Symantec™ ApplicationHA Release Notes

Windows on VMware

6.1

March 2014

Symantec™ ApplicationHA Release Notes

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.

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

Symantec ApplicationHA Release Notes

This document includes the following topics:

What is Symantec ApplicationHA

ApplicationHA is one of the application availability management solutions from Symantec. It 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 ™ 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 VMware vCenter Server.
- 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 either VMware vSphere Client or the VOM Management Server console.
- 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.

Salient features

Following are the salient features of ApplicationHA:

- Support for enterprise applications.
  For the list of supported applications, refer to,
  http://www.symantec.com/docs/TECH209010
- Simple workflow for installation and configuration
- Single sign-on across virtual machines in a vCenter
- Discretionary access control based on user privileges
- Single GUI for managing applications running on Windows and Linux platforms
- Ability to view component dependency of configured applications over the GUI
- A single dashboard interface that provides a consolidated view of the configured applications and makes it easy for administrators to monitor the applications in the VMware virtual environment
- vSphere Client integrated option to install ApplicationHA guest components, manage licenses and configure single sign-on for site recovery.
- Ability to configure graceful reboot of virtual machines in case of an application failure
- Ability to maintain application monitoring continuity in a VMware SRM controlled disaster recovery environment

- Continued updates and additional application support distributed via Symantec Agent Pack releases

What's new

The enhancements in this release of Symantec ApplicationHA are as follows:

Support for Windows Server 2012 and Windows Server 2012 R2

With this release, ApplicationHA provides support for Windows Server 2012 and Windows Server 2012 R2.

You can now install ApplicationHA, Symantec High Availability Console, and configure application monitoring on systems running Windows Server 2012 and Windows Server 2012 R2.

Added support for new applications and versions

With this release, ApplicationHA provides support for the following applications and versions:

- SQL Server 2012
- Oracle 12c
- IIS 8.0

Change of packaging in the ApplicationHA 6.1 installation media

With this release, Symantec ApplicationHA is packaged along with the Storage Foundation and High Availability (SFHA) 6.1 installation media. This change eliminates the need to download and manage separate installation media for ApplicationHA.

The CD browser displays a separate tab for installing ApplicationHA. When you select the ApplicationHA tab, two separate links; ApplicationHA (for VMare) and ApplicationHA (for Hyper-V) are available to install ApplicationHA based on the virtualization environment.

Added support for VMware versions

The following VMware versions are now supported:

- vSphere Client 5.0 Update 1 a/b, 5.1, 5.5
- vCenter Server 5.0 Update 1 a/b, 5.1, and 5.5

- VMware ESXi Server 5.0 Patch 4, 5.1, and 5.5
- VMware SRM Server 5.1, and 5.5

ApplicationHA licensing

Symantec ApplicationHA is a licensed product. Licensing for Symantec ApplicationHA is based on the server operating systems in use.

During installation, the product installer provides the following options to specify the license details.

- Keyless
  A keyless license installs the embedded keys. You can use the keyless license for 60 days.
  If you install the product using the keyless option, a message is logged everyday in the Event Viewer indicating that you must perform any one of the following tasks, within 60 days of product installation. Failing this, a non-compliance error is logged every four hours.
  - Add the system as a managed host to a Veritas Operations Manager (VOM) Management Server.
    For more details, refer to the VOM documentation.
  - Add an appropriate and valid license key on this system using the Symantec product installer from Windows Add or Remove Programs.
- User Entered Key
  In case of an User Entered Key license, you must procure an appropriate license key from the Symantec license certificate and portal. The User Entered Key license allows you to use the product options based on the license key you enter.
  https://licensing.symantec.com/

Note: Evaluation licenses are now deprecated.

Instantaneous fault detection using Intelligent Monitoring Framework (IMF)

ApplicationHA introduces Intelligent Monitoring Framework (IMF) that uses an event-driven design for monitoring the configured application. IMF is asynchronous and provides instantaneous resource state change notifications. This significantly improves the fault detection capability allowing ApplicationHA to take corrective actions faster. IMF works in addition to the poll-based monitoring.

All the ApplicationHA agents are IMF enabled. You can disable IMF if you do not want an event-driven monitoring.

The benefits of intelligent monitoring over poll-based monitoring are as follows:

- Instantaneous notification
  Faster notification of resource state changes result in improved service group failover times.
- Reduction in system resource utilization
  Reduced CPU utilization by ApplicationHA agent processes when number of application components being monitored is high. This provides significant performance benefits in terms of system resource utilization.
- Ability to monitor large number of resources
  With reduced CPU consumption, IMF enables ApplicationHA to effectively monitor a large number of components.

Support for monitoring nested mount points

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.

A MountDependsOn attribute is now added to the MountMonitor agent. This attribute defines the dependency between the nested mount points.

If this attribute is not configured, then ApplicationHA monitors only the last mount point.

The value of this attribute must be specified as a key-value pair.

Where,

Key= mount path

Value= volume name

Support for 64-bit platforms only

With this release, ApplicationHA provides supports for 64-bit platfoms only.

Both, the OS and the application installation must be 64-bit.

Requirements

For information about the supported operating system, hardware and software requirements, supported applications and other general requirements, see the *Symantec™ ApplicationHA Installation and Upgrade Guide*.

For the latest information on supported hardware, see the Hardware Compatibility List (HCL) at:

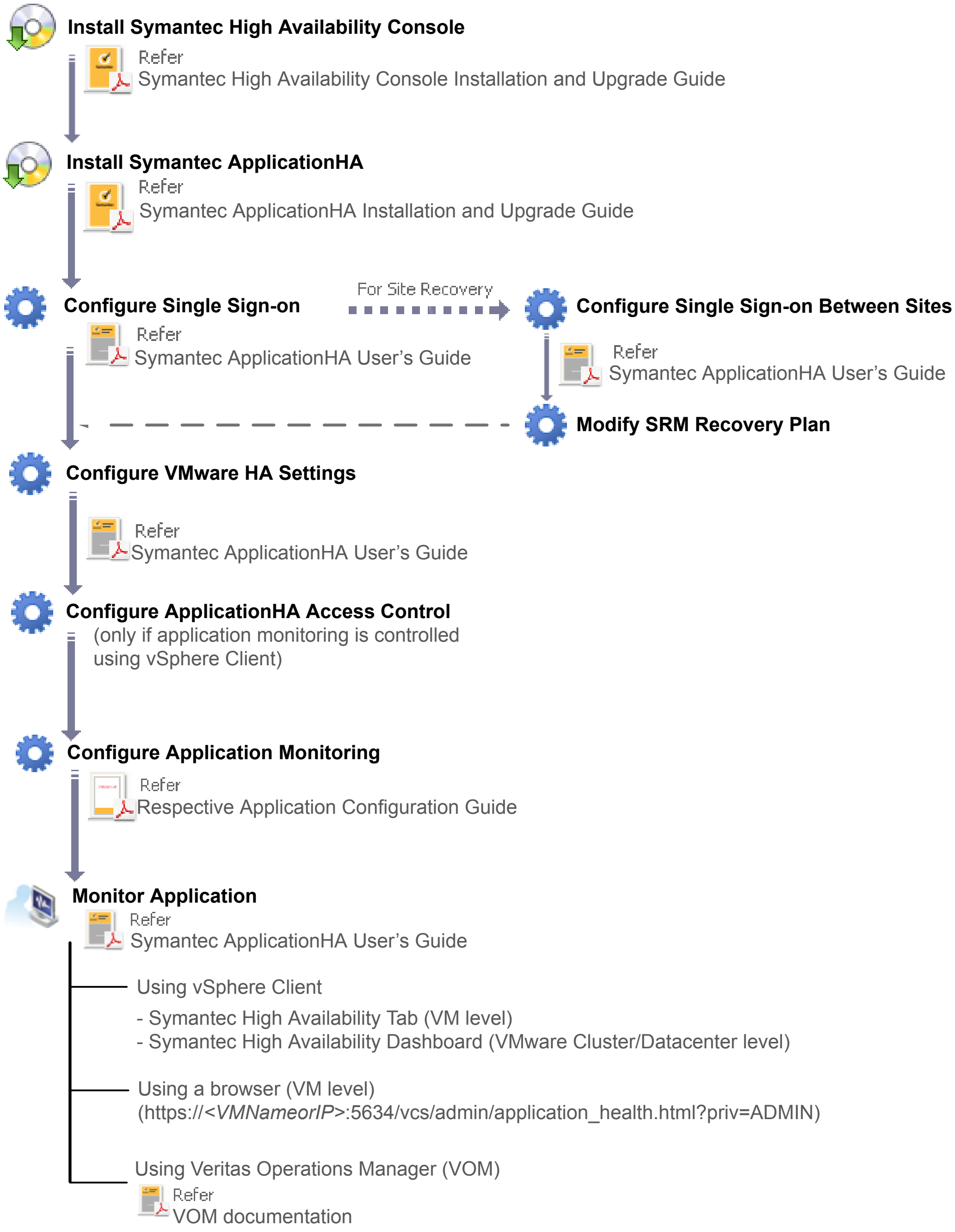
http://www.symantec.com/docs/TECH208993

For the latest information on supported software, see the Software Compatibility List (SCL) at:

http://www.symantec.com/docs/TECH209010

Getting started with ApplicationHA

The following figure represents the workflow for getting started with ApplicationHA and the corresponding document you must refer for details:



Install Symantec High Availability Console

Refer
Symantec High Availability Console Installation and Upgrade Guide

Install Symantec ApplicationHA

Refer
Symantec ApplicationHA Installation and Upgrade Guide

Configure Single Sign-on

Refer
Symantec ApplicationHA User's Guide

For Site Recovery

Configure Single Sign-on Between Sites

Refer
Symantec ApplicationHA User's Guide

Modify SRM Recovery Plan

Configure VMware HA Settings

Refer
Symantec ApplicationHA User's Guide

Configure ApplicationHA Access Control

(only if application monitoring is controlled
using vSphere Client)

Configure Application Monitoring

Refer
Respective Application Configuration Guide

Monitor Application

Refer
Symantec ApplicationHA User's Guide

Using vSphere Client

- Symantec High Availability Tab (VM level)
- Symantec High Availability Dashboard (VMware Cluster/Datacenter level)

Using a browser (VM level)
(https://<*VMNameorIP*>:5634/vcs/admin/application_health.html?priv=ADMIN)

Using Veritas Operations Manager (VOM)

Refer
VOM documentation

Note: The Symantec High Availability Console enables ApplicationHA integration with VMware vSphere Client to perform the following ApplicationHA tasks:

- Install ApplicationHA

- Configure cross site single sign-on for site recovery configuration

- Register virtual machine for auto recovery, if virtual machine auto recovery is configured

- Administer application monitoring

If you do not want to configure site recovery, register the virtual machine for auto recovery, or use the VMware vSphere Client to install ApplicationHA and administer application monitoring, then you need not install Symantec High Availability Console.

No longer supported

Support for the following features, terms, components, or operating sytems is discontinued in release 6.1:

- Veritas Operations Manager 5.0 or earlier
- Veritas Operations Manager Add-on for ApplicationHA management
- VMware Site Recovery Manager (SRM) 4.1
- Symantec ApplicationHA components for VMware SRM Server
  To configure application monitoring continuity in VMware SRM environment, you now do not need to install Symantec ApplicationHA components for VMware SRM Server.
- Symantec ApplicationHA Console is replaced by the Symantec High Availability Console
- Symantec ApplicationHA tab is replaced by the Symantec High Availability tab. Symantec ApplicationHA Dasboard is replaced by Symantec High Availability Dashboard
- Embedded evaluation license keys
- SQL Server 2005
- Exchange 2007
- Windows Server 2003 and Windows Server 2008
  You cannot install ApplicationHA and configure application monitoring on systems running Windows Server 2003 and Windows Server 2008.
- 32-bit architecture (OS and application installations)

You cannot install ApplicationHA and configure application monitoring on 32-bit systems.

Software limitations

The following limitations apply to this release of the product.

ApplicationHA agent for Print Share is supported only on Windows Server 2008 R2

ApplicationHA agent for Print Share is supported only on Windows Server 2008 R2.

You cannot configure PrintShare on systems running Windows Server 2012 and Windows Server 2012 R2.

Dashboard does not detect virtual machines running ApplicationHA guest components of version 5.1 or 5.1 SP1

You cannot use the ApplicationHA dashboard to administer application monitoring on virtual machines that run either ApplicationHA 5.1 on Linux or ApplicationHA 5.1 SP1 on Windows. This is because the dashboard feature was introduced in ApplicationHA 5.1 SP2 and ApplicationHA guest components from the older release do not support the dashboard feature. You can, however, continue to administer application monitoring on such virtual machines through the Symantec High Availability tab.

Workaround:

Upgrade the ApplicationHA guest components from 5.1 or 5.1 SP1 to ApplicationHA 5.1 SP2 or later.

ApplicationHA guest components installation path always defaults to C: drive

This is applicable if you are installing the ApplicationHA guest components from the vSphere client menu.

The guest components installer is unable to detect the drive on which the operating system is installed. The installer always populates the default installation path to C:\Program Files\Veritas. No matter what the %SystemDrive% is, D: or E: or any other drive letter, the installer always defaults to the C: drive.

You can however edit the installation path in the installation wizard. Please ensure that you specify the correct installation path for systems where C: is not the system drive. (2388827)

ApplicationHA Dashboard supports up to 30 (application) component groups per virtual machine

Symantec ApplicationHA introduces a dashboard interface that enables you to monitor the configured applications. In this release, the dashboard supports only 30 (application) component groups per virtual machine.

DBCS characters are not supported

This release does not support Double Byte Character Set (DBCS) characters. Objects such as user names, systems names, directory paths, application instance names, and application component names should not contain DBCS characters. If the system names and directory paths specified while installing the Symantec High Availability Console and guest components contain DBCS characters, the installation may complete successfully. However, you may not be able to configure the virtual machine administrator account on the Symantec High Availability Console. The Symantec ApplicationHA Configuration Wizard may fail to configure application monitoring and the ApplicationHA view in the VMware vSphere Client may not display the status of the virtual machine. (2124936)

Application monitoring is not supported for mounts configured on cluster disk groups

This release does not support application monitoring for volumes and mounts created on cluster disk groups. If you wish to monitor storage managed using Storage Foundation for Windows (SFW), use dynamic disk groups. (2126853)

Application monitoring is not supported for mapped network drives

Symantec ApplicationHA does not support application monitoring for mapped network drives.

Known issues

The following known issues exist in this release of the product.

ApplicationHA may suspend application monitoring if SFW is uninstalled

This issue applies if your setup has SFW and ApplicationHA installed.

After you uninstall SFW, some of the files that are commonly used by SFW and ApplicationHA are removed. As a result, ApplicationHA suspends application monitoring and the Symantec High Availability tab and Symantec High Availability Dashboard fails to display the application status. (3440978)

Workaround: As a workaround, perform the following steps on the virtual machines where SFW is uninstalled:

1. Reboot the virtual machine, after SFW uninstallation is complete
2. Repair ApplicationHA installation
3. Navigate to the following folder and run the Restore_AppHA.bat file:

   Product Install Dir\Veritas Shared\VPI\{F834E070-8D71-4c4b-B688-06964B88F3E8}\

Installation on Windows Server 2012 R2 takes more time when logged on user is a domain administrator

This issue occurs because the Windows Service installation takes approximately 3 to 4 minutes on a Windows Server 2012 R2 system, when logged on user is a domain administrator. (3422177)

To avoid the delay in installation, use the local administrator account. Windows Service installation gets completed within few seconds using a local administrator account.

The application monitoring configuration wizard proceeds with the configuration even if the user account details are invalid

This issue occurs while configuring application monitoring for Oracle databases. (3423351)

On the Oracle Database Selection panel, the configuration wizard enables you to select the databases and provide the following information:

- Domain or host name: The name of the domain or host to which the user belongs in whose context Oracle was installed.
- User Name: The name of the domain user or local user who has Database Administrator privileges for Oracle.
- Password: Password for the user account provided.

The wizard proceeds and completes the configuration even if any of these details are invalid. However, the configured components go in an unknown state later.

Workaround: Unconfigure application monitoring and then configure it again, using valid user account details.

Alternatively, modify the following attributes for the Oracle resource:

- Domain
- UserName
- EncryptedPasswd

To modify the attributes for the Oracle resource

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

```
haconf -makerw
```

This command sets the configuration mode to read/write.

2 Find the Oracle resource name. Type the following on the command prompt and then press **Enter**:

```
hares -list
```

This command lists all the resources that are configured for monitoring. Typically, the Oracle resources are named as "Oracle_*instance name*"

You must modify the attributes for all the Oracle resources.

3 Modify the Domain attribute. Type the following on the command prompt and then press **Enter**:

```
hares -modify resource_name Domain domain or hostname
```

4 Modify the UserName attribute. Type the following on the command prompt and then press **Enter**:

```
hares -modify resource_name UserName username
```

5 Encrypt the user account password. Type the following on the command prompt and then press **Enter**:

```
vcsencrypt -agent password
```

6 Note the encrypted password.

7 Modify the EncryptedPasswd attribute. Type the following on the command prompt and then press **Enter**.

```
hares -modify resource_name EncryptedPasswd encrypted password
```

8 Save and close the configuration. To set the configuration mode to read-only, type the following on the command prompt and then press **Enter**:

```
haconf -dump -makero
```

The application configuration wizard fails to display the SQL Server instances if the provided user account details include any non-English character

This issue occurs while configuring application monitoring for SQL Server 2012. (3423675)

On the Application Inputs panel, the configuration wizard enables you to provide the user account details of a Windows administrative user (SYSADMIN) for SQL Server and accordingly lists the SQL Server instances on the SQL Instance Selection Panel.

If the user account details contain any non-English character, then the wizard fails to display the SQL Server instances.

Workaround: Do not include any non-English characters in the user account details to be provided.

SSO configuration may fail if Symantec High Availability Console is reinstalled

The SSO configuration may fail if you attempt to configure SSO after reinstalling the Symantec High Availability Console. (3414969)

This issue occurs because all the relevant files and folders were not removed during Console uninstallation. The "ApplicationHA" folder is retained even after Console uninstallation.

Workaround: To resolve the issue, perform the following steps:

1. Before reinstalling Console, stop the Veritas Messaging Service.
2. On the machine where you want to reinstall Console, navigate to the following path and delete the "ApplicationHA" folder:

   %programdata%\Symantec
3. Reinstall Console and then configure SSO.

Non-compliance message may be logged even after adding a valid license key

If you install ApplicationHA using the keyless option, a message is logged in the Event Viewer indicating that a valid license must be installed within 60 days of product installation. Failing this, a non-compliance message is logged. (3403622)

The issue occurs if you update the license using Symantec High Availability Home View or Symantec High Availability tab. Even after adding a valid license key the non-compliance message is logged in the Event Viewer.

Workaround: Update/add the valid license key using the Windows Add or Remove Programs.

The SharePoint Server resource fails to come online on a virtual machine other than the SPS Central Administration Console

This issue occurs if the value of AppPoolMon attribute of the ApplicationHA agent for SharePoint Server is set to DEFAULT and IIS 7 is configured to run in the Worker Process Isolation mode. (3379554)

Workaround: Install IIS 6.0 Metabase Compatibility on all the virtual machines where you want to configure monitoring for SharePoint Server.

The application configuration wizard may fail to discover the application

While configuring application monitoring, the application configuration wizard may fail to discover the installed application or may display the "hadiscover is not recognized as an internal or external command" error.

The wizard either does not list the application on the Application Selection panel or displays the error after you click **Next** on the Application Selection panel. (3290602)

This issue occurs if you launch the wizard from a system where you have reinstalled ApplicationHA.

Workaround: Exit the wizard, restart the Veritas Storage Foundation Messaging Service and then re-run the wizard.

Custom settings are lost after repairing Guest Components installation

This issue may occur if you have added custom settings (custom agents, resource types, attributes values, arguments and settings) to your application monitoring configuration after installing this agent pack.

If application monitoring is not yet configured (or if you have unconfigured application monitoring) and then you run a repair of the ApplicationHA Guest Components installation using Windows Add/Remove Programs, all the custom settings made to the configuration are lost.

The repair itself is successful but the customized settings are not retained. The configuration is reverted to the default settings. (3085398)

Workaround: Symantec recommends that before running a repair of the Guest Components installation, you take a backup of the custom settings in the configuration.

Take a backup of the following file:

```
%vcs_home%\conf\config\types.cf
```

Here *%vcs_home%* is the default product installation directory, typically `C:\Program Files\Veritas\Cluster Server`.

After the repair is successful, you manually replace the types.cf file in the existing directory (%vcs_home%\conf\config) with the backup copy you made earlier. This should restore all the customized settings in the configuration.

Configuration wizard cannot discover Allow and Deny permissions of the domain user of a file share

This issue occurs while configuring file shares for application monitoring using the Symantec ApplicationHA Configuration Wizard. If the virtual machine does not have a trust relationship with the domain controller, then the wizard cannot discover the Allow and Deny permissions of the domain user of a file share.

Therefore, you cannot select the permissions of such users for application monitoring. (2326251)

Workaround: There is no workaround for this issue.

Configuration wizard cannot display the SQL instances whose directory paths contain "%"

This issue occurs while configuring SQL Server instances for application monitoring using the Symantec ApplicationHA Configuration Wizard. If the directory path of an instance contains "%" (percent), then that instance is not displayed on the SQL Instance Selection panel of the wizard.

Therefore, you cannot select such instances for application monitoring. (2403740)

Workaround: There is no workaround for this issue.

Configuration wizard does not support monitoring of more than 300 print shares

This issue occurs if you select more than 300 print shares for application monitoring using the Symantec ApplicationHA Configuration Wizard. The wizard times out and fails to configure the shares. To avoid this issue, do not select more than 300 print shares for application monitoring. (2409012, 2409016)

Workaround: There is no workaround for this issue.

Print shares are listed along with file shares while configuring FileShare monitoring

This issue occurs while configuring file shares for application monitoring using the Symantec ApplicationHA Configuration Wizard. The discovery procedure lists print shares along with file shares on the FileShare Monitoring Configuration panel of the wizard. Therefore, the application monitoring for FileShare fails if you select print shares for configuring. (2401444)

Workaround: To resolve this issue, do not select print shares while configuring application monitoring for FileShare. You can configure application monitoring for PrintShare using the wizard by selecting the PrintShare application.

Configuration wizard does not support certain special characters and symbols in the names of printers and print shares

This issue occurs while configuring print shares for application monitoring using the Symantec ApplicationHA Configuration Wizard. For the print shares that you want to configure for monitoring, if any of the share name or its corresponding printer name contains special characters or symbols other than the ones listed below, then the wizard fails to configure the shares for monitoring. (2403557, 2396536)

The wizard supports all the alphanumeric characters and the following special characters and symbols:

~	tilde	(	opening parenthesis
@	at sign	)	closing parenthesis
#	number sign	[	opening bracket
$	dollar sign	]	closing bracket
%	percent	{	opening brace

+	plus sign	}	closing brace
_	underscore		

Workaround: There is no workaround for this issue.

ApplicationHA Configuration wizard cannot configure monitoring for services if a service name contains "&"

This issue occurs while configuring services for application monitoring using the Symantec ApplicationHA Configuration Wizard. If any of the service's name contains "&" (ampersand), then the wizard fails to configure the services for monitoring. (2266698)

Workaround: Perform the following steps to resolve this issue:

1. Using the ApplicationHA view, unconfigure the partial application monitoring.
2. Using the Symantec ApplicationHA Configuration Wizard, configure application monitoring for all the services except the one with "&" in its name.
3. Using the command-line interface (CLI), type the following commands at the command prompt to manually add the resource for the service with "&" in its name:
   - `haconf -makerw`
   - `hares -add <resname> GenericService <groupname>`
   - `hares -modify <resname> ServiceName <servicename>`
   - `haconf -dump -makero`

   Where *resname* is the name of the resource, *groupname* is the name of the group that was created after you completed Step 2, and *servicename* is the name of the service that contains "&".

SSO configuration may fail after upgrading to ApplicationHA 6.1

This issue occurs during the following upgrade paths: (3341666)

- ApplicationHA 5.1 SP2 guest components to ApplicationHA 6.1
- ApplicationHA 5.1 SP2 guest components to ApplicationHA 6.0

The file path where the security certificates for the virtual machine user are saved is different for ApplicationHA 5.1 SP2 than that for ApplicationHA 6.0 and 6.1. During the upgrade to ApplicationHA 6.1, the wizard tries to retrieve these certificates from the path applicable for ApplicationHA 5.1 SP2. Since the certificates are not found at this path, the SSO configuration breaks.

Workaround: Provide the virtual machine user account details on the SSO Configuration panel while installing ApplicationHA 6.1 and reconfigure SSO.

Alternatively, complete the ApplicationHA 6.1 installation without providing the virtual machine user account details and then select the virtual machine from the vCenter Server inventory. Select the Symantec High Availability tab and then provide the user account details to reconfigure SSO.

If more than 10 PrintShare resources are brought online simultaneously, then PrintShare service group faults and the Windows Print Spooler Service crashes

This issue occurs during the first online attempt for the PrintShare service group. (3268645)

If you simultaneously bring more than 10 PrintShare resources online on a single machine, then all the resources try to come online at the same time. As a result, the PrintShare service group faults and the PrintSpooler Service crashes.

Workaround: Restart the Veritas Storage Foundation Messaging Service and the PrintSpooler service.

Note: To avoid the PrintShare resources to simultaneously come online during the first online attempt, set the “NumThreads” attribute of the Print Share agent to 1, before bringing the PrintShare service group online.

This ensures that the resources are brought online one after the other. After the service group is online, you can reset the “NumThreads” attribute to its original value.

App.RestartAttempts setting does not take effect if value is set to 2 or more

App.RestartAttempts configuration option defines the number of times Symantec ApplicationHA tries to restart a failed application or its component. Its value can range from 1 to 6.

For certain application configurations, this setting fails to take effect if its value is set to 2 or more. After successfully configuring an application, if there is a fault in the application or its dependent component, ApplicationHA attempts to restart it once. If the application fails to start, ApplicationHA reports the application state as faulted. (2508392)

This issue is applicable only for the following applications/components:

On Windows

- Custom Application (includes services, processes, and storage mounts)

Workaround

Currently there is no workaround to resolve this issue.

Symantec recommends that for applications mentioned earlier, you set the App.RestartAttempts value to 1.

This ensures that ApplicationHA makes at least one attempt to restart the failed component. If the component still fails to start, ApplicationHA then declares it as faulted and takes further action as per the configuration settings (for example, a graceful reboot of the virtual machine).

Script-based detail monitoring for SQL Server 2008 fails if the script output is more than 1024 characters

This issue occurs if you configure script-based detail monitoring for SQL Server 2008 or SQL Server 2008 R2. If the detail monitoring script output exceeds 1024 characters, the detail monitoring may fail and the SQL resources may either go into an unknown state or fault (if FaultOnDMFailure is set to True) (2710112).

Workaround: Ensure that the output of the script specified for detail monitoring is less than or equal to 1024 characters.

SSO configuration fails if the login user password for Symantec High Availability Console includes a special character "(&)"

This issue occurs during the ApplicationHA guest components installation, using the product installer.

The SSO configuration fails if the login user password for the Symantec High Availability Console specified on the Configure Single Sign-on panel includes the special character—"&".(2594609)

SSO configuration fails if the ApplicationHA guest components installation directory includes a special character ($)

The SSO configuration fails if the custom location path specified during the ApplicationHA guest components installation includes the special character—"$". (2556996)

Application monitoring configuration freezes

This issue occurs if you configure application monitoring on systems where host names start with a hyphen. (2038685)

The application monitoring configuration may freeze and the ApplicationHA view in the vSphere Client may not display the status of the application. If the configured application fails, ApplicationHA takes no action.

Symantec recommends that you rename systems whose host names start with a hyphen before installing ApplicationHA and configuring application monitoring on those systems.

Issues while working with VMware snapshots and migrating virtual machines

The following issues may occur while you are performing virtual machine administration on systems where Symantec ApplicationHA is actively monitoring applications:

- While working with virtual machine snapshots

  This issue occurs if you have installed vCenter Server version 4.0, 4.1, and 4.1 Update 1 only. This issue does not occur if you have installed vCenter Server version 5.0.

  While taking a virtual machine snapshot, the ApplicationHA view may freeze momentarily and may not display the current state of the applications being monitored. Also, after you revert a snapshot, the virtual machine may reboot after the operation completes.

  The Events view on the Tasks & Events tab in the vSphere Client displays the following warning messages:

  Application heartbeat **failed** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

  Application heartbeat status changed to **appStatusRed** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

  Application heartbeat status changed to **appStatusGreen** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

- While migrating virtual machines to an alternate ESX host

  When you initiate a virtual machine migration, the ApplicationHA view may freeze momentarily and may not display the current state of the applications that is being monitored.

  The Events view on the Tasks & Events tab in the vSphere Client displays multiple instances of the following warning messages:

  Application heartbeat status changed to **appStatusGray** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

Application heartbeat status changed to **appStatusGreen** for <virtualmachinedisplayname> on <ESX host> in cluster <clustername> in <datacentername>

Workaround

This is a known issue with VMware HA. Check the following VMware knowledge base article for more information about the hot fix for this issue:

http://kb.vmware.com/kb/1027413

Symantec recommends that you disable the application heartbeat (Disable Application Heartbeat button in the ApplicationHA view) on the virtual machine before working with snapshots or migrating the virtual machine. After the virtual machine administration activity is complete, enable the application heartbeat (Enable Application Heartbeat button in the ApplicationHA view) again.

Symantec ApplicationHA commands do not display the time as per the locale settings

This issue occurs with all the ApplicationHA commands that display the date and time stamp in the output. The date and time stamp do not display as per the locale settings on the system. They are displayed only in English. (2142740)

Symantec High Availability tab may freeze

The Symantec High Availability tab in the vSphere Client may freeze if ApplicationHA is unable to establish a connection with the virtual machine. The application status in the Symantec High Availability view appears to be in a hung state and does not refresh. (2125902)

Workaround

This may occur if the virtual machine fails to respond to ApplicationHA http requests. Either the virtual machine has moved to a suspended state or is in the process of migrating to an alternate ESX host.

Perform the following actions:

- Verify that the virtual machine is powered on and accessible over the network.
- Close the Symantec High Availability tab and open it again.

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

Symantec High Availability Console installation gives an error and the plugin registration fails if the installation directory contains multiple "%" characters

This issue occurs while installing Symantec High Availability Console using the Symantec High Availability Console Installer. On the System Validation panel, if you customize the installation directory to a path that contains consecutive multiple "%" characters, the wizard successfully completes the verification checks and allows you to proceed further. However, when you click **Next** on the Post-install Summary panel the wizard displays a "Failed to create private domain. The system cannot find the path specified" error. You can click **Ok** on the error message and proceed with the installation. However, after the installation workflow is complete the wizard fails to register the ApplicationHA plugin on the vCenter Server.

If you verify the plugin registration using the PluginMgmt.bat utility available on the Console server, the plugin status reflects that the plugin is already registered. However, if you verify the plugin status on the Plug-in Manager available on the vCenter Server, the plugin status reflects "Download & Install".

Workaround

Launch the Symantec High Availability Console installation wizard again and provide a valid path that does not contain multiple "%" characters.

ApplicationHA fails to work if Veritas Operations Manager is uninstalled

The Managed Host components of Veritas Operations Manager (VOM) are installed on the Console Server and the guest virtual machines, during the ApplicationHA installation. A separate entry is created for VOM in the Windows Add Remove Programs. (2361128, 2323516)

Uninstallation of VOM removes the VRTSsfmh package which breaks the ApplicationHA functionality. The sfmh package contains the 'Veritas Storage Foundation Messaging Service' (xprtld) that is used by both, ApplicationHA and VOM.

Note: This issue also occurs when you uninstall the Veritas Operations Manager Central Server.

Workaround

Perform the following steps

1 Insert the ApplicationHA software disc into your system drive and navigate to the Pkgs\Common directory.

If you have uninstalled the Veritas Operations Manager Central Server, you must navigate to the Pkgs\Common\x64 directory.

2 Run the VRTSsfmh.msi

3 Repair ApplicationHA guest installation.

If you have uninstalled the Veritas Operations Manager Central Server, you must repair the ApplicationHA Console installation.

Repairing ApplicationHA Console or guest installation does not affect the application configuration. It thus does not require you to re-configure the applications, after you repair the Console and guest installation.

Note: If you have configured application monitoring for ApplicationHA Console, then you must unconfigure the same before repairing the installation. After the installation repair is complete, you must reconfigure it again for application monitoring.

ApplicationHA guest components installation using the vSphere Client integrated menu may fail with "Failed to log-on..." error

While installing the ApplicationHA guest components using the vCenter integrated menu, the installation workflow completes successfully. However, the installation may fail with the "Failed to log-on" error on some virtual machines after the tasks are queued for installation. (2361891)

Also, a "MKS error..." may appear if you try to connect to these virtual machines using the vSphere client.

Workaround

- Refer to the VMware KB at the following location:

  `http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=749640`

- Restart the virtual machines on which the installation has failed.
- If the problem continues, contact your network administrator.

vMotion causes delay in health view and dashboard refresh

If you have configured application monitoring on a virtual machine with VMware vMotion enabled, the vMotion process gets triggered if the application faults and the virtual machine reboots. (2363462)

Due to vMotion, after a reboot the virtual machine starts and the application comes online on a failover virtual machine on a new ESX host. Even if the application is online, the ApplicationHA health view and the dashboard reflects the application status after a slight delay.

After a vMotion application heartbeat status shows "appStatusGreen" even if the application is faulted

After the application faults if you trigger VMware vMotion instead of VM reboot, the Tasks and Events of a virtual machine reflects the application status as "appStatusGreen", even if the application is faulted. (2363487)

This issue is observed if you are using the VMware vSphere 4.0 and 4.1.

During a test recovery ApplicationHA dashboard at both the sites show the updates

If your VMware cluster network settings for test recovery are such that the failed over virtual machines are able to communicate with the protected site Symantec High Availability Console (due to the MAC address being the same as that of the protected site), then the updates due to the administrative tasks performed for application monitoring are reflected on the ApplicationHA dashboard at both the sites. (2363496)

Guest installation fails with an error "Failed to launch the guest installer process"

This issue is observed while installing the ApplicationHA guest components using the vSphere Client menu.

After the installation workflow is complete the virtual machine is queued for installation. However, the installation process may fail to start with a "Failed to launch the guest installer process" error in the vSphere Client tasks.

Workaround

On the virtual machine where the installation has failed run the installation wizard again.

Refreshing the Symantec High Availability tab multiple times displays a network connectivity error

This issue is typically observed in case of IE7 browser.

Symantec High Availability tab refreshes the application status every 60 seconds. However, in case of network failure if you manually refresh the ApplicationHA view multiple times, IE displays a network connectivity error. (2379946, 2379707)

If you click **Ok** on the error message and then click another virtual machine in the vSphere Client, then the Symantec High Availability tab displays the application status of an unknown application.

This issue also occurs if you refresh the Symantec High Availability tab and simultaneously reset the virtual machine.

Workaround

For details, refer to the following knowledge base article from Microsoft.

http://support.microsoft.com/kb/927917#more_information

ApplicationHA view shows the mount point status as green even if there is a storage disconnect

This issue may occur if the application monitoring configuration contains mount points that reside on shared storage. The ApplicationHA view displays the mount point status as mounted and accessible even if there is a network disconnect between the shared storage and the virtual machine ESX host.

The Events view on the Tasks and Events tab in the vSphere Client may display the following message that confirms the storage disconnect:

```
Lost access to volume <vol> (SharedDataStore) due to connectivity issue.

Recovery attempt is in progress and outcome will be reported shortly.
```

The Symantec ApplicationHA MountMonitor agent that monitors the configured mount points is unable to detect the storage unavailability.

When the storage is connected, application monitoring is restored back to normal.

Configuration wizard may fail if folder mount path contains ampersand (&)

This issue occurs while configuring application monitoring using the Symantec ApplicationHA Configuration Wizard. If you select folder mounts that contain the ampersand (&) character in the path, the wizard may fail while performing the application monitoring configuration tasks. (2132797)

The wizard's Implementation panel may display the following error:

```
Invalid name in entity. [Ln: #, Col: #]
```

Workaround

Do not use the ampersand character (&) in folder mount paths if you wish to configure application monitoring using the Symantec ApplicationHA Configuration Wizard.

If you wish to use this character, configure the MountMonitor agent resource using the VCS commands from the command line.

FileShare agent does not monitor users with denied permissions on shares

This issue occurs after you have configured a file share for application monitoring using the Symantec ApplicationHA Configuration Wizard. If a user has been denied one or more permissions for the configured share, then the FileShare agent does not monitor such user. However, the wizard successfully monitors the share. (2321053)

Workaround

There is no workaround for this issue.

FileShare agent does not support CD-ROM and DVD-ROM drive shares

This issue occurs while configuring file shares for application monitoring using the Symantec ApplicationHA Configuration Wizard. If you are configuring monitoing for CD-ROM or DVD-ROM drive shares, then the wizard cannot configure such shares for monitoring. (2311779)

Workaround

There is no workaround for this issue.

ApplicationHA Configuration Wizard does not support certain special characters and symbols in the names of Mailbox databases

This issue occurs while configuring Exchange 2007 Mailbox databases for application monitoring using the Symantec ApplicationHA Configuration Wizard. If any of the database's name contains special characters or symbols other than the ones listed below, then the wizard fails to configure the databases for monitoring. The wizard supports all the alphanumeric characters and the following special characters and symbols: (2281068)

~	tilde	*	asterisk	}	closing brace
!	exclamation point	(	opening parenthesis	|	pipe, vertical bar
@	at sign	)	closing parenthesis	:	colon
#	number sign	_	underscore	?	question mark
$	dollar sign	+	plus sign	[	opening bracket
%	percent	–	minus sign	]	closing bracket
&	ampersand	{	opening brace	.	period, full stop

Workaround

There is no workaround for this issue.

ApplicationHA Configuration Wizard cannot configure monitoring for a large number of file shares

This issue occurs while configuring a large number of file shares for application monitoring using the Symantec ApplicationHA Configuration Wizard. The wizard fails to configure the shares while performing the **Configure application monitoring** task on the ApplicationHA Configuration panel. (2321442)

Workaround

Use this workaround only after the Symantec ApplicationHA Configuration Wizard has failed to configure shares.

Using the command-line interface (CLI) of the guest computer, type the following commands at the command prompt:

```
%ProgramFiles%\Veritas\VRTSsfmh\bin\xprtlc.exe -l "https://
localhost:5634/vcs/admin/createAppMonHBSG.pl?&ID=CustomApplication&
params=<Cmd><ID>CreateVMWHBSG</ID><ServiceGroups><Name>FileShare_SG</
Name></ServiceGroups></Cmd>";
```

MountMonitor resource is not created for application installation path

This issue occurs when:

- A supported third-party application (such as Microsoft Exchange Server 2007 and SQL Server 2008) is installed on a drive other than the local drive,
- The application is configured for monitoring using the Symantec ApplicationHA Configuration Wizard, and
- The installation path of the application becomes inaccessible.

In such cases, the MountMonitor resource is not created for the application’s installation path. (2325795)

Workaround

You need to manually create the MountMonitor resource for the application’s installation path.

Memory leak in ApplicationHA agent for SharePoint Server 2010

A memory leak occurs in Symantec ApplicationHA agent for SharePoint Server 2010. This issue occurs if you are using IIS 7.0 because the Windows Management Instrumentation (WMI) provider for IIS 7.0 leaks memory. (2210349)

You may receive an error message similar to one of the following:

```
provider not found
```

or

```
provider initialization fail
```

Workaround

Remove IIS 7.0 and use IIS 6.0 instead.

ApplicationHA Configuration Wizard fails to discover a SQL instance if a database name contains double quotation marks

This issue occurs while configuring application monitoring for SQL Server 2008 or 2008 R2 if the database name of an instance contains double quotation marks. In such cases, SQL Server fails to discover the instance, not only the database. (2208925)

Workaround

Either remove the double quotation marks from the database name or configure application monitoring for SQL Server 2008 or 2008 R2 using the command-line interface.

SharePoint Server 2010 applications and services remain online even if the underlying SQL Server faults

Symantec ApplicationHA agent for SharePoint Server 2010 provides monitoring support for SharePoint Server applications and services. This agent does not provide monitoring support for the underlying SQL Server database.

Thus, even if SQL Server faults, the SharePoint Server applications and services remain online. (2212860)

SharePoint Server 2010 applications and services remain online even if the Farm User credentials are changed

If you change the FarmAdminAccount and FarmAdminPassword attribute values, after you have configured the SharePoint Server applications and services, the configured applications and services continue to remain online.

If you want the changed credentials to take effect, you must unconfigure and then reconfigure the applications and services. (2212853)

Memory leak occurs in WMI when monitoring IIS sites using ApplicationHA

On Windows Server 2008 operating systems, a memory leak occurs in Windows Management Instrumentation (WMI) when monitoring the IIS-hosted sites using Symantec ApplicationHA. This issue occurs if IIS 7.o WMI provider is installed on the IIS server. (2077342)

Workaround: This is a known Microsoft problem. To resolve this issue, do the following:

- Ensure that only IIS 6.0 WMI provider is installed on the IIS server.
- Under the Web Server (IIS) role, ensure that the **IIS 6 WMI Compatibility** role service is installed, and the **IIS Management Scripts and Tools** role service is not installed.

Software fixes and enhancements in 6.1

This section provides information about the Symantec ApplicationHA for Windows incidents that have been fixed in the Symantec ApplicationHA 6.0 release.

Incident number	Description
2385156	Single sign-on (SSO) configuration between the virtual machine and the Console host involves specifying the virtual machine administrator account to set up single sign-on for the virtual machine. This configuration fails if the administrator account credential includes the following special characters: ▪ & (ampersand) ▪ * (asterisk) ▪ % (percent) ▪ + (plus) A syntax error dialog is displayed when you try to log on to the virtual machine from the Symantec High Availability tab in the vSphere client.
2376384	You may be unable to install VOM Management Server on a virtual machine where ApplicationHA guest components are installed and a single sign-on is configured with Symantec High Availability Console.
3370571	All applications being monitored on a system are taken offline if any one application faults