Symantec™ ApplicationHA Agent for FileShare Configuration Guide

Windows Server 2003, Windows Server 2008 and 2008 R2

6.0

March 2013



Symantec™ ApplicationHA Agent for FileShare Configuration Guide

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

Product version: 6.0

Document version: 6.0 Rev 0

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

About Symantec Connect

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

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

Contents

Technical Support 4

Chapter 1 Introducing the Symantec ApplicationHA agent for FileShare 9

About the Symantec ApplicationHA agents 9
About the Symantec ApplicationHA agent for FileShare 10
Dependencies 11
Agent functions 11
State definitions 11
About ForceControl function 11
Attributes 12
How Symantec ApplicationHA agent monitors file shares 17

Chapter 2 Configuring application monitoring with Symantec ApplicationHA 19

About configuring application monitoring with Symantec ApplicationHA 19
Before configuring application monitoring 20
Configuring application monitoring for FileShare 21
Administering application monitoring using the ApplicationHA tab 24
To configure or unconfigure application monitoring 25
To view the status of configured applications 26
To start or stop applications 27
To enable or disable application heartbeat 27
To suspend or resume application monitoring 28

Chapter 1

Introducing the Symantec ApplicationHA agent for FileShare

This chapter includes the following topics:

- About the Symantec ApplicationHA agents
- About the Symantec ApplicationHA agent for FileShare
- How Symantec ApplicationHA agent monitors file shares

About the Symantec ApplicationHA agents

Agents are the processes that manage applications and resources of the predefined resource types which are configured for applications and components on a system. The agents are installed when you install Symantec ApplicationHA. These agents start, stop, and monitor the corresponding resources that are configured for the applications and report state changes.

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.
  For more details about the infrastructure agents, refer to the *Symantec™ ApplicationHA Generic Agents Guide*.
- Application agents

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

An agent pack is released on a 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

The following sections provide details about the agent for FileShare.

For more details about other application agents, refer to the application-specific configuration guide.

About the Symantec ApplicationHA agent for FileShare

Fileshare agent makes file shares highly available. The FileShare agent ensures high availability for multiple shared folders including their subfolders.

The FileShare agent enables systems to share multiple folders including their subfolders, making the shared folders highly available.

Using the FileShare agent, you can also do the following:

- Create hidden shares for a specific share or subfolders
- Dynamically share subfolders created after the resource is brought online

The FileShare agent enables sharing folders shared outside ApplicationHA. However, you cannot add special shares (shares created by the operating system for administrative and system use) to the ApplicationHA configuration. For example, you cannot add the shares ADMIN$, print$, IPC$, and DriveLetter$ to the ApplicationHA configuration.

You can configure application monitoring for file shares on a virtual machine using the Symantec ApplicationHA Configuration Wizard. For information on configuring monitoring for a file share, see

See “Configuring application monitoring for FileShare” on page 21.

Dependencies

For a FileShare service group, the FileShare resource depends on the MountMonitor resource.

Agent functions

Online	Shares the specified folders with designated permissions.
Offline	Removes the shares for the specified folders.
Monitor	Verifies that the specified folders are shared with the designated permissions.

State definitions

ONLINE	Indicates that the specified folder is shared.
OFFLINE	Indicates that the specified folder is not shared.
UNKNOWN	Indicates the agent cannot determine the status of the resource.

Note: Sharing a folder with a large number of subfolders and enabling the ShareSubdirectories attribute can cause high CPU and memory utilization.

About ForceControl function

ForceControl is a FileShare agent function that lets you reset the file share properties as per what is defined in the service group configuration. The agent overwrites all modifications made to the file share properties, either externally or from within ApplicationHA, and sets the properties as per what you had defined while configuring the file shares in ApplicationHA. This function overrides the FileShare agent's AutoControl attribute settings.

You can run the ForceControl function from the command line.

To run the ForceControl function on a FileShare resource, type the following command:

```
hares -action <fileshare_resource_name> ForceControl -sys
<system_name>
```

Here, <*fileshare_resource_name*> is the name of the file share resource for which you want to reset the properties and <*system_name*> is the name of the computer.

For example, to run the ForceControl function on a FileShare resource *A_fileshare* that is currently online on a cluster system *System1*, type the following:

```
hares -action A_fileshare ForceControl -sys System1
```

The changes take effect on the next agent monitor function.

Attributes

Table 1-1 lists the required attributes of the FileShare agent.

Table 1-1 FileShare agent required attributes

Required Attributes	Description
MountResName	The name of the MountMonitor resource on which the FileShare resource depends. Type and dimension: string-scalar
ShareName	The name by which the share is known to clients. **Note:** This attribute can take localized values. Type and dimension: string-scalar
PathName	The path of the folder to be shared. To share a drive, specify the PathName as \. For example, to share drive X:, the PathName is \. To share a folder on a mounted drive, specify the PathName as *directoryname*. Type and dimension: string-scalar **Note:** This attribute can take localized values.

Table 1-2 lists the optional attributes of the FileShare agent.

Table 1-2 FileShare agent optional attributes

Optional Attributes	Description
AutoControl	Defines the agent behavior when share properties are modified (either from within or outside ApplicationHA) when the FileShare resource is online. The value 1 indicates that the agent synchronizes the changes made to the share properties with those that were defined while configuring the file share service group. The value 0 indicates that the agent does not synchronize the share properties as per what is defined in the service group configuration. If this attribute is set to 0 and the share properties are modified (either from within or outside ApplicationHA), the FileShare resource goes into the UNKNOWN state. The changes made to the share properties remain in effect until the resource is in the UNKNOWN state. To restore the state of the FileShare resource, you must either restore the share properties manually or set this attribute value to 1. The agent restores the share properties that are defined in the service group configuration in its next monitor cycle. Default is 1. To make an existing share highly available, the share name and the share permissions in the configuration file must be the same as those for the file share. Type and dimension: boolean-scalar
AutoShare	Defines the agent behavior when a folder with shared subdirectories is added to a ApplicationHA file share. The value 1 indicates the agent automatically shares the newly added subfolder in its next monitor cycle. The value 0 indicates the agent does not. Default is 1. This attribute is considered only if the attribute ShareSubdirectories is set to 1. Type and dimension: boolean-scalar

Table 1-2 FileShare agent optional attributes *(continued)*

Optional Attributes	Description
ClientCacheType	A string that specifies whether the documents or programs in the shared directory are cached locally on the client system when accessed by users. It also specifies how the files are cached. The cached files are then available offline even if users are not connected to the share. **Note:** The agent does not cache the files or directories itself. It sets the value so that the server and client interfaces do the needful. This attribute can have the following values: ■ MANUAL: Indicates that only the files and programs specified by the users are cached. ■ NONE: Indicates that the files and programs from the share are not cached. ■ DOCS: Indicates that all files and programs that the users open from the share are automatically cached. Files and programs that are not accessed are not available offline. ■ PROGRAMS: Indicates that all files and programs that the users open from the share are automatically cached and are optimized for performance. The next time the user accesses the executable files, they are launched from the local cache. Files and programs that are not accessed are not available offline. Default is MANUAL. Type and dimension: string-scalar
HiddenShare	Defines whether the agent hides the file share. The value 1 indicates the agent hides the file share. The value 0 indicates it does not. Default is 0. Type and dimension: boolean-scalar **Note:** To create a hidden share, set the HiddenShare attribute to 1. Do not append the share name with a $ (dollar) sign.

Table 1-2 FileShare agent optional attributes *(continued)*

Optional Attributes	Description
HideChildShares	Defines whether the agent hides the subfolder shares. The value 1 indicates the agent hides the subfolder shares. The value 0 indicates it does not. Default is 0. This attribute is considered only if the attribute ShareSubdirectories is set to 1. Type and dimension: boolean-scalar
MaxUsers	The maximum number of users that can access the file share. Default is null, which indicates access is granted to maximum users allowed on Windows. If this attribute is set to zero or greater than the maximum users allowed on Windows, access is granted to the maximum users allowed on Windows. Type and dimension: string-scalar
ShareSubdirectories	Defines whether the agent shares the subfolders of the directory specified in the attribute PathName. Subfolders are shared with their own names, that is, the share name of a subfolder is the same as the subfolder name. If a share with the same name exists, the subfolder will not be shared. However, this does not affect the state of the resource. The value 1 indicates the agent shares the subfolders. The value 0 indicates it does not. Default is 0. **Note:** Sharing a folder with a large number of subfolders and enabling the ShareSubdirectories attribute may cause high CPU and memory utilization. Type and dimension: boolean-scalar

Table 1-2 FileShare agent optional attributes *(continued)*

Optional Attributes	Description
UserPermissions	The permissions with which the directories are shared for users. The following permissions are associated with the FileShare resource: ■ FULL_CONTROL: Permission to read, write, create, execute, and delete the system resources, and to modify its attributes and permissions. ■ READ_ACCESS: Permission to read, and execute the system resources. ■ CHANGE_ACCESS: Permission to read, write, execute, and delete the system resources. ■ NO_ACCESS: Permission to deny access to the system resources. The UserPermissions are specified in the format '*Domain_Name**Username*'=*Permission*. For example, to give full control to user John who belongs to the domain AppHA_Domain, the syntax is `'AppHA_Domain\John'=FULL_CONTROL`. Note that the domain name and the user name must be enclosed in quotation marks. Default is {'Everyone' = READ_ACCESS}. A maximum of 50 users can be configured for each file share. To configure more than 50 users for a file share, configure user groups. The agent monitors only the users and permissions that are defined in the service group configuration. Type and dimension: string-association
AccessBasedEnumeration	Defines whether the agent enables the Windows Access-based Enumeration option for the specified file share. The value 1 indicates that the agent enables it and the value 0 indicates that the agent does not. Default is 0. Type and dimension: boolean-scalar

Table 1-2 FileShare agent optional attributes *(continued)*

Optional Attributes	Description
OnlineRetryLimit	This attribute specifies the number of times ApplicationHA retries to bring a resource online if the initial attempt to bring the resource online was unsuccessful. The default value is 1. Type and dimension: integer-scalar
RestartLimit	This attribute specifies the number of times ApplicationHA tries to bring a failed resource online before declaring it as Faulted. The default value is 1. Type and dimension: integer-scalar

How Symantec ApplicationHA agent monitors file shares

The Symantec ApplicationHA agent for FileShare monitors the configured resources, determines the status of these resources, brings them online, and takes them offline. The agent detects an application failure if the configured file shares become unavailable. The agent then tries to start the shares for a configurable number of attempts. If the configured shares do not start, the agent considers this as an application failure and reports the status to VMware HA.

Depending on the configuration, VMwareHA can then restart the virtual machine. After the machine restarts, the agent starts the configured shares and brings the configured resources online.

Chapter 2

Configuring application monitoring with Symantec ApplicationHA

This chapter includes the following topics:

- About configuring application monitoring with Symantec ApplicationHA
- Before configuring application monitoring
- Configuring application monitoring for FileShare
- Administering application monitoring using the ApplicationHA tab

About configuring application monitoring with Symantec ApplicationHA

This chapter describes the steps to configure application monitoring for file shares with Symantec ApplicationHA in a VMware virtualization environment.

Consider the following before you proceed:

- You can configure application monitoring on a virtual machine using the Symantec ApplicationHA Configuration Wizard. The wizard is launched when you click **Configure Application Monitoring** on the ApplicationHA tab in VMware vSphere Client.
- Apart from the Symantec ApplicationHA Configuration Wizard, you can also configure application monitoring using the Veritas Cluster Server (VCS) commands. For more information, refer to the following Technote: http://www.symantec.com/docs/TECH159846

- Symantec recommends that you first configure application monitoring using the wizard before using VCS commands to add additional components or modify the existing configuration.
  Apart from the application monitoring configuration, the wizard also sets up the other components required for Symantec ApplicationHA to successfully monitor the applications.
- 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. Or, you can use the command-line interface (CLI) to configure more than one applications.
- After configuring file shares for monitoring, if you create another share, then these new components are not monitored as part of the existing configuration. In this case, you can either use the VCS commands to add the components to the configuration or unconfigure the existing configuration and then run the wizard again to configure the required shares.

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

- If a configured application fails, Symantec ApplicationHA attempts to start the application on the computer. If the application does not start, Symantec ApplicationHA communicates with VMware HA to take corrective action. Symantec ApplicationHA tries to stop the other configured applications in a predefined order before communicating with VMware HA. This avoids the other applications from getting corrupted due to a computer restart.
  A single failed application can bring down other healthy applications running on the virtual machine. You must take this behavior into consideration while configuring application monitoring on a virtual machine.

Before configuring application monitoring

Note the following prerequisites before configuring application monitoring for FileShare on a virtual machine:

- Verify that you have installed Symantec ApplicationHA (console and guest components) in your VMware environment.
  For information about installing Symantec ApplicationHA, refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.

- Verify that VMware Tools is installed on the virtual machine.
  Install the version that is similar to or later than that available with VMware ESX 4.1.
- Verify that you have installed VMware vSphere Client. The vSphere Client is used to configure and control application monitoring.
  You can also perform the application monitoring operations directly from a browser window using the following URL:

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

  Note: While using a browser to perform application monitoring operations, if the Symantec ApplicationHA version displayed in the application health view is not correct, it may be because older version information is cached by the browser. To correct this, clear the browser cache and try again. If this is also observed while using the vSphere Client, then re-launch the vSphere Client and try again.

- Verify that the logged-on user has administrative privileges on the virtual machine where you want to configure application monitoring.
- If you want 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.
  For information about the ports that are used, refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.
- If you are configuring application monitoring in a disaster recovery environment, ensure that you are using the disaster recovery solution VMware vCenter Site Recovery Manager (SRM). For more information, refer to the *Symantec™ ApplicationHA User's Guide*.

Configuring application monitoring for FileShare

Perform the following steps to configure monitoring for file shares on a virtual machine using the Symantec ApplicationHA Configuration Wizard.

To configure application monitoring for FileShare

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

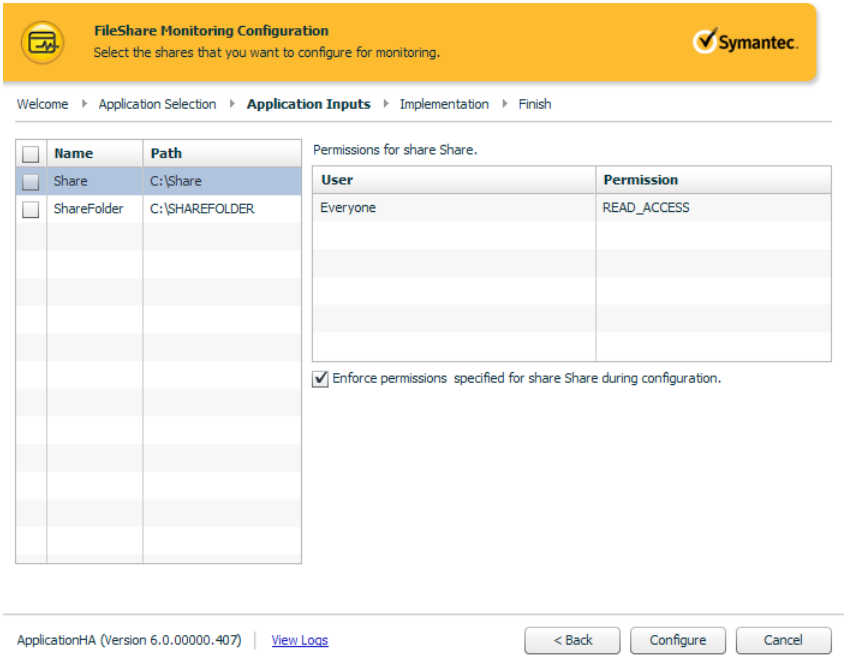
   On theApplicationHA tab, specify the credentials of a user account that has administrative privileges on the virtual machine and then click **Configure**. The ApplicationHA Console sets up a permanent authentication for the user account.

   For more information about single sign-on, refer to the *Symantec™ ApplicationHA User's Guide*.

   After the authentication is successful, the ApplicationHA tab refreshes and displays the application health view.
4. Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard.
5. Review the information on the Welcome panel and then click **Next**.
6. On the Application Selection panel, click **FileShare** in the Supported Applications list.

   You can use the Search box to find the application and then click **Next**.

   If you want to download any of the Symantec ApplicationHA agents, click the **Download Application Agents (SORT)** link to download the agents from the Symantec Operations Readiness Tools (SORT) site.
7. On the FileShare Monitoring Configuration panel, select the file shares that you want to configure for monitoring, and then click **Configure**.



For each file share, the panel displays the path of the share, users for the share, and the permissions for the users.

Perform the following steps to configure file shares for monitoring:

- Choose the file shares that you want to monitor by selecting the respective check boxes. When you select a file share, the users and permissions for the selected file share are displayed in the *Permissions for share <name of the selected file share>* box.
- Select the **Enforce permissions for *<name of the selected file share>* during configuration** check box if you want the user permissions for the selected file share to be in sync with the changes made after you have configured the share for monitoring.

8 On the ApplicationHA Configuration panel, the wizard performs the application monitoring configuration tasks, creates the required resources, and enables the application heartbeat that communicates with VMware HA.

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

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

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

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

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

If the application status shows as not running, click **Start Application** to start the configured components on the computer.

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 in a graphical user interface (GUI). For information about the latter, refer to the *Symantec™ ApplicationHA User's Guide*.

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

Using the ApplicationHA tab, you can also manage the Symantec ApplicationHA licenses by clicking the **Licenses** link. For more information, refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.

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.

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

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

Note: While using a browser to perform application monitoring operations, if the Symantec ApplicationHA version displayed in the application health view is not correct, it may be because older version information is cached by the browser. To correct this, clear the browser cache and try again. If this is also observed while using the vSphere Client, then re-launch the vSphere Client and try again.

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 want 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.

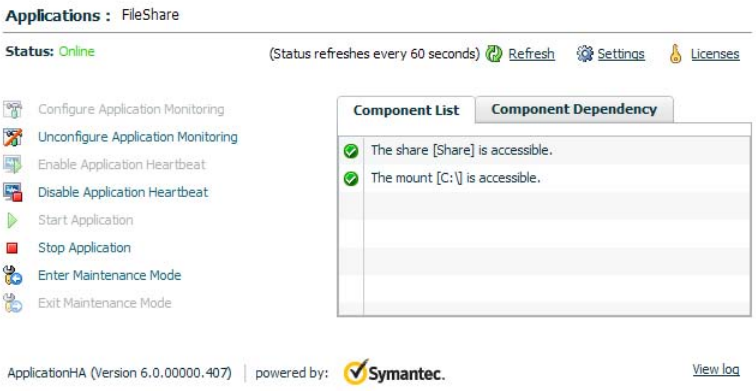
  Symantec ApplicationHA removes all the configured resources for the application and its services.

  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

Note: To view applications at a component level and their dependencies, see the Component Dependency tab under the ApplicationHA tab. For more information, refer to the *Symantec™ ApplicationHA User's Guide*.

Under the ApplicationHA tab, the Component List tab displays the status of the configured file shares.



For example, if you have configured monitoring for FileShare agent, the Component List tab displays the following information:

```
The share [file share] is accessible.
```

Where, *mount point* and *file share* are, respectively, the names of the mount point and file share configured on the virtual machine.

The Component List tab also displays the state of the configured application and its components. The following states are displayed:

```
The mount [mount point] is accessible.
```

online	Indicates that the file share is accessible on the virtual machine.
offline	Indicates that the file share is not accessible on the virtual machine.
partial	Indicates that either the components are being started on the virtual machine or Symantec ApplicationHA was unable to start one or more of the configured file shares.

faulted	Indicates that the configured 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.

Click **Settings** to change ApplicationHA settings for the configured application and the virtual machine. For more information, refer to the *Symantec™ ApplicationHA User's Guide*.

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 the configured file shares.
  Symantec ApplicationHA attempts to start the configured shares and its associated services in the required order. The configured resources are also brought online in the appropriate hierarchy.
- Click **Stop Application** to stop the configured file shares.
  Symantec ApplicationHA begins to stop the configured shares and its associated services gracefully. The configured resources are also taken offline in the appropriate hierarchy.

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 send a heartbeat. You can select VM and Application Monitoring if you also want to enable application monitoring.

ApplicationHA tab lets you 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.