Symantec™ ApplicationHA agent for FileShare Configuration Guide

Windows on Hyper-V

6.1

February 2014

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: 6.1

Document_version: 6.1 Rev 0

Legal Notice

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

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

Contents

Introducing ApplicationHA agents

This chapter includes the following topics:

About ApplicationHA agents

Agents are application-specific modules that plug into the ApplicationHA framework that manages the components of the configured applications.

The agents are installed when you install ApplicationHA. These agents start, stop, and monitor the components of the configured applications and report its state changes. If an application or its components fail, these agents restart the applications and its components on the virtual machine.

A virtual machine has one agent per component that monitors all the components of that type. For example, a single GenericService agent manages all services that are configured using the GenericService components. When the agent starts, it obtains the necessary configuration information from these components and then monitors the configured applications. The agents then periodically updates ApplicationHA with the component and application status.

Agents perform the following operations:

- Brings the components online

- Takes the components offline
- Monitors the components and reports the state changes

ApplicationHA agents are classified in the following categories:

- Infrastructure agents (bundled 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 ApplicationHA.
- Application agents
  Application agents are used to monitor third party applications such as Microsoft SQL Server, Microsoft Exchange and so on. These agents are packaged separately and are available in the form of an agent pack that gets installed when you install ApplicationHA.
  The 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 installation.
  Refer to the Symantec Operations Readiness Tools (SORT) Website for information on the latest agent pack availability:
  https://sort.symantec.com

This document describes the ApplicationHA bundled agents along with their resource type definitions, attribute definitions, and sample configurations.

About intelligent monitoring framework

ApplicationHA provides Intelligent Monitoring Framework (IMF) to determine the status of the configured application and its components. IMF employs an event-based monitoring framework that is implemented using custom as well as native operating system-based notification mechanisms.

IMF provides instantaneous state change notifications. ApplicationHA agents detect this state change and then trigger the necessary actions.

IMF provides the following key benefits:

- Instantaneous notification
  Faster fault detection resulting in faster fail over and thus less application down time.
- Ability to monitor large number of components
  With reduced CPU consumption, IMF effectively monitors a large number of components.
- Reduction in system resource utilization

Reduced CPU utilization by ApplicationHA agent processes when number of components being monitored is high. This provides significant performance benefits in terms of system resource utilization.

About the agent functions and attributes

Every agent has a collection of attributes and performs a definite set of functions.

Attributes are the set of variables whose values configures the corresponding application component to function in a specific way. By modifying attribute values you can change the way in which ApplicationHA agent manages the component.

For example, the IP agent monitors an IP address. The specific address to be monitored is identified by the attribute "Address" whose value is the specific IP address.

Depending on the category to which an agent belongs, an agent performs either or all of the following functions:

Online	Brings the configured component online
Offline	Takes the configured component offline
Monitor	Verifies if the configured component is online

As part of the Monitor function, an agent reports the following states:

ONLINE	Indicates that the configured component is online
OFFLINE	Indicates that the configured component/application has faulted
UNKNOWN	Indicates that the agent encountered errors while monitoring the configured component

About the 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.

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.

Attributes

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

Table 1-1 Required attributes for FileShare agent

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

Table 1-1 Required attributes for FileShare agent *(continued)*

Required Attributes	Description
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 Optional attributes of FileShare agent

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

Table 1-2 Optional attributes of FileShare agent *(continued)*

Optional attributes	Description
AutoShare	Defines the agent behavior when a folder with shared subdirectories is added to a file share configured for monitoring. 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
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

Table 1-2 Optional attributes of FileShare agent *(continued)*

Optional attributes	Description
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.
HideChildShares	Defines whether the agent hides the subfolder shares. 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

Table 1-2 Optional attributes of FileShare agent *(continued)*

Optional attributes	Description
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 Optional attributes of FileShare agent *(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 Optional attributes of FileShare agent *(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 ApplicationHA agents monitor FileShare

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 "Application critical state" to the Hyper-V host.

Depending on the configuration, the Hyper-V host then restarts the virtual machine. After the virtual machine restarts, the agent starts the configured Web sites and the associated application pools and brings the configured resources online on the system.

Chapter 2

Configuring application monitoring

This chapter includes the following topics:

Considerations for configuring application monitoring

Symantec ApplicationHA provides an interface, Symantec ApplicationHA Health View, to configure and administer application monitoring.

A shortcut to access the Health View is created on the system's desktop after you install ApplicationHA. The Health View is Web-based and can be accessed using any of the available browser.

You can also access the Health View directly from a browser window using the following URL:

https://*VMNameorIP*:5634/vcs/admin/application_health.html?priv=ADMIN

Consider the following before you configure application monitoring:

- 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 Symantec ApplicationHA Health View.
- You can use the wizard to configure monitoring for only one application per virtual machine.
  To configure application monitoring on the same virtual machine, for any additional applications, you must use the VCS commands.

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

- The wizard runs in a logged-on user context. You must thus ensure that the logged-on user has administrative privileges on the virtual machine where you want to configure application monitoring.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.

  For information about the ports used, refer to the *Symantec ApplicationHA Deployment Guide*.
- If the application data is stored on nested mount points, then it is required to set the dependency between these mount points. This enables ApplicationHA to monitor all the nested mount points.

  To define the dependency between the nested mount points, you must set the value for MountDependsOn attribute of the MountMonitor agent. The value of this attribute must be specified as a key-value pair.

  Where,

  Key= mount path

  Value= volume name
- 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 all the components.

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.

Configuring application monitoring

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

Note: You can configure monitoring for multiple services and processes in a single wizard workflow. However, you cannot configure multiple applications simultaneously. To configure another application, run the wizard again.

To configure application monitoring for FileShare

1. Launch the Symantec ApplicationHA Health View, using the shortcut created or in a browser, using the following URL:

   https://*VMNameorIP*:5634/vcs/admin/ application_health.html?priv=ADMIN

2. Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard.

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

4. On the Application Selection panel, click **FileShare** in the Supported Applications list.

5. 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.

6. 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 Hyper-V host.

   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.

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

   This completes the application monitoring configuration.

   Use the ApplicationHA Health View to monitor the application status and control application monitoring.

   For more details refer to the *Symantec ApplicationHA Deployment Guide*.

Index