

Configuring ApplicationHA in VMware SRM 5.1 environment

Windows Server 2003 and 2003 R2,
Windows Server 2008 and 2008 R2

6.0

Contents

Chapter 1	About the ApplicationHA support for VMware SRM	
	5.1	3
	About ApplicationHA and its components	3
	How does ApplicationHA integrate with VMware SRM 5.1	5
	Typical ApplicationHA configuration in a VMware SRM 5.1 environment	6
	About configuring ApplicationHA in VMware SRM environment with customized specifications	8
Chapter 2	Deploying ApplicationHA in VMware SRM 5.1 environment	9
	About setting up ApplicationHA in VMware SRM 5.1 environment	9
	Configuring single sign-on between virtual machine and Console	12
	Configuring single sign-on between recovery and protected site	13
	Modifying the SRM recovery plan	15

About the ApplicationHA support for VMware SRM 5.1

This chapter includes the following topics:

- [About ApplicationHA and its components](#)
- [How does ApplicationHA integrate with VMware SRM 5.1](#)
- [Typical ApplicationHA configuration in a VMware SRM 5.1 environment](#)

About ApplicationHA and its components

Symantec ApplicationHA provides monitoring capabilities for applications running inside virtual machines managed by a VMware vCenter Server. It adds a layer of application awareness to the core HA functionality offered by VMware virtualization technology.

ApplicationHA monitors the overall health of the configured applications by running specific commands, tests, or scripts. It uses the application heartbeat as the communication medium to convey the status of the application to VMware HA.

If an application fails, ApplicationHA attempts to restart the application for a configurable number of times. If the application fails to restart, ApplicationHA gracefully restarts the virtual machine (only if ApplicationHA-initiated virtual machine restart is configured). If the application fails to restart even after the virtual machine reboot, ApplicationHA stops sending the application heartbeat to VMware HA. Depending on the configuration, VMware HA then takes the necessary corrective action.

ApplicationHA consists of the following components:

Console

Note: The term Console and all the Console-specific information mentioned in this document applies to both, the Symantec ApplicationHA Console and the Symantec High Availability Console.

The Console performs the following functions:

- Registers the ApplicationHA plugin for VMware vCenter Server. The plugin enables Symantec ApplicationHA integration with VMware vSphere Client and adds the ApplicationHA tab and the ApplicationHA dashboard to the VMware vSphere Client. This plugin is required to view the ApplicationHA tab, the ApplicationHA dashboard and the ApplicationHA home page, in the vSphere Client.

Note: If you have installed Symantec High Availability Console, then the name of the plugin, tab, dashboard and the home page that is added in vSphere Client corresponds to Symantec High Availability.

You can use the ApplicationHA tab to configure application monitoring, control application start and stop, and monitor the application status on a virtual machine. You can use the ApplicationHA dashboard to administer application monitoring on a VMware cluster or datacenter.

The ApplicationHA home page is added as an vSphere Client extension under the VMware Solutions and Applications pane. You can use the ApplicationHA home page to perform any of the following tasks:

- Install ApplicationHA or Symantec High Availability guest components
- Manage ApplicationHA or Symantec High Availability licenses
- In case of ApplicationHA, configure Single Sign-on between sites for site recovery
- Provides a single sign-on mechanism so that an authenticated vCenter user does not have to provide the virtual machine user credentials to configure and control application monitoring. The user also does not have to log on each time to connect to the virtual machine from the vSphere Client.
- Adds the Symantec ApplicationHA privileges to the vSphere Client environment. You can use the privileges to configure access control for vCenter Server users and groups.
- In case of ApplicationHA, you can configure the virtual machine for auto recovery.

In a virtual machine auto recovery configuration, Console registers the specified virtual machine for auto-restore and adds the entries to the Console Server database. After the Console Server registers the virtual machine for auto-restore, the ApplicationHA tab displays that the "Virtual Machine Auto Recovery" is configured.

ApplicationHA guest components

The Symantec ApplicationHA guest components are installed separately on the virtual machines where you wish to monitor applications.

The guest components include the following:

- Configuration wizard and the ApplicationHA agents that are used for configuring and monitoring applications.
- Veritas Storage Foundation Messaging Service (xprtld). This service communicates the application monitoring status on the virtual machine and displays it in the ApplicationHA tab.

How does ApplicationHA integrate with VMware SRM 5.1

VMware vCenter Site Recovery Manager (SRM) is a disaster recovery solution for the virtual machines. SRM supports array-based replication of the virtual machines configured at the primary or protected site, to the recovery site and helps to manage synchronization of data between the protected and the recovery site. In case of any disaster, migration of the virtual machines from the protected site to the recovery site is defined by a recovery plan that specifies the recovery tasks to be performed.

ApplicationHA seamlessly integrates with VMware infrastructure to provide application monitoring continuity. The application monitoring continuity is defined in a form of an ApplicationHA recovery command that must be added to the SRM recovery steps, in an appropriate sequence.

The hotfix 'Hotfix_6_0_7_3274237a' provides scripts that must be installed on all the virtual machines (at the protected site) where you want to configure application monitoring. During site recovery, after the virtual machines are failed over to the recovery site, ApplicationHA recovery command invokes these scripts and executes script-based monitoring. The scripts retrieve the application status and provides the same in the SRM history status report.

After all the virtual machines are brought online, ApplicationHA guest components continue to monitor the configured application.

Note: For SRM 5.0 and earlier versions, ApplicationHA provides components that must be installed on VMware SRM Server at the recovery site.

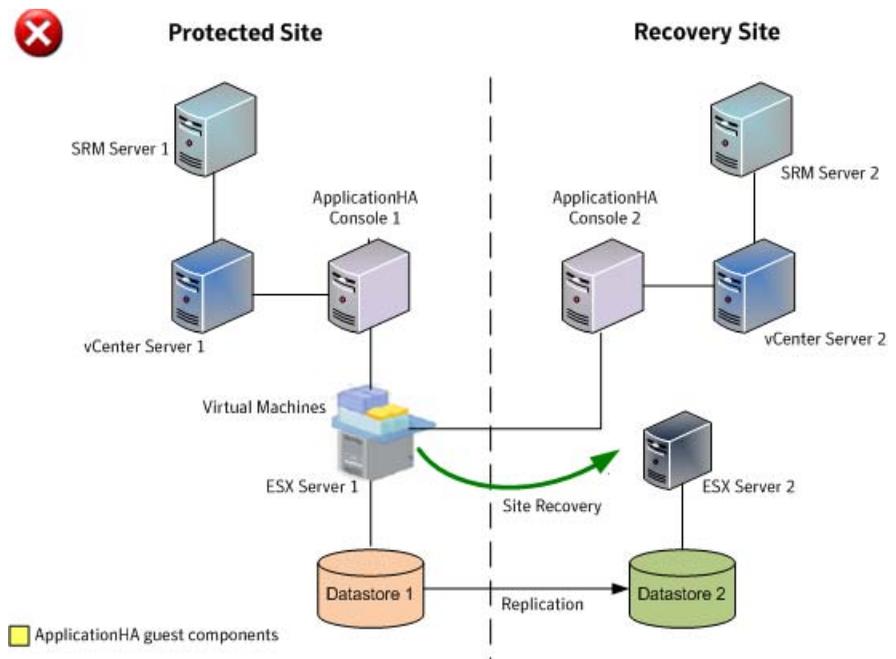
However, for SRM 5.1 and later versions, the hotfix 'Hotfix_6_0_7_3274237a' provides scripts that must be installed on all the virtual machines (at the protected site) where you want to configure application monitoring.

For SRM 5.1 and later versions, you must not install the ApplicationHA Components for VMware SRM.

Typical ApplicationHA configuration in a VMware SRM 5.1 environment

Figure 1-1 represents the typical site recovery VMware cluster configuration with Symantec ApplicationHA enabled for application monitoring continuity.

Figure 1-1 Typical site recovery VMware cluster configuration with Symantec ApplicationHA enabled for application monitoring continuity.



A typical VMware site recovery setup involves VMware cluster configuration on both, the protected site and the recovery site. Each cluster has a SRM Server configured on a separate physical or virtual machine.

For more details on configuring a VMware site recovery setup refer to the VMware documentation.

Along with the SRM Server each site also has a separate vCenter server and a Console configured on a separate physical or a virtual machine. The Symantec ApplicationHA guest components are installed on the virtual machines where you want to configure application monitoring.

After the ApplicationHA guest components are installed a single sign-on is configured between the following:

- Console and the virtual machines at the respective site.
- Console at the recovery site and the virtual machines at the protected site.
This enables the recovery site Console to display the application status in the ApplicationHA tab and the ApplicationHA dashboard, after the virtual machines are failed over to the recovery site.

The ApplicationHA hotfix 'Hotfix_6_0_7_3274237a' is then installed on all the virtual machines (at the protected site) where you want to configure application monitoring.

This hotfix provides scripts that retrieve the application status during site recovery.

Note: For SRM 5.0 and earlier versions, the ApplicationHA hotfix 'Hotfix_6_0_7_3274237a' provides components that must be installed on VMware SRM Server at the recovery site.

However, for SRM 5.1 and later versions, the ApplicationHA hotfix 'Hotfix_6_0_7_3274237a' provides scripts that must be installed on all the virtual machines (at the protected site) where you want to configure application monitoring. For SRM 5.1 and later versions, you must not install the ApplicationHA Components for VMware SRM.

After the hotfix is installed on the virtual machines, the SRM recovery plan is edited to define the action for application monitoring continuity. This action is defined in the form of an ApplicationHA recovery command that must be added to the SRM recovery steps in an appropriate sequence.

When a disaster occurs the protected site virtual machines fail over to the recovery site and are brought online as per the configured VMware disaster recovery plan. The recovery plan executes the ApplicationHA recovery command in the specified sequence. This command executes script-based monitoring on the virtual machines to retrieve the application status. The application health status is displayed in the SRM history status report.

The highlighted step in the following figure represents a sample application recovery status displayed in the SRM history status report. This sample represents the "Online" application state.

If the application is not online, the Application recovery command displays an error. You can view the error details in the ApplicationHA log file.

Following are the application states and its status displayed in the log file.

Application state	Status displayed
Online	Application is running
Partially online	Application is partially running
Faulted	Some of the application components are faulted
Offline	Application is not running

If these states are observed while the application is starting, the status is appended by "[Starting Application ...]". However, if the states are observed while the application is stopping, the status is appended by "[Stopping Application ...]".

About configuring ApplicationHA in VMware SRM environment with customized specifications

In most cases the VMware site recovery clusters may have customized specifications such that after a failover,

- the computer name of a virtual machine on the protected site changes at the recovery site.
- the network settings at the protected site provide an IP address different from that at the recovery site.

If you have configured ApplicationHA in a VMware cluster where the computer name of a virtual machine changes at the recovery site, the ApplicationHA tab at the recovery site displays the cluster state as "Unknown" and the application fails to come online.

Similarly, if the configured application uses the virtual machine IP address, then the application may fail to come online or may not be accessible over the network after a site recovery. You must re-configure the application at the recovery site with the new IP address, using the ApplicationHA tab.

Deploying ApplicationHA in VMware SRM 5.1 environment

This chapter includes the following topics:

- [About setting up ApplicationHA in VMware SRM 5.1 environment](#)
- [Configuring single sign-on between virtual machine and Console](#)
- [Configuring single sign-on between recovery and protected site](#)
- [Modifying the SRM recovery plan](#)

About setting up ApplicationHA in VMware SRM 5.1 environment

[Table 2-1](#) describes the tasks for setting up ApplicationHA in a VMware SRM 5.1 environment.

Table 2-1 Tasks for setting up ApplicationHA in a VMware SRM 5.1 environment

Task	Details
Configure VMware site recovery cluster setup	<p>A typical VMware site recovery setup involves VMware cluster configuration on both, the protected site and the recovery site.</p> <p>Array-based replication is set across the storage on protected site and the recovery site. Each site has a vCenter Server and a SRM Server configured on separate physical or virtual machines.</p> <p>A cluster is set up between the SRM Servers across sites. Both the sites are paired to exchange authentication information and discover replicated storage arrays, and supported devices.</p> <p>Additionally,</p> <ul style="list-style-type: none"> ■ The folders, networks, and resource pools on the protected site to which the virtual machines are assigned are mapped on the recovery site. ■ A protection group is created for the protected site virtual machines. ■ A recovery plan is configured specifying the failover priority order and the recovery steps to be performed. <p>Refer to the VMware documentation for more details on configuring a VMware site recovery cluster setup.</p>
Install Console	<p>At both the sites, install Console on a separate physical or virtual machine.</p> <p>You must ensure that the recovery site Console is powered on and accessible from the guest virtual machines at the protected site, before and after the failover.</p> <p>If you are installing Symantec ApplicationHA Console, refer to the <i>Symantec™ ApplicationHA Installation and Upgrade Guide</i>.</p> <p>If you are installing Symantec High Availability Console, refer to <i>Symantec High Availability Console Installation and Upgrade Guide</i>.</p>
Install ApplicationHA guest components	<p>Install ApplicationHA guest components on the virtual machines where you want to configure application monitoring.</p> <p>For more details on installing the ApplicationHA guest components refer to the <i>Symantec™ ApplicationHA Installation and Upgrade Guide</i>.</p>

Table 2-1 Tasks for setting up ApplicationHA in a VMware SRM 5.1 environment (*continued*)

Task	Details
Configure single sign-on (SSO) at protected site	<p>Configure SSO between the protected site Console and the protected site virtual machines.</p> <p>SSO configuration involves specifying the virtual machine administrator account to set up a permanent authentication for the virtual machine.</p> <p>Single sign-on authentication is used for all operations on the virtual machine. This is also required so that the server does not prompt you for a user name and password each time you log on to the vSphere Client and click on a virtual machine to view its status.</p>
Install hotfix <i>Hotfix_6_0_7_3274237a</i>	<p>You can download the hotfix from the following location: https://sort.symantec.com/patch/detail/7850</p> <p>Install the hotfix on all the virtual machines (at the protected site) where you want to configure application monitoring.</p> <p>This hotfix provides scripts that retrieve the application status during site recovery.</p> <p>During site recovery when the virtual machines fail over to the recovery site the ApplicationHA recovery command from the SRM recovery plan invokes the scripts on the virtual machines to retrieve the application status. The application status is then displayed in the SRM history status report.</p> <p>For more details on installing the hotfix refer to the <i>README</i> that is downloaded along with the hotfix binaries.</p>
Configure SSO between the recovery site Console and the protected site virtual machines	<p>From the Console at the recovery site, launch the Symantec ApplicationHA SRM Components Configuration Wizard.</p> <p>Use this wizard to configure single sign-on between the virtual machines at the protected site and the Console at the recovery site.</p> <p>This configuration is used for all operations on the virtual machines when they fail over to the recovery site.</p> <p>See “Configuring single sign-on between recovery and protected site” on page 13.</p>

Table 2-1 Tasks for setting up ApplicationHA in a VMware SRM 5.1 environment (*continued*)

Task	Details
Modify the SRM recovery plan	<p>After you have configured SSO between the recovery site Console and the protected site virtual machines, you must modify the SRM recovery plan to define the action for application monitoring continuity.</p> <p>This action is defined in a form of an ApplicationHA recovery command that must be added to the SRM recovery steps, in an appropriate sequence.</p> <p>See “Modifying the SRM recovery plan” on page 15.</p>

Configuring single sign-on between virtual machine and Console

SSO configuration involves specifying the virtual machine administrator account to set up a permanent authentication for the virtual machine.

Use the ApplicationHA tab to manually configure single sign-on between the virtual machine and the Console host.

You are required to manually configure the single sign-on during the following cases:

- SSO configuration has failed during the guest installation or upgrade
- You have not configured SSO during the guest installation or upgrade
- You have installed or upgraded the guest components using the CLI

Note: Symantec ApplicationHA uses platform-based authentication; it does not store user passwords.

Console server uses the Symantec ApplicationHA Authentication service to provide secure communications between the virtual machine and the Console. It uses digital certificates for authentication and uses SSL to encrypt communications.

This single sign-on authentication is used for all operations on the virtual machine. This is also required so that the server does not prompt you for a user name and password each time you log on to the vSphere Client and click on a virtual machine to view its status.

Perform the following steps to configure the single sign-on for the virtual machines.

To configure single sign-on for the virtual machines

- 1 Launch the vSphere Client and connect to the vCenter Server used to manage your virtual machines.
- 2 On the Security Warning dialog that displays information about the Console certificate, perform the following:
 - Select the option to install the certificate.
 - Click **Ignore**.

If you do not install the Console certificate, this dialog pops up each time you log on to the vCenter Server using the vSphere Client.

- 3 Open the Hosts and Clusters view in the vSphere Client and then expand the Cluster to display the list of virtual machines.
- 4 From the left pane select a virtual machine where you installed ApplicationHA guest components and then in the right pane select the **ApplicationHA** tab.
- 5 Click **Yes** on the security certificate related dialog box, if displayed.
- 6 In the User Name and Password field, specify the credentials of a user that has administrative privileges on the virtual machine.
- 7 Click **Configure**.

The Console uses the specified user account to set up a permanent authentication for the virtual machine.

After the authentication is successful, the ApplicationHA tab refreshes and displays the application configuration view.

- 8 Repeat these steps for all virtual machines where you wish to configure application monitoring.

Configuring single sign-on between recovery and protected site

Use the Symantec ApplicationHA SRM Components Configuration Wizard to configure single sign-on between the recovery and the protected site. You must launch this configuration wizard from the Console host at the recovery site.

Before you begin to configure SSO, ensure that you meet the following points:

- ApplicationHA guest components are installed and SSO is configured between the Console and the virtual machines on the protected site.
- The vCenter logged-on user has ApplicationHA administrator privileges on the virtual machines at the protected site.

- The https port used by the VMware Web Service is enabled for inbound and outbound communication. The default port is 443.
- The https port used by Veritas Storage Foundation Messaging Service (xprtld) is enabled for inbound and outbound communication. The default port is 5634.
- The Console host at the recovery site can access the vCenter Server and the Console host at the protected site.
- The virtual machines can access the Console host at both the sites.
- The virtual machines can access the Console host at recovery site using the fully qualified host name.
- The clock times on the protected site virtual machines and the recovery site Console are within 30 minutes of one another.
- The following services are running on the Console hosts at both the sites:
 - Symantec ApplicationHA Service
 - Veritas Storage Foundation Messaging Service (xprtld)
 - Symantec Authentication Service
- Ports 5634, 14152, and 14153 are not blocked by a firewall on the Console hosts and the virtual machines.

To configure single sign-on for the virtual machines

- 1 On the recovery site, using the vSphere Client, connect to the vCenter Server and navigate to **Home > Solutions and Applications > Symantec ApplicationHA**
- 2 On the Symantec ApplicationHA home page, click the **Disaster Recovery** tab.
- 3 On the Disaster Recovery tab, click **Configure Single Sign-on**.
 This launches the Symantec ApplicationHA SRM components configuration wizard.
- 4 Review the prerequisites on the Welcome panel and then click **Next**.
- 5 On the ApplicationHA Inputs panel, specify the required details of the ApplicationHA Console and the vCenter Server at the protected site.
 The installer uses these details to set up a link with the protected site vCenter Server and the ApplicationHA Console. This link enables communication with the guest virtual machines at the protected site.
- 6 On the System Selection panel, select the virtual machines for configuring single sign-on.
 All the vCenter virtual machines are listed.

- 7 The Implementation panel displays the SSO configuration progress for each virtual machines. After the configuration process is complete, click **Next**.

If the configuration has failed on any of the machine, refer to the log files for details.

The log file is located on the protected site ApplicationHA Console at the following location:

- For virtual machines running Windows Server 2008 or 2008 R2 operating system
%AllUsersProfile%\Symantec\ApplicationHA\Logs
- For virtual machines running Windows Server 2003 operating system
%AllUsersProfile%\Application Data\Symantec\ApplicationHA\Logs

You may have to rectify the cause and repeat the configuration on the failed machines.

- 8 On the Finish panel, click **Finish**.

This completes the SSO configuration between the virtual machines at the protected site and the Console at the recovery site.

During a disaster, to ensure application monitoring continuity at the recovery site, proceed to update the VMware SRM recovery plan.

See [“Modifying the SRM recovery plan”](#) on page 15.

Modifying the SRM recovery plan

After you have configured SSO between the recovery site Console and the protected site virtual machines, you must modify the SRM recovery plan to define the action for application monitoring continuity. This action is defined in a form of an ApplicationHA recovery command that must be added to the SRM recovery steps, in an appropriate sequence. You must define this command for virtual machines in the SRM Recovery Plan.

Following is a sample ApplicationHA recovery command that defines the action for application monitoring continuity.

```
C:\Windows\system32\cmd.exe /c "c:\program files\Veritas\cluster server\portal\admin\getappstatus.bat"
```

To add the ApplicationHA recovery command for a single virtual machine

- 1 On the recovery site, using the vSphere client connect to the vCenter Server and navigate to **Home > Solutions and Applications > Site Recovery**.
- 2 From the tree view, select the desired recovery plan and select the **Virtual Machines** tab.
- 3 On the desired virtual machine, right click and select **Configure**.
- 4 On the VM Recovery Property, select **Post Power On Steps** and then click **Add**.
- 5 On the Edit Post Power on Steps for this VM panel, select **Command on Recovered VM** and perform the following:
 - Specify the ApplicationHA command step name in the **Name** text box.
 - Specify the ApplicationHA command in the **Content** text box.
 - Click **OK**
- 6 On the VM Recovery Property, click **OK**.

This adds the ApplicationHA recovery command to the SRM recovery plan.

Repeat these steps for all the virtual machines included in the SRM recovery plan.