Symantec ApplicationHA Release Notes

Windows on Hyper-V

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

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

Introducing ApplicationHA

This document includes the following topics:

About this document

This document provides important information about Symantec ApplicationHA.

Review this document before you install ApplicationHA. You can download the latest version of this document from the Symantec Operations Readiness Tools (SORT) website here:

https://sort.symantec.com

The information in the Release Notes supersedes the information provided in the product documents for ApplicationHA.

For the latest patches available for this release, go to:

https://sort.symantec.com/patch/matrix

What is ApplicationHA

ApplicationHA is one of the application availability management solution from Symantec.

ApplicationHA provides monitoring capabilities for applications running inside virtual machines that are configured on a Hyper-V host. It monitors an application in a start/stop mode on a single virtual machine and adds a level (virtual machine restart) of recovery feature to that provided by Microsoft Failover Cluster.

ApplicationHA employs the agent framework to monitor the state of applications and their dependent components running on the virtual machines. Specific agents are available to monitor the application, storage, and network components. Together, these agents monitor the overall health of the configured applications by running specific commands, tests, or scripts.

What's new

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

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.

Support for Microsoft Hyper-V

ApplicationHA introduces support for Microsoft Hyper-V.

You can now configure application monitoring on virtual machines configured on a Hyper-V host.

When you configure application monitoring, ApplicationHA monitors the application components and conveys its status to the Hyper-V host in form of a heartbeat.

If an application fails, ApplicationHA performs the following actions in the specified sequence:

1. ApplicationHA attempts to restart the components for a configurable number of times.
2. ApplicationHA gracefully restarts the virtual machine. This action is performed only if you have configured ApplicationHA-initiated virtual machine restart. This action is not performed if you have not configured ApplicationHA-initiated virtual machine restart.
3. If the application fails to start, Symantec ApplicationHA sends an "Applications Critical" heartbeat to the Hyper-V host.
4. Depending on the VM Monitoring configuration, the Recovery features of the application take action.

Hyper-V host and guest virtual machines- supported OS versions

ApplicationHA supports the following operating systems for Hyper-V host and guest virtual machines:

For Hyper-V host:

- Windows Server 2012
- Windows Server 2012 R2

For Hyper-V guest virtual machines:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Note: In case of Windows Server 2008 R2 virtual machines you must upgrade the "Integration Service". Failing this, ApplicationHA does not send an "Applications Critical" heartbeat to the Hyper-V host.

New Heartbeat agent for application monitoring

ApplicationHA introduces new Heartbeat agent "HyperVAppMonHB" for monitoring applications in Hyper-V environment.

This heartbeat agent is represented by "HyperVAppMonHB" resource type.

This agent supports intelligent resource monitoring and uses Intelligent Monitoring Framework (IMF) for resource state change notifications.

After you configure application monitoring, a single resource is configured to monitor all components of the configured application.

Note: No separate resources are created, if you configure additional applications using the command line. The single resource that is created monitors all the components, even if multiple applications are configured.

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

ApplicationHA Console and Symantec High Availability Console do not support Microsoft Hyper-V

You must not install ApplicationHA Console or Symantec High Availability Console for configuring application monitoring on virtual machines configured on Hyper-V host.

ApplicationHA Console and Symantec High Availability Console do not support Microsoft Hyper-V.

Compatible Hyper-V features

ApplicationHA is compatible with the following features of Hyper-V

- Live Migration
- Hyper-V Replica

The sequence of ApplicationHA recovery actions remain the same if Hyper-V Live Migration or Hyper-V Replica is configured.

Note: If you have configured Hyper-V Live Migration, then you must configure the virtual machine to use static MAC Address.

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.

Supported applications

With this release, ApplicationHA introduces support for the following applications, in Hyper-V environment:

- Custom application
- IIS
- FileShare
- PrintShare
- Exchange Server 2010
- SQL Server 2008
- SQL Server 2012
- SharePoint Server 2010
- Oracle

Supported software

For the latest information on the supported hardware and software, refer to the hardware and software compatibility lists at the following location:

For Software Compatibility List (SCL):

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

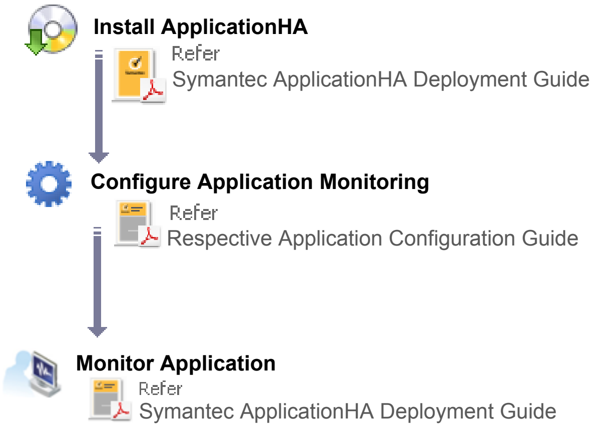
For Hardware Compatibility List (HCL):

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

Getting started with ApplicationHA in Hyper-V environment

The following figure represents the workflow for getting started with Symantec ApplicationHA in a Hyper-V environment. It also shows the corresponding document you must refer to for details.

Figure 1-1 Getting started with ApplicationHA in Hyper-V environment


Install ApplicationHA
Refer
Symantec ApplicationHA Deployment Guide
Configure Application Monitoring
Refer
Respective Application Configuration Guide
Monitor Application
Refer
Symantec ApplicationHA Deployment Guide

No longer supported

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

- 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.
- SQL Server 2005

- Exchange 2007
- Embedded evaluation license keys
- 32-bit architecture (OS and application installations)
- Veritas Operations Manager 5.0 or earlier
- Veritas Operations Manager Add-on for ApplicationHA management

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.

Known issues

This section lists the known issues that are applicable 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.

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.

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.

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.