# Symantec™ ApplicationHA Deployment Guide

## Windows on Hyper-V

## 6.1

February 2015

Symantec™

# Symantec™ ApplicationHA Deployment Guide

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

Product_version: 6.1

Document_version: 6.1 Rev 1

## 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_apj@symantec.com |
| Europe, Middle-East, and Africa | semea@symantec.com |
| North America and Latin America | supportsolutions@symantec.com |

## About Symantec Connect

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

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

## Documentation

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

doc_feedback@symantec.com

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

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

# Contents

Chapter 1

# Introducing Symantec ApplicationHA

This chapter includes the following topics:

## 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.

# How ApplicationHA works in Hyper-V environment

Symantec ApplicationHA uses the agent framework to monitor the state of the applications and their dependent components running on the virtual machines. These agents monitor the overall health of the configured applications by running specific commands, tests, or scripts. The agents are installed when you install ApplicationHA.

When you configure application monitoring, the ApplicationHA Heartbeat agent begins to monitor 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. The ApplicationHA agents attempt to restart the components for a configurable number of times.
2. If you have configured ApplicationHA-initiated virtual machine restart, ApplicationHA gracefully restarts the virtual machine. This action is not performed if you have not configured ApplicationHA-initiated virtual machine restart. ApplicationHA then skips this action and proceeds to step 3.

   **Note:** ApplicationHA sends the "Applications Critical" heartbeat to the Hyper-V host, only if the Hyper-V host runs Windows Server 2012 operating system (OS).

   To enable ApplicationHA to send the "Applications Critical" heartbeat to the Hyper-V host running Windows Server 2008 R2 OS, you must upgrade the Windows Integration Services. If you do not upgrade the Windows Integration Services, ApplicationHA is unable to send the "Applications Critical" heartbeat to the Hyper-V host.

3. If the application fails to start, 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.

## About ApplicationHA agents

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

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

ApplicationHA agents are classified in the following categories:

- Infrastructure agents (bundled agents)
  Infrastructure agents are packaged (bundled) with the base software and include agents for mount points, generic services, and processes. These agents are immediately available for use after you install ApplicationHA.
  Refer to the *Symantec ApplicationHA Bundled Agents Guide* for more details about the infrastructure agents.
- Application agents
  Application agents are used to monitor third party applications such as Microsoft SQL Server, Microsoft Exchange and so on. These agents are packaged separately and are available in the form of an agent pack that gets installed when you install ApplicationHA. The ApplicationHA agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing ApplicationHA installation.
  Refer to the Symantec Operations Readiness Tools (SORT) Web site for information on the latest agent pack availability.
  https://sort.symantec.com
  Refer to the application-specific configuration guide for more details about the application agents.

## About intelligent monitoring framework

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

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

IMF provides the following key benefits:

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

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

### How IMF works

The following steps outline how IMF-based monitoring works:

1. When IMF is enabled, the ApplicationHA agent waits for the components to report the same steady state (whether online or offline) for two consecutive monitor cycles and then registers the components for IMF-based monitoring.
2. The agent then registers itself for receiving specific custom or operating system specific event notifications.
3. In case of an application failure, the agent determines the affected component and then executes a monitor cycle for that component. The monitor cycle determines the component status. If the component state is offline, then ApplicationHA takes the necessary corrective action, depending on the configuration.
4. If the component state remains the same, then the agent moves to a wait state and then waits for the next event to occur.

## Supported operating systems

ApplicationHA 6.1 supports the following operating systems:

| Hyper-V host | Hyper-V guest virtual machine |
|---|---|
| Windows Server 2012 | Windows Server 2008 R2 |
| Windows Server 2012 R2 | Windows Server 2012 |
| | Windows Server 2012 R2 |

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

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

## Supported Hyper-V features- compatibility matrix

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.

Failing this, the following issues may arise:

- After migrating to a new Hyper-V host, a different MAC address may be assigned to the virtual machine. This may occur because the range of MAC address is different for different hosts.

- While the virtual machine is rebooted as part of the recovery action, the existing MAC address may get reassigned to another system.

As a result of these issues, the virtual machine IP and MAC address may go in to an Unknown state and the application may fail.

For details on configuring the virtual machine to use static MAC Address, refer to Microsoft documentation.

# About the ports and firewall settings

Symantec ApplicationHA uses certain ports and services during installation and configuration. If you have configured a firewall, ensure that the firewall settings allow access to these ports and services.

Table 1-1 displays the services and ports used by ApplicationHA.

**Note:** Ensure that you enable the ports and services for both, inbound and outbound communication.

**Table 1-1** Service and ports used by Symantec ApplicationHA

| Component Name | Process/Service | Port/Protocol | Description |
|---|---|---|---|
| Symantec ApplicationHA installer | File and Printer Sharing | | Used by the installer to copy the installation files to the machine. |
| | Windows Management Instrumentation (WMI) service | | Used by the installer to discover virtual machines. |

**Table 1-1** Service and ports used by Symantec ApplicationHA *(continued)*

| Component Name | Process/Service | Port/Protocol | Description |
|---|---|---|---|
| Symantec ApplicationHA | Veritas Storage Foundation Messaging Service (xprtld) | 5634 / TCP | Used by ApplicationHA to access the application health view through a browser. |

# About ApplicationHA licenses

Symantec ApplicationHA is a licensed product. Licensing for Symantec ApplicationHA are applicable on a per virtual machine basis.

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.
  - Add an appropriate and valid license key on this system using the Symantec product installer from Windows Add/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.
  https://licensing.symantec.com/

## Licensing notes

Review the following licensing notes before you install the product:

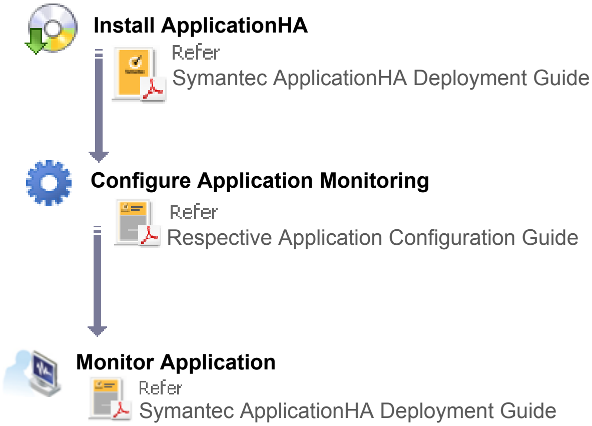
- If you are installing the product for the first time, the "Keyless" option is available by default.
- The product installer enables you to switch from a Keyless license to a User Entered license and vice-a-versa.

- You can manage the licenses using the Windows Add Remove programs and the Symantec ApplicationHA Health View.
- Managing the licenses using the ApplicationHA Health View allows you to only add the license keys. You cannot remove the license keys or change the license type (Keyless to User defined or vice-a-versa), using the ApplicationHA Health View.
- While managing the licenses using the Windows Add Remove programs, you can change the license option from Keyless to User Entered or vice a versa, and add or remove the license keys.
- While repairing the product installation, licenses can be managed only if "Keyless" license option was selected during the installation. You cannot manage the licenses, if the license option selected was "User Entered Key".

## 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

Chapter 2

# Installing and administering ApplicationHA installation

This chapter includes the following topics:

## About installing, repairing or uninstalling ApplicationHA

You can install, repair and uninstall ApplicationHA using any of the following methods:

- Using the installation wizard
  For installing ApplicationHA:
  See "Installing ApplicationHA using installation wizard" on page 17.
  For repairing ApplicationHA installation
  See "Repairing ApplicationHA installation" on page 20.
  For uninstalling ApplicationHA
  See "Uninstalling ApplicationHA using installer" on page 21.
- Using command line interface (CLI)

See “Installing, repairing or uninstalling ApplicationHA using the automated installation mode” on page 23.

## Installing ApplicationHA using installation wizard

Consider the following points before you proceed with the installation:

- The installer uses the logged-on user account context for installation. Verify that the logged-on user has local administrator privileges on the virtual machine where you want to install ApplicationHA.
- Using the product installer you can simultenously install the software on multiple virtual machines.

**Perform the following steps to install ApplicationHA using the installation wizard**

1. From the virtual machine where you want to install ApplicationHA access the software disc or download the installation package from the following location:

   https://fileconnect.symantec.com

2. Double-click **Setup.exe**.

   The CD browser appears.

   ---

   **Note:** If you are installing the software using the product software disc, the CD browser displays the installation options for all the products specified earlier. However, if you are downloading the installation package from the Symantec website, the CD browser displays the installation options only for the product to be installed.

   ---

3. Select the **Symantec ApplicationHA** tab and click **Install ApplicationHA (for Hyper-V)**.

4. Review the prerequisites on the Welcome panel and then click **Next**.

   Note that the **Check for product updates** check box is selected by default. The installer searches for the available product updates on the SORT website. You can download and apply the available updates. If you do not want to apply the available patches, clear the selection of **Check for product updates** check box.

5 On the License Agreement panel, read the Symantec Software License Agreement, select **I accept the terms of License Agreement**, and then click **Next**.

The **Participate in the Symantec Product Improvement Program by submitting system and usage information anonymously** check box is selected by default. The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, clear the selection of the check box.

6 On the Product Updates panel, review the list of available product updates.

This panel appears only if you have selected the **Check for product updates** check box on the Welcome panel.

The product updates comprise of the pre-installation patches, post-installation patches, and the ApplicationHA Agents. The panel lists the available pre-installation patches and the post-installation patches. Download and apply the pre-installation patches in the sequence shown in the table and rerun the wizard. After the successful installation of the product, apply the post-installation patches. Also download and install the ApplicationHA Agents from the SORT website.

7 On the System Selection panel, select the systems and the desired Installation options.

You can select the systems in one of the following ways:

- In the System Name or IP text box, manually type the system name or its IP address and click **Add**.
  The local host is populated by default.
- Alternatively, browse to select the systems.
  The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click **OK**.

Once you add or select a system, the wizard performs certain validation checks and notes the details in the Verification Details box. To review the details, select the desired system.

To select the installation options, perform the following tasks on each of the selected system:

**Note:** You can select the installation options for a single system and then apply them for the other specified systems.

To apply the selection to multiple systems, select the system for which you have selected the installation options and then click **Apply Install Options to Multiple Systems**.

Applying the selected installation options to multiple systems

- By default the wizard uses %ProgramFiles%\Veritas as the installation directory. To customize the installation directory, click **Browse** and select the desired location. Click **OK**.
- Select the required license type from the **License key**drop-down list.
  The default license type is "Keyless".
  If you select "User entered license key" as your license type, the License Details panel appears by default. On the License Details panel, enter the license key and then click **Add**.
  The wizard validates the entered license keys and displays the relevant error if the validation fails. After the validation is complete, click **OK**.

8 On the System Selection panel, click **Next**.

Note that the wizard fails to proceed with the installation, unless all the selected systems have passed the validation checks and are ready for installation. In case the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation, select the system and click **Re-verify** to re-initiate the validation checks for this system.

9 On the Pre-install Summary panel, review the summary and click **Next**.

10 On the Installation panel, review the progress of installation and click **Next** after the installation is complete.

If an installation is not successful on any of the systems, the status screen shows a failed installation.

If the installation has failed, you may have to re-install the software.The details of the failed installation are displayed on the Post-install summary panel.

11 On the Post-install Summary panel, review the installation result and click **Finish**.

This completes the product installation. You must now proceed to configure application monitoring for the application you want to monitor.

For details refer to the respective application configuration guide.

## Applying the selected installation options to multiple systems

**To apply the selected installation options to multiple systems, perform the following steps:**

1. Click on any one of the selected system and specify the desired installation options.
2. Click **Apply to multiple systems**.
3. On the Apply Installation Options panel, select the installation options to be applied and then select the desired systems. Click **OK**.

# Repairing ApplicationHA installation

Use the Symantec ApplicationHA installer to repair the ApplicationHA installation. You can repair the installation on the local machine only. Repairing an installation remotely is not supported.

Repairing the installation restores the installation to its original state, fixes missing or corrupt files, shortcuts, and registry entries on the local machine.

Consider the following points before you begin to repair the installation:

- If the virtual machine is added as a managed host to the VOM central server, before repairing the Symantec ApplicationHA installation, you must repair the Veritas Operations Manager (Host Component) on the system.
- If you have configured application monitoring, then application monitoring may be temporarily suspended, while the installer is repairing the installation. The Symantec ApplicationHA Health View may thus not display the most current status of the application configured.
- The installer uses the logged-on user account context to perform the repair. Verify that the logged-on user has local administrator privileges on the machine where you want to repair the installation.
- While repairing the product installation, licenses can be managed only if "Keyless" license option was selected during the installation. You cannot manage the licenses, if the license option selected was "User Entered Key".
- While repairing the product installation, you cannot modify the installation options.

**To repair the installation**

1. Open the Windows Control Panel and click **Programs and Features**.
2. In the Add or Remove Programs window, select **Symantec ApplicationHA 6.1 (for Hyper-V)** and then click **Change** to launch the Symantec ApplicationHA installer.

3 On the Mode Selection panel, click **Repair** and then click **Next**.

4 Click **OK** on the dialog box that prompts you to repair the Veritas Operations Manager (Host Component).

Refer to VOM documentation for more information.

5 On the System Selection panel the installer automatically selects the local system for repair and begins the validation checks. After the status shows as "Ready for repair", click **Next**.

In case the verification checks have failed, review the details and rectify the issue. Before you choose to proceed with the installation, click **Re-verify** to re-initiate the verification checks.

6 On the Pre-install Summary panel, review the information and click **Next** to begin the repair process.

Note that the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot the system immediately after the repair operation is complete. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

7 On the Installation panel review the installation progress. After the panel indicates that the installation is complete, click **Next**.

If the installation has failed, review the post-install summary report and refer to the wizard log file for details.

The log file is located at,

`%AllUsersProfile%\Veritas\VPI\log\`*`date_timestamp`*

8 On the Post-install Summary panel, review the installation results and then click **Finish**.

This completes the Symantec ApplicationHA installation repair.

## Uninstalling ApplicationHA using installer

Using the product installer, you can simultaneously uninstall the product from multiple remote systems. To uninstall the product from remote systems, ensure that the product is installed on the local system.

Consider the following points before you proceed:

- If application monitoring is configured on the virtual machine, you must first unconfigure the same. This is required for a clean uninstall of ApplicationHA.

- The installer uses the logged-on user account context for uninstallation. Verify that the logged-on user has local Administrator privileges on the system where you want to uninstall.

**Perform the following steps to uninstall ApplicationHA**

1 In the Windows Control Panel, select **Programs and Features**.

2 Select **Symantec ApplicationHA 6.1 (for Hyper-V)** and then click **Remove**.

3 On the Welcome panel review the prequisites and then click **Next**.

4 On the System Validation panel, the wizard selects the local host by default and begins the validation checks. After the status reflects "Ready for uninstall", click **Next**.

**Note:** In case you are performing a remote uninstallation and do not want to uninstall the software from the local system, you must remove that system from the list.

If a system does not meet the required criteria, the status is reflected as "Verification failed". To view the cause of a validation failure, click the Information icon. Rectify the issue and then click **Re-verify** to perform the validation checks again.

5 On the Pre-uninstall Summary panel, review the pre-uninstallation summary and then click **Next**.

Note that the **Automatically reboot systems after installer completes operation** check box is selected by default. This will reboot the system immediately after the uninstall operation is complete. If you do not want the wizard to initiate this auto reboot, clear the selection of **Automatically reboot systems after installer completes operation** check box.

6 On the Un-installation panel review the un-installation progress. After the panel indicates that the tasks are complete, click **Next**.

If the uninstallation has failed on any of the system, review its post-uninstall summary report and check the log file for details.

The log file is located at the following location:

`%AllUsersProfile%\Veritas\VPI\log\`*`date_timestamp`*

7 On the Post-uninstall Summary panel, review the uninstallation results and click **Finish**.

# Installing, repairing or uninstalling ApplicationHA using the automated installation mode

You can install, uninstall or repair the ApplicationHA installation using the Setup.exe command. Using the command line you can perform these operations on one system at a time.

Before installation ensure that you verify the following points:

- There are no parallel installations, live updates, or Microsoft Windows updates in progress.
- If User Access Control (UAC) is enabled, you must launch the command prompt in the Run as administrator mode and then run the command mentioned in this procedure.

---

**Note:** If you are uninstalling ApplicationHA and application monitoring is configured on the virtual machine, you must first unconfigure the same. This is required for a clean uninstall of Symantec ApplicationHA.

---

**To perform an automated install, repair or uninstall**

1 If you want to install ApplicationHA, insert the product software disc into your system's drive or download the software package at a temporary location on your system.

You can download the software package from the following location:

https://fileconnect.symantec.com

2 From the command prompt, navigate to the Symantec ApplicationHA software package root directory.

If you want to repair or uninstall ApplicationHA, navigate to the installation directory.

3 Use the following command syntax to perform the operations:

For installing ApplicationHA:

```
Setup.exe /s SOLUTIONS="10" install_mode=1 TELEMETRY=1
installdir="Installdir" node="VirtualMachine_Name"
licensekey="licensekey" GetPatchInfo=1
```

For repairing ApplicationHA installation:

```
VPI.exe /s SOLUTIONS="10" install_mode=4 TELEMETRY=1
installdir=" Installdir " node=" VirtualMachine_Name "
licensekey=" licensekey " GetPatchInfo=1
```

For uninstalling ApplicationHA installation:

```
VPI.exe /s SOLUTIONS="10" install_mode=5 TELEMETRY=1
installdir=" Installdir " node=" VirtualMachine_Name "
licensekey=" licensekey " GetPatchInfo=1
```

The maximum length of the argument string is 2048 characters and the syntax is not case sensitive.

**Note:** The "Licensekey" parameter is applicable only for "User entered license key" as your license type. You need not specify this parameter for "Keyless" license type.

The following table lists the command line parameters and their values:

| Parameters | Description |
|---|---|
| /s | Specifies the silent or unattended mode of installation.<br>If not set, this launches the product installation wizard. |
| Solutions | Set this parameter to install, repair or uninstall ApplicationHA<br>Example: Solutions= 10 |
| install_mode | Specifies the type of operation.<br>The possible values are:<br>■ 1= install<br>■ 4= repair<br>■ 5= uninstall |
| Telemetry | Set this parameter to participate in the Symantec Product Improvement Program by submitting system and usage information anonymously.<br>The Product Improvement Program allows the product installer to collect installation, deployment, and usage data and submit it anonymously to Symantec. The collected information helps identify how customers deploy and use the product. If you do not want to participate in the product improvement program, set this parameter to 0. |

| Parameters | Description |
|---|---|
| installdir | Set the installation directory path. The path must start and end with a quotation mark.<br>If you do not specify a path, the default installation directory is %ProgramFiles%\Veritas.<br>Example: INSTALLDIR="C:\Program Files\Veritas"<br>This is an optional parameter. |
| Node | Set the physical name of the virtual machine. Specify only one node at a time.<br>If you do not specify a virtual machine name, the operation is performed on the local system by default.<br>The machine name of the node must start and end with a quotation mark ("). |
| licensekey | Set the license key for the installation. Enter multiple keys by separating them with a comma (e.g. 123-345-567-789-123, 321-543-765-789-321, etc.). Do not enter spaces around the comma. The license key must start and end with a quotation mark (").<br>**Note:** This parameter is applicable only if you plan to use the "User entered license key" as your license type. You need not specify this parameter for "Keyless" license type.<br>If you do not specify a license key, the embedded keyless license is installed by default. |
| GetPatchInfo | Set this parameter to search for available product updates.<br>■ 1 = Lists available updates<br>■ 0 = Does not list available updates<br>Default value is 1.<br>The product updates comprise of the pre-installation patches, post-installation patches, High Availability Agents, and Array-Specific Modules. If you set this parameter to 1, then the available pre-installation patches and post-installation patches are listed. If any pre-installation patches are available, then the setup exits to let you download and apply the pre-installation patches. Apply the pre-installation patches in the sequence displayed and rerun the setup with GetPatchInfo = 0. After the successful installation of the product, apply the post-installation patches. Also download and install the High-Availability Agents and Array-Specific Modules from the SORT website. |

# Managing licenses

You can manage your licenses to perform any of the following tasks:

**Note:** You can manage licenses on the local virtual machine only.

- Change the license type from Keyless to User Entered or vice a versa

  During the installation if you have selected Keyless license type, you must add the system as a managed host to a Veritas Operations Manager (VOM) Management Server.

  If you do not want to add the system as a managed host, you must change the license type to **User entered license key** and then specify the appropriate key.
- Adding or removing the license keys

  During the installation if you have selected **User entered license key**, then you can add of remove the license keys.

Use any of the following methods to manage the licenses:

- Navigate to the Windows Add or Remove Programs to launch the Symantec ApplicationHA installer and then select the **Add or Remove** option.

  Managing licenses using Windows Add Remove program
- Access the Symantec ApplicationHA Health View and use the **Licenses** link to launch the License Management panel.

  Managing licenses using ApplicationHA Health View

## Managing licenses using Windows Add Remove program

Use the Windows Add Remove program to manage the ApplicationHA licenses on the local system. You can perform any of the following tasks to manage the licenses:

- Modify the license type (Keyless to User defined or vice-a-versa)
- Add a license key
- Remove a license key

**To manage the Symantec ApplicationHA license keys**

1. Open the Windows Control Panel and click **Programs and Features**.
2. Select **Symantec ApplicationHA 6.1 (for Hyper-V)** and then click**Change** to launch the Symantec ApplicationHA installer.
3. On the Mode Selection panel, select **Add or Remove** and then click**Next**.
4. On the System Selection panel, the wizard performs the verification checks and displays the applicable installation options. In case the verification checks

have failed, review the details and rectify the issue. Before you choose to proceed with the installation click **Re-verify** to re-initiate the verification checks.

To manage the licenses, perform any of the following applicable task:

- To change the license type, select the required license type from the**License key** drop-down list.
  If you change your license type to "User entered license key", the License Details panel appears.
- If you had selected "Keyless" as the license type and now want to enter a license key, click **Edit**.
- If you had selected "User entered license key" as the license type and now want to add or remove the licenses, click **Edit**.

5 To add a license key, enter the key on the License Details panel and then click **Add**.

The wizard validates the entered license keys and displays the relevant error if the validation fails.

To review the license details, select the license key. The details are displayed in the License key details box.

If you want to remove a license key, select the license key and click **Remove**.

6 On the License Details panel, click **OK**.

The wizard displays the applicable installation options on the System Selection panel.

7 On the Pre-install Summary panel, review the summary and click **Next**.

8 On the Installation panel, review the progress of installation and click **Next**after the installation is complete.

If an installation is not successful, the status screen shows a failed installation. Refer to the Post-install summary for more details. Rectify the issue and then proceed to re-install the component.

9 On the Post-install Summary panel, review the installation result and click**Finish**.

The specified licenses take effect immediately.

# Managing licenses using ApplicationHA Health View

Use the ApplicationHA Health View to add the licenses on the local virtual machine.

**Note:** License management using ApplicationHA Health View does not allow you to modify the license type or to remove any licenses. Using the ApplicationHA Health View, you can only add the license keys.

**To manage the licenses using ApplicationHA Health View**

1 Use the following URL to open the ApplicationHA Health View for the virtual machine on which you want to manage the licenses.

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

   Where,

   VirtualMachine IP is the IP address of the individual virtual machine.

2 On the ApplicationHA Health View, click **Licenses**.

3 On the License Management panel, enter the license key and click **Add** and then click **Close**.

   The specified license keys take effect immediately.

   To view the license details, select the license key from the list of Installed licenses.

Chapter 3

# Configuring application monitoring

This chapter includes the following topics:

## Considerations for configuring application monitoring

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

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

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

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

Consider the following before you configure application monitoring:

- Configure "Virtual Machine" role, on the virtual machines where you plan to configure application monitoring.
- Ensure that the "Integration Services" role is enabled on all the virtual machines where you plan to configure application monitoring.
- In case of virtual machines running Windows Server 2008 R2, upgrade the Integration Service.
- You can configure application monitoring on a virtual machine using the Symantec ApplicationHA Configuration Wizard. The wizard is launched when

you click **Configure Application Monitoring** on the Symantec ApplicationHA Health View.

- You can use the wizard to configure monitoring for only one application per virtual machine.
  To configure application monitoring on the same virtual machine, for any additional applications, you must use the VCS commands.
  To configure another application using the wizard, you must first unconfigure the existing application monitoring configuration.
  www.symantec.com/docs/TECH159846
- The wizard runs in a logged-on user context. You must thus ensure that the logged-on user has administrative privileges on the virtual machine where you want to configure application monitoring.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.
  For information about the ports used, refer to the *Symantec ApplicationHA Deployment Guide*.
  For information about the ports that are used, refer to,
  See “About the ports and firewall settings” on page 13.
- If the application data is stored on nested mount points, then it is required to set the dependency between these mount points. This enables ApplicationHA to monitor all the nested mount points.
  To define the dependency between the nested mount points, you must set the value for MountDependsOn attribute of the MountMonitor agent. The value of this attribute must be specified as a key-value pair.
  Where,
  Key= mount path
  Value= volume name
- After configuring services, processes, and mount points for monitoring, if you create another service, process, or mount point, then these new components are not monitored as part of the existing configuration.
  In this case, you can either use the VCS commands to add the components to the configuration or unconfigure the existing configuration and then run the wizard again to configure all the components.

**Note:** When you configure or unconfigure application monitoring, it does not affect the state of the application. The application runs unaffected on the virtual machine.

- If you want to monitor storage managed using Storage Foundation for Windows (SFW), ensure that the volumes and mount points are created on dynamic disk groups.

  Symantec ApplicationHA does not support monitoring for volumes and mount points created on cluster disk groups.

# Configuring application monitoring

Perform the following steps to configure monitoring for services, processes, and mount points on a virtual machine using the Symantec ApplicationHA Configuration Wizard.

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

**To configure application monitoring for services, processes, and mount points**

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

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

   **Note:** *VMNameorIP* refers to the Host name or IP address of the virtual machine.

2. Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard.
3. Review the information on the Welcome panel and then click **Next**.
4. On the Application Selection panel, click **Custom Application** in the Supported Applications list.
5. On the Windows Service Selection panel, select the services that you want to monitor.

   The wizard automatically discovers the services on the virtual machine.

   If a selected service depends on some other services, you must also select those services. You can define the dependencies between those services on the Start-Stop panel later.

   If you do not want to configure any services, click **Next**.
6. On the Windows Process Selection panel, specify the processes that you want to monitor.

Perform the following steps to add a process:

- Click **Add Process** to display the Process Parameters dialog box.
- In the Process Full Path field type the complete path of the process executable file including its extension.

  If you define the process as a script (a Perl script, or a vbs script), specify the full path of the program that interprets the script (perl.exe, or cscript.exe) in the Process Full Path field and specify the full path of the script itself in the Arguments field.

  For example, to specify Perl.exe, type the path as follows:

  `C:\Program Files\Perl\Perl.exe.`
- In the Arguments field, type the command line arguments for the process, if any.
- The specified process runs in the context of the local system account by default. To run the process in a different user's context, check the **Run process using specified credentials** check box and then specify the user name and password in the respective fields.

  The user name must be in the format *user@domain.com* or*domain.com\username*.
- Click **OK**.

  The process that you add is displayed on the wizard page.

  Repeat these steps for all the processes that you want to configure for monitoring.

If you do not want to configure any processes, click **Next**.

7 On the Mount Point Selection panel, select the mount points that you want to monitor.

If you do not want to monitor any mount points, click **Next**.

8 On the Define Start-Stop Order panel, specify the order in which you want the configured services, processes, and mount points to be started or stopped and then click **Configure**.

Perform the following steps to define the dependency between the components:

- Click on an application component name in the Parent Component box on the left.
- Select the check box for the desired component in the Component box on the right.

While starting the service or process, the components are brought online in the defined order. For example, if a service is dependent on a mount point, then while starting the service the mount point is first brought online and then the service itself.

9 On the ApplicationHA Configuration panel, the wizard performs the application monitoring configuration tasks, creates the required resources, and enables the application heartbeat that communicates with Hyper-V host.

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

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

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

This completes the application monitoring configuration.

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

See “About administering application monitoring” on page 34.

Chapter 4

# Administering application monitoring

This chapter includes the following topics:

## About administering application monitoring

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

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

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

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

Use the Health View to perform the following tasks:

- Configure application monitoring
- Unconfigure application monitoring

- Enable application heartbeat
- Disable application heartbeat
- Start application
- Stop application
- Suspend application monitoring
- Resume application monitoring

Using the Health View, you can also manage ApplicationHA licenses and modify the configuration settings.

For details on managing licenses refer to,

See "Managing licenses using ApplicationHA Health View" on page 27.

For details on modifying the configuration settings refer to,

See "Administering application monitoring settings" on page 38.

# Configuring or unconfiguring application monitoring

Use the ApplicationHA Health View to configure or unconfigure application monitoring configuration from a virtual machine.

- To configure application monitoring, click **Configure Application Monitoring**. The Symantec ApplicationHA Configuration Wizard is launched. Follow the wizard to configure monitoring for the desired application.
- To remove application monitoring configuration from a virtual machine, click **Unconfigure Application Monitoring**. This may be required in case you want to re-create the configuration or configure another application using the wizard. Symantec ApplicationHA removes all the configured resources for the application and its services.
  Note that this does not uninstall Symantec ApplicationHA from the virtual machine. This only removes the configuration. The unconfigure option removes all the application monitoring configuration resources from the virtual machine. To monitor the application, you have to configure them again.

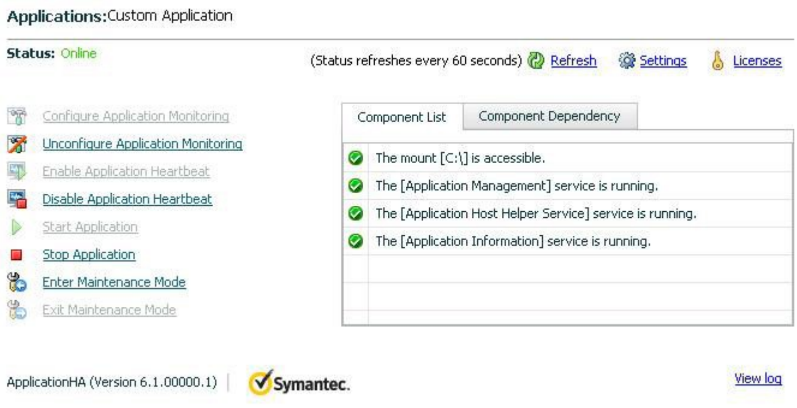
# Viewing the status of configured applications

The ApplicationHA Health View displays the status of configured applications, services or processes. It displays status in the following two views:

- Component List:

This view displays the list of services, processes or mount points configured on the virtual machine for monitoring.

The following figure represents a sample Health View, showing the component list for the configured services, processes and mount points:



**Applications:** Custom Application

**Status:** Online

(Status refreshes every 60 seconds)

The mount [C:\] is accessible.

The [Application Management] service is running.

The [Application Host Helper Service] service is running.

The [Application Information] service is running.

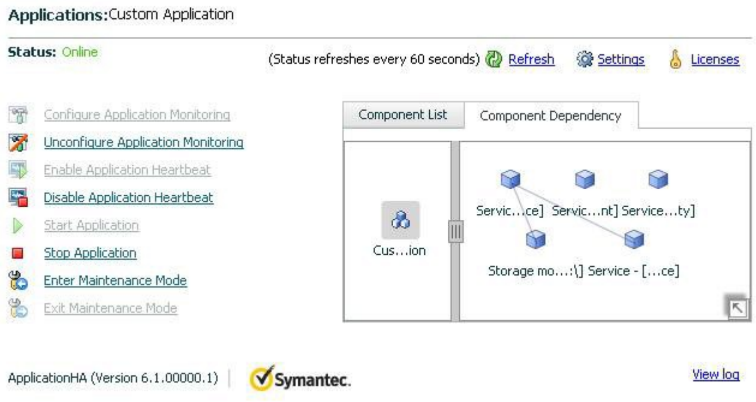
ApplicationHA (Version 6.1.00000.1)

- Component Dependency

  This view displays the dependency between the configured services, processes and mount points.

  The set dependency defines the order in which the components are started or stopped during a failure.

  The following figure represents a sample Health View, showing the component dependency for the configured services, processes and mount points:



**Applications:** Custom Application

**Status:** Online

(Status refreshes every 60 seconds)

ApplicationHA (Version 6.1.00000.1)

The status is displayed in the following states:

| | |
|---|---|
| Online | Indicates that the services and processes are running on the virtual machine. |
| Offline | Indicates that the services and processes are not running on the virtual machine. |
| Partial | Indicates that either the services and processes are being started on the virtual machine or ApplicationHA was unable to start one or more of the configured services or processes. |
| Faulted | Indicates that the configured services or components have unexpectedly stopped running. |

The status is refreshed every 60 seconds by default.

# Starting or stopping the configured applications

Use the following options on the ApplicationHA Health View to start or stop the configured application and the associated components:

- Click **Start Application** to start a configured application.
  Symantec ApplicationHA attempts to start the configured application and its components in the required order. The configured components are brought online in the appropriate hierarchy.
- Click **Stop Application** to stop a configured application that is running on the virtual machine.
  Symantec ApplicationHA begins to stop the configured application and its components gracefully. The configured resources are taken offline in the predefined order.

# Enabling or disabling application heartbeat

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

In case of a failure, Symantec ApplicationHA sends an "Application Critical" heartbeat to the Hyper-V host.

Use the following options on the ApplicationHA Health View to enable or disable the heartbeat of the configured application:

- Click **Enable Application Heartbeat** to enable the heartbeat communication between the configured applications running on the virtual machine and the Hyper-V host.

The application heartbeat is enabled by default when an application is configured for monitoring. However, you must manually enable the heartbeat after resuming application monitoring.

- Click **Disable Application Heartbeat** to stop the heartbeat communication between the configured applications running on the virtual machine and the Hyper-V host.

  Application monitoring is unaffected.

  If an application fails, the virtualization platform-specific recovery actions are not initiated on the system.

  Only the following recovery actions are performed:

  - The application is restarted for the configured number of attempts
  - If VM.GracefulRebootPolicy is enabled, the system reboot is initiated

# Administering application monitoring settings

The ApplicationHA Health View provides a set of options that you can use to control the way Symantec ApplicationHA handles application monitoring, application and dependent component faults, and application recovery on the virtual machine. These configuration settings are applicable on a per virtual machine basis. The settings apply to all the applications that Symantec ApplicationHA monitors on the virtual machine.

The following settings are available:

- App.RestartAttempts

  This option defines the number of times Symantec ApplicationHA should try to restart a failed application or its dependent component. If an application fails to start in the specified number of attempts, Symantec ApplicationHA sends the "Applications Critical" status to the Hyper-V host.

  AppRestartAttempts value can vary between 1 and 6. The default is 1.

- App.ShutdownGraceTime

  This option defines the number of seconds Symantec ApplicationHA should wait before communicating the "Applications Critical" status to the Hyper-V host.

  If a configured application or its dependent component fails, Symantec ApplicationHA tries to restart the component for the configured number of times. If the component fails to start, Symantec ApplicationHA sends an "Applications Critical" status to Hyper-V host. Hyper-V host may then restart the virtual machine depending on the configuration settings.

  An abrupt shutdown may affect the other healthy application components running on the machine. If those components require more time to stop, Symantec ApplicationHA may not be able to stop them gracefully in time before the reboot is initiated. For such cases, you can use AppShutdownGraceTime to delay the virtual machine reboot so that Symantec ApplicationHA stops all the application components gracefully.

Whenan application fails to start, Symantec ApplicationHA initiates a graceful shutdown of all the healthy applications being monitored on the virtual machine and waits for time specified in this option. A virtual machine reboot takes place only after all the application components are shut down gracefully or at the end of the grace time, whichever is earlier.

This setting is applicable to the heartbeat service group that is created when you configure application monitoring using the Symantec ApplicationHA Configuration Wizard. Internally, it sets the DelayBeforeAppFault attribute of the Heartbeat agent resource (VMWAppMonHB) in the configuration.

AppShutDownGraceTime value can vary between 0 and 600. The default is 300 seconds.

- App.StartStopTimeout

  When you click the **Start Application** or **Stop Application** links in the ApplicationHA view, Symantec ApplicationHA initiates an orderly start or stop of the application and its dependent components. This option defines the number of seconds Symantec ApplicationHA must wait for the application to start or stop. If the application does not respond in the stipulated time, an error is displayed in the ApplicationHA Health View.

  A delay in the application response does not indicate that the application or its dependent component has faulted. Parameters such as workload, system performance, and network bandwidth may affect the application response. Symantec ApplicationHA continues to wait for the application response even after the timeout interval is over. If the application fails to start or stop, ApplicationHA takes the necessary action depending on the other configuration settings.

  AppStartStopTimeout value can vary between 0 and 600. The default is 30 seconds.

- VM.GracefulRebootPolicy

  Use this option to enable or disable ApplicationHA-initiated virtual machine restart policy. This option defines whether or not ApplicationHA restarts the virtual machine in response to application and component failures. When a configured application or component fails, ApplicationHA attempts to restart the failed components. If the component fails to start, ApplicationHA then takes no action.

  If this policy is disabled, and an application or component fails, then ApplicationHA sends an "Applications Critical" status to the Hyper-V host. Hyper-V host may then restart the virtual machine depending on the configuration settings.

**Note:** ApplicationHA sends the "Applications Critical" heartbeat to the Hyper-V host, only if the Hyper-V host runs Windows Server 2012 operating system (OS).

To enable ApplicationHA to send the "Applications Critical" heartbeat to the Hyper-V host running Windows Server 2008 R2 OS, you must upgrade the Windows Integration Services. If you do not upgrade the Windows Integration Services, ApplicationHA is unable to send the "Applications Critical" heartbeat to the Hyper-V host.

Refer to the compatibility matrix below.

| Hyper-V host OS | Guest virtual machine OS | ApplicationHA behaviour if VM.GracefulRebootPolicy is 0 |
|---|---|---|
| Windows Server 2012 | Windows Server 2012 | Sends an "Applications Critical" heartbeat to the Hyper-V host. |
| Windows Server 2012 | Windows Server 2008 R2 | Requires you to upgrade the Windows Integration Service. If you do not upgrade this service, then ApplicationHA fails to send an "Applications Critical" heartbeat to the Hyper-V host. |
| Windows Server 2008 R2 | Windows Server 2008 R2 | Does not send an "Applications Critical" heartbeat to the Hyper-V host.<br>You must enable ApplicationHA-initiated virtual machine restart if both, the Hyper-V host and the hosted virtual machines have Windows Server 2008 R2 OS. |

If this policy is enabled, ApplicationHA itself invokes a native operating system command to restart the virtual machine.
VM.GracefulRebootPolicy value can be Enabled (1) or Disabled (0). The default value is Disabled.

- VM.GracefulRebootAttempts
  This option defines the number of times ApplicationHA attempts to restart the virtual machine gracefully if the configured application or component becomes unresponsive. The number of restart attempts is time bound and is defined by the option VM.GracefulRebootTimeSpan. The restart attempts count is reset after the reboot time span elapses.
  For example, if the reboot attempts value is 4, the time span value is 1 hour, and ApplicationHA has restarted the virtual machine once, then the restart attempt count is 3 (initial set value of 4 minus one reboot) for the remaining

period of the 1-hour interval. The restart attempts count is reset to 4 at the beginning of the next 60-minute span.

If the restart attempts are exhausted and the application or component fails within the reboot time span again then ApplicationHA does not take any action.

VM.GracefulRebootAttempts value can vary between 1 and 10. The default value is 1.

- VM.GracefulRebootTimeSpan

  This option defines the time interval, in hours, during which ApplicationHA can gracefully restart the virtual machine for the number of times defined by the option VM.GracefulRebootAttempts.

  VM.GracefulRebootTimeSpan value can vary between 1 and 24. The default value is 1 hour.

**To modify the application monitoring configuration settings**

1. Launch the ApplicationHA Health View.

   Use the following URL to launch the Health View:

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

2. Click the **Settings** link to display the Settings dialog box.

3. Specify the values for the available options displayed in the Settings box and then click **OK**.

   The specified values are updated in the configuration and they take effect immediately.

Appendix A

# IMF- Attribute keys and CLI-based modification

This appendix includes the following topics:

## About the attributes for IMF and the associated keys

The ApplicationHA agents are enabled by default for IMF-based monitoring.

The following attributes define where or not an agent uses IMF-based monitoring for the corresponding application component. You can modify the attribute values to enable or disable IMF-based monitoring.

Table A-1 lists the attributes that determine whether an agent performs IMF-based monitoring.

**Table A-1** Attributes for IMF-based monitoring

| Attribute | Description |
|---|---|
| IMF | |

**Table A-1** Attributes for IMF-based monitoring *(continued)*

| Attribute | Description |
|---|---|
| | Determines whether the IMF-aware agent must perform intelligent resource monitoring. You can also override the value of this attribute at component-level.<br>Type and dimension: integer-association<br>The IMF attribute has three keys: Mode, MonitorFreq, RegisterRetryLimit. A combination of these keys determine whether or not an agent uses IMF-based monitoring for the corresponding component.<br>■ Mode<br>Define this key to enable or disable intelligent resource monitoring.<br>This key takes the following values:<br>■ 0 —Does not perform intelligent monitoring<br>■ 1 —Performs intelligent monitoring for offline components and poll-based monitoring for online components<br>■ 2 —Performs intelligent monitoring for online components and poll-based monitoring for offline components<br>■ 3 —Performs intelligent monitoring for both online and for offline components<br>Default value is 3.<br>■ MonitorFreq<br>This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer.<br>After the component is registered for IMF-based monitoring, the agent calls the monitor agent function as follows:<br>■ For online components: (MonitorFreq X MonitorInterval) number of seconds.<br>■ For offline components: (MonitorFreq X OfflineMonitorInterval) number of seconds.<br>For agents that support IMF, the default value is 5.<br>You can set this attribute to a non-zero value in cases where the agent requires to perform poll-based monitoring in addition to the intelligent monitoring.<br>■ RegisterRetryLimit<br>Determines the number of times the agent must retry registration for a component. |

**Table A-1** Attributes for IMF-based monitoring *(continued)*

| Attribute | Description |
|---|---|
| | If the agent cannot register the component within the limit that is specified, then intelligent monitoring is disabled until the component state changes or the value of the Mode key changes.<br>Default value is 3. |
| IMFRegList | An ordered list of attributes whose values are registered for IMF-based monitoring.<br>Type and dimension: string-vector<br>Default: Not applicable |

# Enabling or disabling IMF

IMF is enabled by default. However, you can manually enable or disable it using the following steps.

**To enable IMF**

1. Change the configuration to read/write mode.

   Type the following at the command prompt:

   ```
   haconf -makerw
   ```

2. Run the following command to enable intelligent monitoring:

   - To enable intelligent monitoring of offline components:

     ```
     hatype -modify resource_type IMF -update Mode 1
     ```

   - To enable intelligent monitoring of online components:

     ```
     hatype -modify resource_type IMF -update Mode 2
     ```

   - To enable intelligent monitoring of both online and offline components:

     ```
     hatype -modify resource_type IMF -update Mode 3
     ```

3. Modify the values of MonitorFreq and the RegisterRetryLimit keys of the IMF attribute.

4. Save the configuration.

   Type the following at the command prompt:

   ```
   haconf -dump -makero
   ```

**Perform the following steps to manually disable IMF**

1. Change the configuration to read/write mode.

   Type the following at the command prompt:

   ```
   haconf -makerw
   ```

2. Run the following commands to disable intelligent monitoring:

   - To disable intelligent monitoring for all the components of a certain type, run the following command:

     ```
     hatype -modify resource_type IMF -update Mode 0
     ```

   - To disable intelligent monitoring for a specific component, run the following commands:

     ```
     hares -override resource_name IMF
     hares -modify resource_name IMF -update Mode 0
     ```

3. Save the configuration.

   Type the following at the command prompt:

   ```
   haconf -dump -makero
   ```

# Index