Symantec™ ApplicationHA Release Notes

AIX on IBM PowerVM

6.0

December 2011

Symantec

Symantec™ ApplicationHA Release Notes

Product Version: 6.0.0

Document Version: 6.0.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec Web site.

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

About Symantec Connect

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

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

Symantec ApplicationHA Release Notes

This document includes the following topics:

Introduction

This document provides important information about Symantec ApplicationHA 6.0. Review this entire document before you install or upgrade ApplicationHA.

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 Symantec ApplicationHA

Symantec ApplicationHA provides monitoring capabilities for applications running inside logical partitions in the IBM PowerVM virtualization environment. Symantec ApplicationHA adds a layer of application awareness to the core high availability (HA) functionality offered by Veritas™ Cluster Server (VCS) in the management LPAR.

Symantec ApplicationHA is based on 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), Low Latency Transport (LLT), Asynchronous Monitoring Framework (AMF), and Veritas Fencing (VxFEN). Symantec ApplicationHA has a lightweight server footprint that allows faster installation and configuration.

Key benefits include the following:

- Out of the box integration with VCS.
- Full visibility and control over applications with the ability to start, stop, and monitor applications running inside managed LPARs.
- High availability of the application as well as the managed LPAR inside which the application runs.
- Graded application fault-management responses such as:-
  - Application restart
  - ApplicationHA-initiated, graceful internal reboot (soft reboot) of a managed LPAR
  - VCS-initiated, external reboot (hard reboot) of managed LPAR
  - Failover of the managed LPAR to another VCS node.
- Standardized way to manage applications using a single interface that is integrated with the Veritas Operations Manager (VOM) console.
- Specialized Application Maintenance mode, in which ApplicationHA allows you to intentionally take an application out of its purview for maintenance or troubleshooting.

Salient features

Following are the salient features of ApplicationHA:

- Support for enterprise applications such as Oracle Database, Apache HTTP Server and DB2.
- Simple workflow for installation and configuration
- Ability to view component dependency of configured applications over the GUI
- Ability to configure graceful reboot of virtual machines in case of an application failure
- Continued updates and additional application support distributed via Symantec Agent Pack releases

Software limitations

The following limitations apply to this release of the product.

Configuration wizard does not support hardware monitoring

You cannot configure hardware components such as storage and network, using the ApplicationHA wizard.

Workaround

- You can ensure that these components do not require monitoring. For example, for storage, you can add appropriate entries in the /etc/fstab file.
- Alternately, you can configure hardware components by using the Command Line Interface of Veritas Cluster Server (VCS) or Veritas Operations Manager (VOM).

ApplicationHA supports only one application per managed LPAR

You can use the Symantec ApplicationHA Configuration wizard to monitor only one application per virtual managed LPAR.

Workaround

If you are familiar with underlying VCS and VOM concepts, you can add more applications or application components for monitoring.

For more information on how to use VCS commands orVOM to configure additional applications, see the following technical note:

http://www.symantec.com/docs/TECH159846

You cannot edit an application monitoring configuration

Once you configure an application, ApplicationHA does not support edits or additions to the configuration.

Workaround

Remove existing configuration and then re-configure

Simultaneous multiple installations may be slow

If you try to install ApplicationHA guest components on a large number of systems, the process may take a long time.

Workaround

Specify smaller batches of systems while using the ApplicationHA install program or response file for multi-system installations.

Multiple VCS clusters are not supported on a single physical server

In the IBM PowerVM virtualization environment, you can designate only one LPAR as a management LPAR on each physical server.

VCS on the management LPAR provides high availability to managed LPARs, by forming a cluster with management LPARs on other physical servers, not the same physical server.

In a VCS cluster, management LPARs must belong to same subnet

If you want to configure application-aware monitoring of managed LPARs, then management LPARs in the same VCS cluster must be on the same subnet. If the management LPARs are on different subnets, VCS may not be able to successfully fail over managed LPARs from one management LPAR to another. (2623075)

VCS support for ApplicationHA cannot be enabled remotely

You must run the enable_applicationha script on each VCS node (management LPAR). You cannot run it remotely from another VCS node in the same cluster, or from a central console.

Known issues

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

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 AIX

- Custom Application

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 managed LPAR).

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)

ApplicationHA fails to work if Veritas Operations Manager is uninstalled

The Managed Host components of Veritas Operations Manager (VOM) are installed on the management LPAR and the managed LPAR, during the ApplicationHA installation. (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 directory that contains the fileset for the AIX operating system:

   ```
   # cd cdrom_root/unix-ppc64-lpar/aix-ppc64/pkgs
   ```

2. Run the following command:

   ```
   # installp -a VRTSsfmh.bff
   ```

3 Stop the `xprtld` service.

```
# /opt/VRTSsfmh/adm/xprtldctrl stop
```

4 Ensure that the file `/etc/opt/VRTSsfmh/xprtld.conf` contains the following text:

```
namespaces vcs=/opt/VRTSvcs/portal
```

5 Start the `xprtld` service.

```
# /opt/VRTSsfmh/adm/xprtldctrl start
```

Refreshing the ApplicationHA view multiple times displays a network connectivity error

This issue is typically observed in case of IE7 browser.

ApplicationHA view 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 on the VOM console, then the ApplicationHA tab displays the application status of an unknown application.

This issue also occurs if you refresh the ApplicationHA view 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

VCS configuration incorrectly retains read-write mode

When you execute the enable_applicationha script on the management LPAR, if an error occurs, the script exits. However, the VCS configuration remains in the read-write mode. In this mode, the configuration is vulnerable to unintentional editing. (2607134)

Workaround

Revert the VCS configuration to the read-only mode by using the following command:

```
# haconf -dump -makero
```

Configuration option of ApplicationHA installer malfunctions

When you run the Symantec ApplicationHA installer, it displays the following option to configure ApplicationHA: **Configure an Installed Product**.

If you specify this option, the installer fails to configure ApplicationHA. Instead, the installer starts stopping certain ApplicationHA processes. (2621468)

Workaround

Do not use the installer option to configure an application. Instead, to configure Symantec ApplicationHA for monitoring an application, use one of the following methods:

- If you have already installed ApplicationHA, navigate to the following URL, and use the **Configure Application Monitoring** link to launch the Symantec ApplicationHA Application Monitoring Configuration Wizard:

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

- You can launch the wizard from the ApplicationHA tab of the Veritas Operations Manager console.
  For more information on working with VOM and accessing the ApplicationHA, see the *Symantec ApplicationHA User's Guide*.

Heartbeat service group may fail to come online

If the high availability daemon (HAD) on the managed LPAR is restarted, the configured heartbeat service group (VCSAppMonHBSG) does not automatically come online. (2605506)

Workaround

To continue application monitoring, you must manually bring the VCSAppMonHBSG online by using the following command:

```
# /opt/VRTSvcs/bin/hagrp -online VCSAppMonHBSG -sys System
```

Where *System* is name of the managed LPAR.

Failure of management LPAR may obstruct managed LPAR monitoring

If a management LPAR fails, VCS may be unable to execute VCS-specific fault-management steps such as hard reboot or fail over of managed LPARs. However, ApplicationHA functionalities such as application restart and graceful internal (soft) reboot of the managed LPARs continue to work. (2564186)

Workaround

Restart the management LPAR to enable re-connection with the managed LPAR on the physical frame.

Attributes of a managed LPAR may retain stale values

If the physical frame crashes, the managed LPARs may indicate stale values for attributes such as ConnectionState and SysState. The settings are updated after a managed LPAR fails over to a new physical frame. (2611726)

Communication between managed LPARs and management LPAR is non-secure

In a secure VCS cluster, the communication between the managed LPARs and the associated management LPAR is through a non-secure TCP/IP channel. (2625819)