Symantec™ ApplicationHA Agent for Microsoft Internet Information Services (IIS) Configuration Guide

Windows on VMware

6.1

February 2014

Symantec

Symantec™ ApplicationHA Agent for Microsoft Internet Information Services (IIS) Configuration Guide

Product version: 6.1

Document version: 6.1 Rev 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 website at the following URL:

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Contents

Chapter 1

Introducing the Symantec ApplicationHA agent for Microsoft Internet Information Services (IIS)

This chapter includes the following topics:

About the Symantec ApplicationHA agents

Agents are the processes that manage applications and resources of the predefined resource types which are configured for applications and components on a system. The agents are installed when you install Symantec ApplicationHA. These agents start, stop, and monitor the corresponding resources that are configured for the applications and report state changes.

Symantec ApplicationHA agents are classified as follows:

- Infrastructure 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 Symantec ApplicationHA.

For more details about the infrastructure agents, refer to the *Symantec™ ApplicationHA Generic Agents Guide*.

- Application agents
  Application agents are used to monitor third party applications such as Oracle, Microsoft SQL Server, and Microsoft Exchange. These agents are packaged separately and are available in the form of an agent pack that gets installed when you install Symantec ApplicationHA.
  An 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 guest components installation.
  Refer to the Symantec Operations Readiness Tools (SORT) Web site for information on the latest agent pack availability.
  https://sort.symantec.com
  The following sections provide details about the agent for Microsoft Internet Information Services (IIS).
  For more details about other application agents, refer to the application-specific configuration guide.

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.

About the ApplicationHA agent for Internet Information Services (IIS)

The Microsoft Internet Information Services (IIS) agent for IIS provides monitoring support for sites configured using Microsoft Internet Information Services (IIS).

The agent monitors the Web sites and the associated application pools configured on a virtual machine. The agent brings IIS sites online, monitors their status, and takes them offline.

The agent provides the following ways of monitoring application pools associated with IIS Web sites:

- One IIS resource configures a Web site and sets monitoring options for application pools associated with the site
- One IIS resource configures a Web site; other resources configure individual application pools

IIS agent functions

Online	Starts the configured site or application pool.
Offline	Stops the configured site or application pool.
Monitor	Verifies the configured site or application pool is running.

IIS agent state definitions

ONLINE	Indicates the configured site or application pool is available.
OFFLINE	Indicates the configured site or application pool is not available.
UNKNOWN	Indicates the agent cannot determine the status of the resource.

IIS agent resource type definition

This agent is represented by the IIS resource type.

```
type IIS (
    static int IMF{} = { Mode=2, MonitorFreq=1, RegisterRetryLimit=3 }
    static i18nstr ArgList[] = {SiteType, SiteName,
    "IPResName:Address", PortNumber, AppPoolMon, DetailMonitor,
    DetailMonitorInterval }
    str SiteType
    i18nstr SiteName
    int PortNumber
    str AppPoolMon = NONE
    boolean DetailMonitor = 0
    int DetailMonitorInterval = 5
    str IPResName
)
```

IIS agent attributes

To configure the agent to monitor an application pool, configure the SiteType and SiteName attributes only. The agent ignores other attributes when it is configured to monitor an application pool.

Table 1-1 describes the IIS agent required attributes.

Table 1-1 IIS agent required attributes

Required Attributes	Description
SiteType	Defines whether the resource is configured to monitor an IIS site or an application pool. If the resource is configured to monitor an application pool, set the attribute to APPPOOL. If the resource is configured to monitor an IIS site, set this attribute to the name of the IIS service associated with the site. The attribute can take any of the following values: ■ W3SVC ■ MSFTPSVC ■ SMTPSVC ■ NNTPSVC Type and dimension: string-scalar
SiteName	The name of the IIS site, or the application pool to be monitored by the agent. The value of this attribute depends on the value of the SiteType attribute. The SiteName attribute can take the following values: ■ The name of a site, if SiteType is W3SVC or MSFTPSVC ■ The name of a virtual server, if SiteType is SMTPSVC or NNTPSVC ■ The name of an application pool, if SiteType is APPPOOL Type and dimension: string-scalar
IPResName	The name of the IP resource configured for the IP to which the site is bound. Type and dimension: string-scalar
PortNumber	This attribute is not applicable for Microsoft Internet Information Services (IIS).

Table 1-2 describes the IIS agent optional attributes.

Table 1-2 IIS agent optional attributes

Optional Attributes	Description
AppPoolMon	Defines the monitoring modes for the application pool associated with the Web site being monitored. Configure this attribute only if SiteType is W3SVC and IIS is configured to run in the Worker Process Isolation mode. The attribute can take one of the following values: ■ NONE: Indicates that the agent will not monitor the application pool associated with the Web site. ■ DEFAULT or ALL: Indicates that the agent will monitor the application pool associated with the Web site. If this attribute is set, the agent starts, stops, and monitors the application pool associated with the Web site. If the application pool is stopped externally, the agent fails over the service group. Type and dimension: integer-scalar
DetailMonitor	A flag that defines whether the agent monitors the site in detail. The value 1 indicates the agent will monitor each site in detail by attempting an actual socket connection to the port. Default is 0, which means that detail monitoring is disabled by default. Type and dimension: boolean-scalar
DetailMonitorInterval	The number of monitor cycles after which the agent attempts detail monitoring. For example, the value 5 indicates that the agent will monitor the resource in detail after every 5 monitor cycles. This attribute is ignored if DetailMonitor is set to 0. Default is 5. Type and dimension: integer-scalar

How ApplicationHA agent monitors IIS sites and applications

The IIS agent monitors the configured resources, determines the status of these resources, brings them online, and takes them offline. The agent detects an application failure if the configured IIS Web sites or application pools become unavailable. The agent then tries to start the Web sites for a configurable number of attempts. If the configured Web sites do not start, the agent considers this as an application failure and reports the status to VMware HA.

Depending on the configuration, VMware HA can then restart the virtual machine. After the computer restarts, the agent starts the configured Web sites and the associated application pools and brings the configured resources online on the system.

Chapter 2

Configuring application monitoring with Symantec ApplicationHA

This chapter includes the following topics:

About configuring application monitoring with Symantec ApplicationHA

This chapter describes the steps to configure application monitoring for Microsoft Internet Information Service (IIS) Web sites and associated application pools with Symantec ApplicationHA in a VMware virtualization environment.

Consider the following before you proceed:

- 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 High Availability tab in VMware vSphere Client.
- Apart from the Symantec ApplicationHA Configuration Wizard, you can also configure application monitoring using the Veritas Cluster Server (VCS) commands. For more information, refer to the following Technote:

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

- Symantec recommends that you first configure application monitoring using the wizard before using VCS commands to add additional components or modify the existing configuration.
  Apart from the application monitoring configuration, the wizard also sets up the other components required for Symantec ApplicationHA to successfully monitor the applications.
- You can use the wizard to configure monitoring for only one application per virtual machine.
  To configure another application using the wizard, you must first unconfigure the existing application monitoring configuration. Or, you can use the command-line interface (CLI) to configure more than one applications.
- IIS lets you create sites with duplicate bindings but only one site can run at a time. After configuring an IIS site for monitoring, if you create another Web site with the same IP:Port:HostHeader binding, it may potentially affect the existing configuration. To understand how this affects the monitoring configuration, consider the following example.
  Configure and start monitoring a site with Symantec ApplicationHA. Then, from IIS add another site with the same bindings as the configured site. IIS will let you create the site but you will not be able to start it.
  From the ApplicationHA view, stop the site that is configured for monitoring. Then from IIS start the other site that has duplicate bindings.
  Now, if you try to start the configured site from the ApplicationHA view, IIS will not allow the site to run as another site with the same binding is already running on the system. This may lead to a situation where Symantec ApplicationHA is unable to start the configured site on the system and may trigger the VMware HA solution to restart the virtual machine. If the virtual machine is restarted, Symantec ApplicationHA will still not be able to start the configured IIS site on the virtual machine as there are two sites having the same bindings. As a result the monitoring configuration will not serve its purpose.
  You must therefore ensure that virtual machines where you configure IIS monitoring host sites with unique bindings.
- After configuring IIS Web sites for monitoring, if you create another site or application pool, 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 the required 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. This also does not require any additional steps on the vCenter Server.

- If a configured application fails, Symantec ApplicationHA attempts to start the application on the computer. If the application does not start, Symantec ApplicationHA communicates with VMware HA to take corrective action. Symantec ApplicationHA tries to stop the other configured applications in a predefined order before communicating with VMware HA. This avoids the other applications from getting corrupted due to a computer restart.
  A single failed application can bring down other healthy applications running on the virtual machine. You must take this behavior into consideration while configuring application monitoring on a virtual machine.

Before configuring application monitoring

Note the following prerequisites before configuring application monitoring for Internet Information Services (IIS) on a virtual machine:

- Verify that you have installed Symantec ApplicationHA in your VMware environment.
  For information about installing Symantec ApplicationHA, refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.
- Verify that VMware Tools is installed on the virtual machine.
  Install the version that is similar to or later than that available with VMware ESX 4.1.
- Verify that you have installed VMware vSphere Client. The vSphere Client is used to configure and control application monitoring.
  You can also perform the application monitoring operations directly from a browser window using the following URL:

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

Note: While using a browser to perform application monitoring operations, if the Symantec ApplicationHA version displayed in the application health view is not correct, it may be because older version information is cached by the browser. To correct this, clear the browser cache and try again. If this is also observed while using the vSphere Client, then re-launch the vSphere Client and try again.

- 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
- Verify that you have installed IIS and configured the sites and application pools that you want to monitor on the virtual machine.
- Ensure that the sites have unique IP:Port bindings, host header names, and site names.
- For IIS 7.0, you must install the following role services:
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility or the IIS Management Scripts and Tools
    These options are available under Management Tools on the Role Services page of the Add Roles Wizard.
    If IIS 6 Metabase Compatibility role is installed, the WMI 6 Provider is used. If IIS Management Scripts and Tools role is installed, the WMI 7 Provider is used. If both the roles are installed, the WMI 7 Provider is used.

- 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 that are used, refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.
- If you are configuring application monitoring in a disaster recovery environment, ensure that you are using the VMware disaster recovery solution, VMware vCenter Site Recovery Manager (SRM). For more information, refer to the *Symantec™ ApplicationHA User's Guide*.

Configuring application monitoring for Internet Information Services (IIS)

Perform the following steps to configure monitoring for IIS sites and associated application pools on a virtual machine using the Symantec ApplicationHA Configuration Wizard.

Note: You can configure monitoring for only one application in a single wizard workflow.

To configure application monitoring for Internet Information Services (IIS)

1. Launch the vSphere Client and connect to the vCenter Server that manages the virtual machine.
2. From the vSphere Server's Inventory view in the left pane, select the virtual machine where you want to configure application monitoring, and then in the right pane select the **Symantec High Availability** tab.
3. Skip this step if you have already configured the single sign-on during the guest installation.

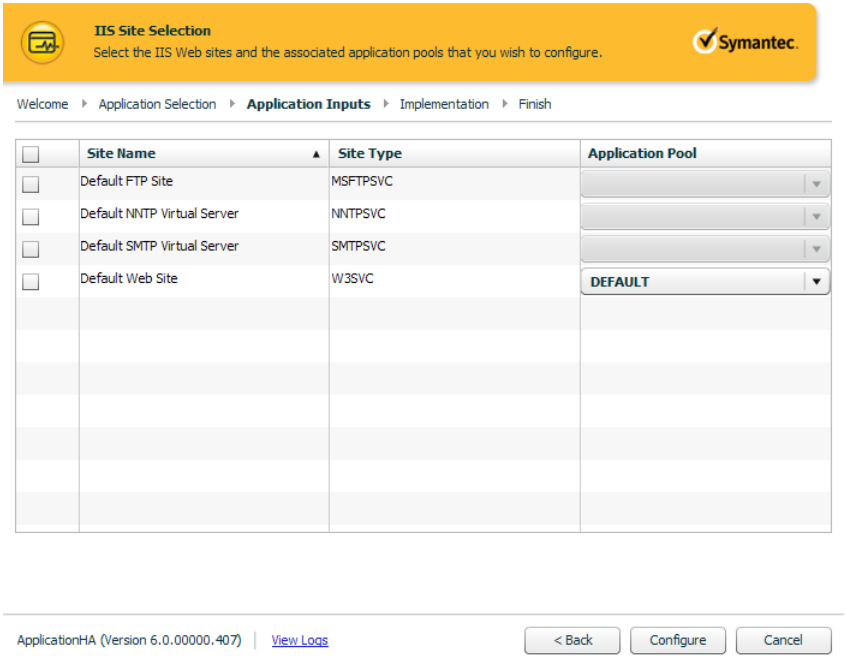
   On the Symantec High Availability tab, specify the credentials of a user account that has administrative privileges on the virtual machine and then click **Configure**. The Symantec High Availability Console sets up a permanent authentication for the user account.

   For more information about single sign-on, refer to the *Symantec™ ApplicationHA User's Guide*.

   After the authentication is successful, the Symantec High Availability tab refreshes and displays the application health view.
4. Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard.
5. Review the information on the Welcome panel and then click **Next**.
6. On the Application Selection panel, click **Microsoft IIS** in the Supported Applications list.

   You can use the Search box to find the application and then click **Next**.

   If you want to download any of the Symantec ApplicationHA agents, click the **Download Application Agents (SORT)** link to download the agents from the Symantec Operations Readiness Tools (SORT) site.
7. On the IIS Site Selection panel, select the IIS sites and the associated applications pools that you want to monitor and then click **Configure**.



Site Name	Displays the sites currently configured on the virtual machine. Click the check box adjacent to the site name to select that site to monitor.
Site Type	Displays the type of each site.
Application Pool	For each selected site, select the application pool monitoring options from the drop-down list. The following options are available: ■ **Default**: Starts and monitors the root application pool associated with the site. ■ **All**: Starts all the application pools associated with the selected site and monitors the root application pool. ■ **None**: Does not monitor the application pools associated with the selected site.

8 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 VMware HA.

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.

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

This completes the application monitoring configuration. You can view the application status in the Symantec High Availability tab.

The view displays the application as configured and running on the virtual machine. The Description box displays the details of the configured components.

If the application status shows as not running, click **Start Application** to start the configured components on the computer.

Administering application monitoring using the Symantec High Availability tab

Note: You can administer application monitoring in two ways. One, using the Symantec High Availability tab as described below and two, using the Symantec High Availability Dashboard. Using the Symantec High Availability dashboard, you can administer application monitoring in a graphical user interface (GUI). For information about the latter, refer to the *Symantec™ ApplicationHA User's Guide*.

Symantec ApplicationHA provides an interface, the Symantec High Availability tab, to configure and control application monitoring. The Symantec High Availability tab is integrated with the VMware vSphere Client.

Use the Symantec High Availability tab to perform the following tasks:

- configure and unconfigure application monitoring
- start and stop configured applications
- enable and disable application heartbeat
- enter and exit maintenance mode

Using the Symantec High Availability tab, you can also manage the Symantec ApplicationHA licenses by clicking the **Licenses** link. For more information, refer to the *Symantec™ ApplicationHA Installation and Upgrade Guide*.

To view the Symantec High Availability tab, launch the VMware vSphere Client, select a virtual machine from the Inventory pane, and in the Management pane on the right, click the **Symantec High Availability** tab.

If you have not configured single sign-on for the virtual machine, specify the user credentials of a user that has administrative privileges on the virtual machine.

You can also perform the application monitoring operations directly from a browser window using the following URL:

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

Note: While using a browser to perform application monitoring operations, if the Symantec ApplicationHA version displayed in the application health view is not correct, it may be because older version information is cached by the browser. To correct this, clear the browser cache and try again. If this is also observed while using the vSphere Client, then re-launch the vSphere Client and try again.

To configure or unconfigure application monitoring

Use the Symantec High Availability tab to configure or delete an application monitoring configuration from the virtual machine. This may be required in case you want to re-create the configuration or configure another application using the wizard.

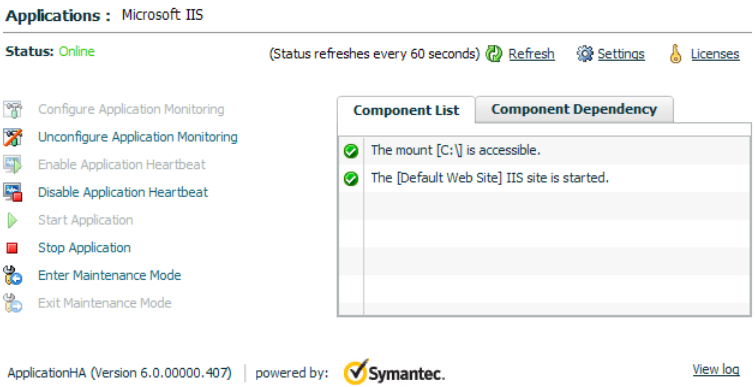
You can use the following buttons:

- Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard. Use the wizard to configure application monitoring.
- Click **Unconfigure Application Monitoring** to delete the application monitoring configuration from the virtual machine.
  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.

To view the status of configured applications

Note: To view applications at a component level and their dependencies, see the Component Dependency tab under the Symantec High Availability tab. For more information, refer to the *Symantec™ ApplicationHA User's Guide*.

Under the Symantec High Availability tab, the Component List tab displays the status of the configured IIS Web sites on the virtual machine.



For example, if you have configured monitoring for IIS Web sites, the Component List tab displays the following information:

```
The mount [mount point] is accessible.

The [site name] IIS site is started.
```

Where, *mount point* and *site name* are, respectively, the names of the mount point and the IIS Web site that is configured.

The Component List tab also displays the state of the configured application and its components. The following states are displayed:

online	Indicates that the configured Web sites are running on the virtual machine
offline	Indicates that the configured Web sites are not running on the virtual machine
partial	Indicates that either the configured Web sites are being started on the virtual machine or Symantec ApplicationHA was unable to start one or more of the configured Web sites

faulted	Indicates that the configured services or components have unexpectedly stopped running.

Click **Refresh** to see the most current status of the configured components. The status is refreshed every 60 seconds by default.

Click **Settings** to change ApplicationHA settings for the configured application and the virtual machine. For more information, refer to the *Symantec™ ApplicationHA User's Guide*.

To start or stop applications

Use the following options on the Symantec High Availability tab to control the status of the configured application and the associated components:

- Click **Start Application** to start the configured IIS Web sites.
  Symantec ApplicationHA attempts to start the configured sites in the required order. The configured resources are also brought online in the appropriate hierarchy.
- Click **Stop Application** to stop the configured IIS Web sites that are running on the virtual machine.
  Symantec ApplicationHA begins to stop the configured sites gracefully. The configured resources are also taken offline in the appropriate hierarchy.

To enable or disable application heartbeat

The VMware virtual machine monitoring feature uses the heartbeat information that VMware Tools captures as a proxy for guest operating system availability. This allows VMware HA to automatically reset or restart individual virtual machines that have lost their ability to send a heartbeat. You can select VM and Application Monitoring if you also want to enable application monitoring.

Symantec High Availability tab lets you control the application heartbeat on the virtual machines.

Use the following options on the Symantec High Availability tab to control the status of the configured application heartbeat:

- Click **Enable Application Heartbeat** to enable the heartbeat communication between the configured applications running on the virtual machine and VMware HA.
  The application heartbeat is enabled by default when an application is configured for monitoring.

- Click **Disable Application Heartbeat** to disable the heartbeat communication between the configured applications running on the virtual machine and VMware HA.

  Disabling the application heartbeat does not instruct VMware HA to restart the virtual machine. This option disables the application monitoring feature in the VMware virtual machine monitoring settings.

To suspend or resume application monitoring

After configuring application monitoring you may want to perform routine maintenance tasks on those applications. These tasks may or may not involve stopping the application but may temporarily affect the state of the applications and its dependent components. If there is any change to the application status, Symantec ApplicationHA may try to restore the application state. This may potentially affect the maintenance tasks that you intend to perform on those applications.

If stopping the application is not an option, you can suspend application monitoring and create a window for performing such maintenance tasks. When application monitoring is suspended, ApplicationHA freezes the application configuration, disables the application heartbeat, and stops sending the heartbeat to VMware HA.

The Symantec High Availability tab provides the following options:

- Click **Enter Maintenance Mode** to suspend the application monitoring for the applications that are configured on the virtual machine. During the time the monitoring is suspended, Symantec ApplicationHA does not monitor the state of the application and its dependent components. The Symantec High Availability tab does not display the current status of the application. If there is any failure in the application or its components, ApplicationHA takes no action.
- Click **Exit Maintenance Mode** to resume the application monitoring for the applications configured on the virtual machine. You may have to click the **Refresh** link in the Symantec High Availability tab to see the current status of the application.

  When application monitoring is restarted from a suspended state, ApplicationHA does not enable the application heartbeat. Click **Enable Application Heartbeat** to enable it.

  If you have made changes that include database addition or change in the underlying storage mount point that was being monitored, then those changes may not reflect in the application monitoring configuration. In such cases, you may have to unconfigure and reconfigure the application monitoring.