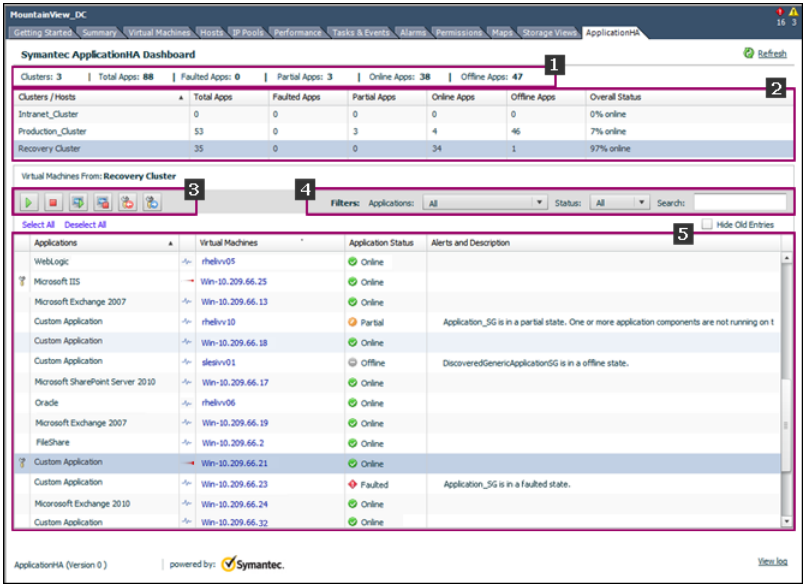
See "Understanding the dashboard work area" on page 58.

Understanding the dashboard work area

The ApplicationHA dashboard displays the aggregate application health status information for a datacenter or a VMware cluster.

Depending on whether you click a datacenter or a VMware cluster in the inventory view of the VMware vSphere Client, the dashboard displays the aggregate application status information. The dashboard uses color code and tool tips to indicate the status of an application, apart from the detailed application table described below.

The following figure illustrates the dashboard work area:



In the above figure, the labels stand for the following elements of the dashboard

1	Aggregate status bar	**2**	Cluster table	**3**	Taskbar
4	Filters menu	**5**	Application table		

Aggregate status bar

For a datacenter, the aggregate (health) status bar displays the total number of VMware clusters and the total number of configured applications running in the datacenter.

The aggregate status bar also lists the following details to indicate the overall health of the configured applications in the datacenter:

- Number of faulted applications
- Number of applications in partial state
- Number of online applications
- Number of offline applications

For a VMware cluster, the aggregate (health) status bar displays the total number of configured applications in the VMware cluster.

The aggregate status bar also lists the following details to indicate the overall health of the configured applications in the VMware cluster:

- Number of faulted application instances
- Number of application instances in partial state
- Number of online application instances
- Number of offline application instances

Cluster table

The ApplicationHA dashboard displays this table only if you click a datacenter in the inventory view of the vSphere Client, and then click the ApplicationHA tab. The cluster table lists the following columns for each VMware cluster (or independent ESX server) in the datacenter :

- Total number of virtual machines in the selected cluster
- Number of virtual machines with faulted applications
- Number of virtual machines with application alerts
- Number of virtual machines with healthy application status
- Overall status of applications in the VMware cluster (percentage of healthy applications)

Note: If an ESX server is not part of a cluster, then the ESX server appears as a cluster in this table. If you click the ESX server, then the dashboard displays the applications running on the various virtual machines on the ESX server. You cannot view the applications on such virtual machines, if you click a cluster in the inventory view and then click ApplicationHA tab.

Taskbar

The taskbar displays icons for various administrative tasks. A tool tip highlights the task that each icon represents.

The following tasks are presently supported:

- Start Application: Starts a configured application
- Stop Application: Stops a configured application
- Enable Application Heartbeat: Enables 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.
- Disable Application Heartbeat: Disables heartbeat communication between the configured applications running on the virtual machine and VMware HA.

- Enter Maintenance Mode: Suspends application monitoring for the configured application. During the time the monitoring is suspended, ApplicationHA does not monitor the state of the application and its dependent components.
- Exit Maintenance Mode: Resumes application monitoring for a configured application.

Filters menu

The filters menu lets you dynamically filter the applications that are displayed in the Applications table. You can filter the applications by the following parameters:

- Application name
- Application status
- Search (key string)

Application table

If you click a VMware cluster in the cluster table or in the inventory view of the VMware vSphere Client, then the list of virtual machines in the selected cluster appears in the application table. In the datacenter view of the dashboard, if you click an ESX server that is not part of a VMware cluster, then the list of virtual machines that are configured on that ESX server appears.

The following table lists each column in the application table and its description:

Column	Description
Maintenance mode	Indicates if the application is in maintenance mode. The maintenance mode icon appears. If you roll the mouse over a row, an appropriate tool tip appears. This column has no heading.
Application	Indicates the application name.
Heartbeat	Indicates if ApplicationHA is currently using the heartbeat mechanism to send application status updates to VMware HA. If you roll the mouse over the row, an appropriate tool tip appears. ApplicationHA stops using the mechanism only when an application is in maintenance mode. This column has no heading.

Column	Description
Application Status	Indicates one of the following states of an application: ■ Online ■ Offline ■ Faulted ■ Partial **Note:** After you perform an administrative task such as start or stop application, or enter maintenance mode, the dashboard requires a few seconds to update the status of the configured application.
Virtual machine	Indicates the virtual machine on which the application is running.
Alerts and description	Indicates the reasons why an application is not running or is in a partial state.

Understanding how the dashboard works

Symantec ApplicationHA leverages its awareness of the application health to enable the datacenter administrator to quickly intervene by using the dashboard.

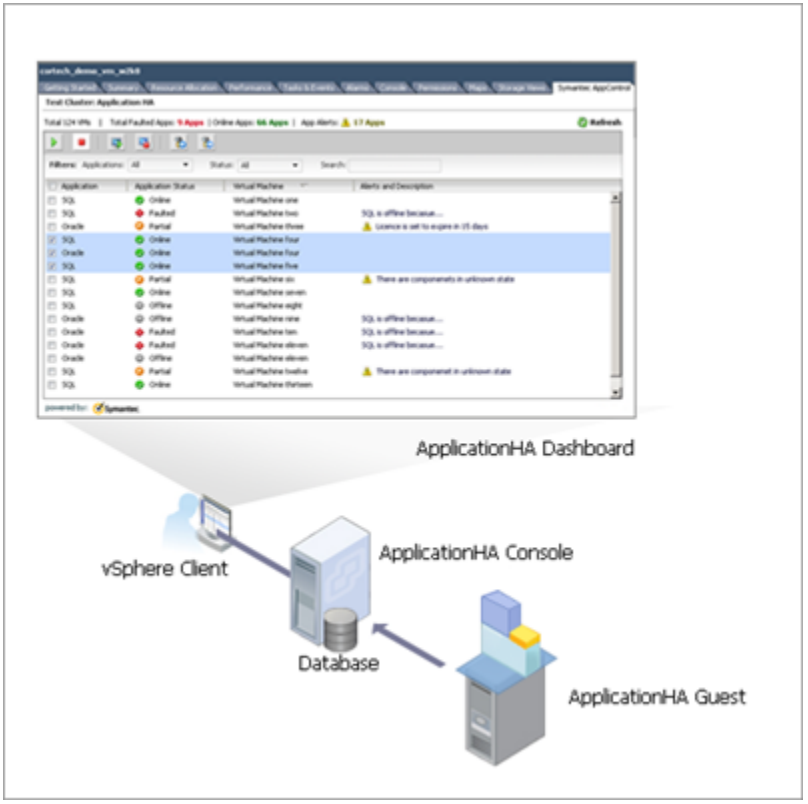
Application control with Symantec ApplicationHA is based on the exchange of heartbeat signals between the virtual machines and the ApplicationHA console.

Application-specific agents of ApplicationHA persistently monitor various components of a configured application on each virtual machine in a VMware cluster. The agents relay the status of the application components to a database that resides at the base of the ApplicationHA console. Dashboard components further process this data to determine the state of the application: Online, Offline, Partial, or Faulted.

ApplicationHA components further relay the application health status to the dashboard over the vSphere Client.

Note: To display the latest status of all configured applications in the selected datacenter or cluster, you must click **Refresh**.

The following figure illustrates the functioning of the dashboard:



Accessing the dashboard

You may need to access the ApplicationHA dashboard if you want to:

- Search for an application across the datacenter or VMware cluster and perform an administrative action
- Perform an administrative action on an application across a datacenter or a VMware cluster
- Suspend monitoring of an application for maintenance purposes, across a VMware cluster or a datacenter

Prerequisites for accessing the dashboard

Before you access the ApplicationHA dashboard to administer an application, ensure:

- The application that you want to administer is configured for application monitoring with Symantec ApplicationHA
- ApplicationHA console is able to communicate with ApplicationHA guest components on designated port (port 5634).

How to access the dashboard

When you install ApplicationHA, the product installation script or wizard automatically installs the required dashboard components. As a result, the ApplicationHA dashboard appears in the **ApplicationHA** tab of the vSphere Client.

You must, however, ensure that Symantec ApplicationHA is successfully installed and that you have adequate user privileges to access the dashboard.

To access dashboard

Perform the following step:

- In the inventory view (left pane) of the vSphere Client, click a datacenter or a VMware cluster. In the right pane, the Symantec ApplicationHA dashboard appears in the ApplicationHA tab.

Who can access the dashboard

To access ApplicationHA, the VMware vCenter administrator must assign one the following roles to you:

- Guest : Only view application status
- Operator: View and control application
- Admin: Configure application monitoring, besides viewing and controlling applications.

For more information on the roles:

See "Symantec ApplicationHA user privileges" on page 20.

Note: The roles and their privileges are subject to Discretionary access control (DAC) policies.

For more information on what is discretionary access control:

See "What is discretionary access control " on page 65.

For more information on configuring access control:

See "Configuring Symantec ApplicationHA access control" on page 26.

What is discretionary access control

Discretionary access control (DAC) is a feature that lets the vCenter administrator restrict access for a ApplicationHA user to only certain VMware clusters or virtual machines in a datacenter.

For example, as an ApplicationHA administrator, you may be able to monitor and control applications on virtual machines only in specified VMware clusters. ApplicationHA dashboard does not display the other VMware clusters to you.

This feature helps prevent unwanted or accidental administrative intervention in some VMware clusters. It also restricts visibility for guest users and operators to only the required VMware clusters.

Monitoring applications across a datacenter

If you click a datacenter in the inventory view of the VMware vSphere Client, and then click the ApplicationHA tab, then the ApplicationHA dashboard displays various VMware clusters, virtual machines and applications running in the selected datacenter. The dashboard also displays application health and application monitoring information.

You can use filters to drill down from all applications running across the datacenter and view a single application and its various instances in the datacenter.

Monitoring applications across a cluster

If you click a VMware cluster in the inventory view of the VMware vSphere Client, and then click the ApplicationHA tab, the ApplicationHA dashboard displays consolidated information on the virtual machines and applications running in the VMware cluster. The dashboard also displays the application health and application monitoring information.

You can use filters to drill down from all applications running in the VMware cluster, to view a single application and its various instances in the VMware cluster.

Searching for application instances by using filters

The ApplicationHA dashboard helps you search for all instances of a particular application in selected datacenter or a VMware cluster. You can use three types of filters to search for the application that you want to monitor.

You can simultaneously search for an application by using one or more filters.

The following table lists each field in the filter menu and its description:

Field	Description
Application	Lets you specify the name of the application that you want to filter in the application table. A drop-down list displays all configured and heartbeat enabled applications in the datacenter or VMware cluster. Click to select the name of the application that you want to filter.
Status	Lets you specify the status of the application by which you want to filter the application table. A drop-down list displays following status values: Online, Offline, Faulted Partial, Unknown. Click the status by which you want to filter applications.
Search	Lets you search for an application by using a string or pattern of characters. Enter the pattern by which you want to filter applications. The dashboard dynamically filters the list.

Selecting multiple instances of an application for administering

You can select one or more instances of an application for administering by using the dashboard

To select one application instance, click inside the row of that application instance.

To select various instances, keep the **Control** key pressed and then click inside the row of each instance.

To select consecutive instances in the application table, keep the **Shift** key pressed, click inside the row of the first instance, and then click inside the row of the last instance.

To select all instances in the application table, click **Select All**.

Starting an application by using the dashboard

To start an application on one or more virtual machines, perform the following steps in the application table of the ApplicationHA dashboard.

To start an application

1. Filter the application that you want to start.

   See "Searching for application instances by using filters" on page 65.

2. In the applications table, select the virtual machines on which you want to start the application.
3. To start the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

Stopping an application by using the dashboard

To stop an application on one or more virtual machines, perform the following steps in the application table of the ApplicationHA dashboard.

To stop an application

1. Filter the application that you want to stop.

   See "Searching for application instances by using filters" on page 65.

2. In the applications table, select the virtual machines on which you want to stop the application.

3. To stop the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

Enabling application heartbeat by using the dashboard

To enable application heartbeat for an application on one or more virtual machines, perform the following steps in the application table of the ApplicationHA dashboard.

For more information on

To enable application heartbeat

1. Filter the application for which you want to enable heartbeat.

   See "Searching for application instances by using filters" on page 65.

2. In the applications table, select the virtual machines on which you want to start the application.

3. To enable heartbeat for the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

Disabling application heartbeat by using the dashboard

To disable application heartbeat for an application on one or more virtual machines, perform the following steps in the application table of the ApplicationHA dashboard.

To disable application heartbeat

1. Filter the application for which you want to disable heartbeat.

   See "Searching for application instances by using filters" on page 65.

2. In the applications table, select the virtual machines on which you want to disable heartbeat.
3. To disable heartbeat for an application, in the taskbar, click the appropriate icon for stopping application monitoring (use the tool tip to recognize the appropriate icon).

Entering an application into maintenance mode

You may need to take an application intentionally offline for maintenance purposes.

To take an application on one or more virtual machines into maintenance mode, perform the following steps in the application table of the ApplicationHA dashboard.

To enter maintenance mode

1. Filter the application that you want to gracefully take offline for maintenance.

   See "Searching for application instances by using filters" on page 65.

   All the instances of the application that you want to gracefully take offline for maintenance appear.

2. In the applications table, select the appropriate instances to enter maintenance mode.
3. To gracefully take an application offline for maintenance, in the taskbar, click the appropriate icon for entering maintenance mode (use the tool tip to recognize the appropriate icon).

Bringing an application out of maintenance mode

To bring an application out of maintenance mode on one or more virtual machines, perform the following steps in the application table of the ApplicationHA dashboard.

To exit maintenance mode

1 Filter the application that you want to bring out of maintenance mode.

See "Searching for application instances by using filters" on page 65.

All the instances of the application that you want to bring out of maintenance mode appear.

2 In the applications table, select the appropriate instances to bring out of maintenance mode.

3 To bring the application out of maintenance mode, in the taskbar, click the appropriate icon for exiting maintenance mode (use the tool tip to recognize the appropriate icon).

Troubleshooting dashboard issues

This section lists the troubleshooting scenarios that you may encounter while working with the ApplicationHA dashboard.

All virtual machines disappear from the dashboard

No virtual machines are visible on the dashboard.(2332024)

Workaround

1. If all virtual machines disappear from the ApplicationHA dashboard, then check on the ApplicationHA console if the database service is up and running. If not, bring up the database.
2. Check if the application is faulted and the virtual machine is booting. The virtual machines may disappear from the dashboard while the restart is in progress.

Dashboard displays old timestamp

In the application table, the dashboard displays and old timestamp for an application. (2332263)

Workaround

1. Execute the following command:

```
<VRTSsfmh install dir>\bin\perl.exe
<VCS_HOME>\portal\admin\synchronize_guest_config.pl
```

2. Also ensure that the `notify.sink.exe` file is present at the following location:

```
%vcs_home%\cluster server\bin
```

Application status error related to old timestamp

If the ApplicationHA dashboard displays an old timestamp in the description column for an application, then the status of that application may not be the latest. The dashboard displays the old timestamp in the description column for an application if the database on the ApplicationHA console is not updated. (2352091)

Workaround

Verify if the virtual machine is up and running. Also verify if the application is correctly configured. If the problem persists, then first unconfigure and then reconfigure application monitoring on that virtual machine.

Dashboard displays error

If the network connections are slow, then the ApplicationHA dashboard displays the following popup:

```
Unable to retrieve application status.
Please verify the following:
- The ApplicationHA Console host is powered on and accessible.
- The ApplicationHA Console service (Symantec ApplicationHA service)
  is running on the Console host
- Ports 5634, 443, and 14152 are not blocked by a firewall.
- Network connection problems.
```

(2332539)

Workaround

Ensure that none of the problems exist as per the popup.

ApplicationHA console reinstall error

If you reinstall ApplicationHA console or repair an existing ApplicationHA console installation and then access the ApplicationHA dashboard, then the dashboard may display the following error:

```
Unable to retrieve the application status.
Please verify the following:
-The ApplicationHA Console host is powered on and accessible.
-The ApplicationHA Console service (Symantec ApplicationHA Service)
 is running on the Console host.
-Ports 5634, 443, and 14152 are not blocked by a firewall.
-Network connection problems.
```

(2332019 and 2349592)

Workaround

Close the vSphere Client and reopen it.

VM networking issue

If a virtual machine is not properly configured into the local network, the dashboard does not display the configured application/s.

This behavior is observed if ApplicationHA is unable to determine the MAC ID or NIC of a virtual machine from a vCenter MOB. When you try to view the configured application/s on that virtual machine over the dashboard, one of the following messages appear in the ApplicationHA logs:

```
"No MAC address is present for the VM: vmName"
"Please check VMware tools are updated and running on the VM."
```

or

```
"No NIC information is present for the VM: vmName"
```

You can view the related entries in the ApplicationHA logs located here:

```
ProgramData/log/ApplicationHA.log
```

(2357368)

Workaround

Ensure that the VM is properly configured on the local network. That is, the MAC ID and NIC of the VM are available in vCenter MOB.

Application status updates takes a few seconds, some virtual machines momentarily disappear

If you perform certain administrative actions by using the ApplicationHA dashboard (or by using the ApplicationHA tab of the vSphere Client), then the dashboard may require a few seconds to update the updated status.

For example, if you start or stop an application using the dashboard, then the new status of the application takes a few seconds to appear on the dashboard.

If you exit maintenance mode for an application on a particular virtual machine, then the application and the virtual machine momentarily disappear from the application table of the dashboard. They reappear after a few seconds and the dashboard indicates that the application is not in the maintenance mode. (2348253 and 2366680)

Access privileges propagation issue

If you propagate access privileges for a user across a datacenter or cluster, then the user is unable to view the applications running inside the datacenter or cluster over the dashboard. (2377656)

Workaround

You must assign access privileges to the user for each required virtual machine via the VMware vSphere Client.

Virtual machine count may fluctuate on dashboard

If you refresh the dashboard while configuring a large number of virtual machines for application monitoring with ApplicationHA, then the count of configured applications may fluctuate on the dashboard. This behavior occurs because a large amount of information is simultaneously updated. (2378577)

About ApplicationHA-initiated virtual machine restarts

When you configure application monitoring, ApplicationHA uses heartbeat to communicate the application status to VMware HA. If the application or its component fails, ApplicationHA attempts to restart it. If the application does not start, ApplicationHA stops sending the heartbeat. Depending on the configuration, VMware HA then restarts the virtual machine instantaneously.

A hard restart has various implications and may not be the desired solution at all times. It may prove to be counter productive in several cases, including the following:

- The virtual machine itself is running fine but the application is unable to get the required resources
- The other applications and tools running on the machine may either hang or take longer time to recover or restart after an abrupt shut down
- A hard restart can be potentially disruptive if there are multiple critical applications running on the virtual machine

ApplicationHA provides another layer of application control wherein you can configure ApplicationHA itself to restart the virtual machine using native operating system commands. An operating system driven restart is graceful and allows for a more orderly shut down of applications and tools running on the machine and can help reduce potential disruption to critical applications.

ApplicationHA provides attributes that you can use to configure ApplicationHA to restart the virtual machine.

See "Administering application monitoring settings" on page 54.

Does ApplicationHA-initiated reboot affect VMware HA?

ApplicationHA-initiated reboot works independently of VMware HA functionality. It is not intended to replace VMware HA. It is useful in cases where there is a need to first bring down other healthy applications and dependent components before actually restarting the virtual machine and also in VMware virtualization environments where VMware HA is not available.

ApplicationHA-initiated reboot complements VMware HA by offering an additional layer of control that helps in building customized application management and recovery plans in virtualization environments. ApplicationHA-initiated reboot can co-exist with VMware HA. You can configure both ApplicationHA-initiated reboot and VMware HA as part of your recovery plan. ApplicationHA-initiated reboot can act as the first line of action against application failures. If a graceful restart does not resolve the application failures, then depending on the reboot configuration settings, ApplicationHA stops the application heartbeat and VMware HA then takes control of the virtual machine.

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.

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.

You perform the following steps on the ApplicationHA Console host.

To back up ApplicationHA Console files and registry

1. Stop the following ApplicationHA services.
   - Symantec ApplicationHA Authentication Service
   - Symantec ApplicationHA Database Service
   - Symantec ApplicationHA Service
2. 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`.
3. 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`
4. 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.
5. Back up the following directories on the ApplicationHA Console host:

   ```
   %AllUsersProfile%\Symantec\ApplicationHA\sec
   %AllUsersProfile%\Symantec\ApplicationHA\conf
   %AllUsersProfile%\Symantec\ApplicationHA\BESec\certstore
   %AllUsersProfile%\Symantec\ApplicationHA\BESec\keystore
   ```

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

   Store the backup files at a location from where you can retrieve 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.

Appendix A

Troubleshooting Symantec ApplicationHA configuration

This appendix includes the following topics:

Symantec ApplicationHA logging

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

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

ApplicationHA 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.

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.

ApplicationHA view logging

The ApplicationHA view generates log files that are appended by letters. The log files are segregated based on operations and configuration settings, as follows:

- 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.

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.

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.

The Symantec ApplicationHA plugin available in the vCenter Server Plug-in Manager is "Disabled"

This issue typically occurs if the vCenter Server fails to access the ApplicationHA Console IP, that was used while configuring single sign-on between the ApplicationHA Console and the vCenter Server. Since the plugin is disabled the ApplicationHA tab and dashboard are not available.

Resolution:

Perform the following steps to resolve the issue

1. Using the PluginMgmt.bat utility unregister the plugin and then register it again.

   While registering the plugin again, specify a Console server IP address that is accessible over the network from the vCenter Server.

2. On the Console Server, run the following command and then restart the Symantec ApplicationHA Service.

   ```
   "c:\Program Files\Veritas\VRTSsfmh\bin\perl.exe" "c:\Program
   Files\Veritas\ApplicationHA\bin\create_cert.pl"
   AppHAConsoleIP=ConsoleIP
   ```

   The *ConsoleIP* is the IP address you specified while registering the plugin again.

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.

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 VMware Web Service is running on the vCenter Server.
- Verify that the VMware Tools Service is running on the guest virtual machine.
- Verify that the Veritas Storage Foundation Messaging Service (xprtld process) 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`

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 VMware Tools Service is running on the guest virtual machine.
- Verify that the Veritas Storage Foundation Messaging Service is running on the guest virtual machines and the ApplicationHA Console.
  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 73.

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.
```

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.

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

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 73.
   - If you have lost the existing ApplicationHA Console host, perform the operation manually.
     See "Symantec ApplicationHA plugin registration error" on page 80.
2. Install ApplicationHA Console on the new server.

   For details refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.
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 23.
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 26.

Application monitoring recovery step fails with an Error: 5

After a site recovery, the VMware recovery status report may display the following error for the application monitoring recovery step.

```
Error: User designed callout Command : has failed to execute ....
Error:5
```

The application monitoring recovery step displays this error if the monitored application exists in any of the following states after the site recovery.

- Offline
- Partially online
- Faulted

Workaround:

For details, verify the "AppStatusSRM_A.log" file. The file is located at the following location on the SRM server.

For Windows Server 2003:

```
C:\Documents and Settings\All Users\Application Data\
Symantec\ApplicationHA\SRM\Logs
```

For Windows Server 2008 and 2008 R2:

```
C:\Program Data\All Users\Application
Data\Symantec\ApplicationHA\SRM\Logs
```

Application monitoring recovery step fails with a "non-zero value: 5" error

After a test recovery, the VMware test recovery status report may display the following error for the application monitoring recovery step.

```
Error: User designed callout
'"C:\WINDOWS\system32\cmd.exe" /C
"C:\Program Files\Veritas\ApplicationHA\SRM\
bin\getAppStatus.bat" <VirtualMachine_IP>' has returned
a non-zero value: 5.
```

The AppStatusSRM_A.log file located on the SRM server displays the following details:

```
[forbidden & Application status could not be determined because
authorization failed]
```

This error typically occurs if the ApplicationHA credentials on the SRM Server are corrupted.

Workaround:

Perform the following steps:

1. On the virtual machine, run "services.msc" and stop the "Veritas Storage Foundation Messaging Service" service.
2. Navigate to the following path.

   C:\Documents and Settings\All Users\Application Data\Symantec\VRTSsfmh\sec\
3. Delete the "systemprofile" folder.
4. Start the "Veritas Storage Foundation Messaging Service" service.
5. Re-configure the single sign-on between the protected site virtual machines and the protected site ApplicationHA Console.
6. Re-configure the single sign-on between the protected site virtual machines and the recovery site ApplicationHA Console.
7. Run the test recovery plan.

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 73.
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 26.

VMware HA restarts a virtual machine even if VMware HA is disabled at the cluster level

Disabling VMware HA ensures that VMware HA takes no action in case of a loss of a heartbeat from the virtual machines. In some cases, VMware HA restarts the virtual machine even if VMware HA is disabled at the VMware cluster level.

Workaround:

This may occur if the VMware HA settings are set incorrectly. To completely disable VMware HA, you must disable two settings, VM Monitoring and Turn On VMware HA, from the vSphere client.

See "Disabling VMware HA at a cluster level" on page 26.

Index