Symantec™ Cluster Server 6.1 Generic Application Agent Configuration Guide - Linux

January 2014

Symantec™ Cluster Server 6.1 Generic Application Agent Configuration 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 2

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 High Availability solution

This chapter includes the following topics:

How the Symantec High Availability solution works

The Symantec High Availability solution employs Symantec Cluster Server (VCS) and its agent framework to monitor the state of the applications and their dependent components running on physical or virtual machines. The Symantec High Availability Configuration wizard can also be used to configure applications that use active-passive storage. An active-passive storage can access only one node at a time. This solution uses various agents to monitor the application, storage, and networking components. These agents monitor the overall health of the configured applications by running specific commands, tests, or scripts.

In VMware environment, the application data can be stored in Virtual Machine Disk (VMDK) or Raw Disk Mapping (RDM) disks that may reside on a shared datastore. This datastore may be accessible to multiple virtual machines. However, in Symantec High Availability configuration, the disks are attached to a single virtual machine at any given point of time. The storage failover is managed by a new agent named VMwareDisks. During application failover, this agent detaches the disks from one virtual machine and attaches the same to another virtual machine.

For details on the storage agents, refer to the *Symantec Cluster Server Bundled Agents Reference Guide*.

In event of an application failure, the agents attempt to restart the application services and components for a configurable number of times. If the application fails to start, the Symantec High Availability solution initiates application failover to the failover target system. During the failover, the storage agents bring the storage components online and the application-specific agents then start the application services on the failover target system.

For details on the VCS configuration concepts and clustering topologies, refer to the *Symantec Cluster Server Administrator’s Guide*.

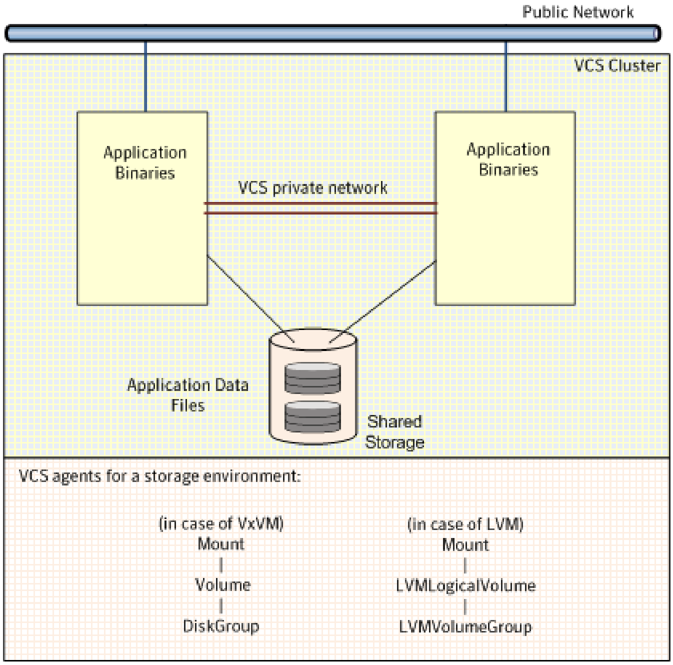
For details on a particular application agent, refer to the application-specific agent guide.

Typical VCS cluster configuration in a physical environment

A typical VCS cluster configuration in a physical environment involves two or more physical machines.

The application binaries are installed on a local or shared storage and the data files should be installed on a shared storage. The VCS agents monitor the application components and services, and the storage and network components that the application uses.

Figure 1-1 Typical generic applications cluster configuration in a physical environment



During a fault, the VCS storage agents fail over the storage to a new system. The VCS network agents bring the network components online and the application-specific agents then start application services on the new system.

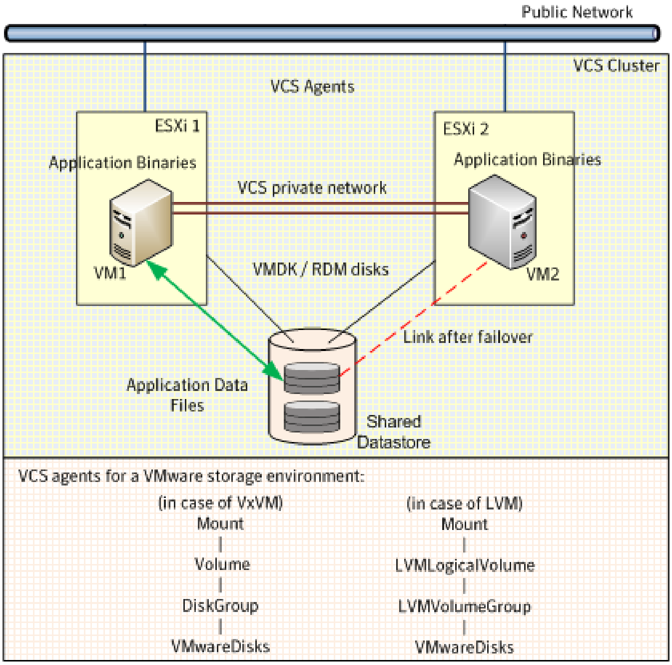
Typical VCS cluster configuration in a virtual environment

A typical VCS cluster configuration in a VMware virtual environment involves two or more virtual machines. The virtual machine on which the application is active, accesses a non-shared VMware VMDK, or RDM disk that resides on a VMware datastore.

The virtual machines involved in the VCS cluster configuration may belong to a single ESX/ESXi host or could reside on separate ESX/ESXi hosts. If the virtual machines reside on separate ESX/ESXi hosts, the datastore on which the VMware VMDK or RDM disks (on which the application data is stored) reside must be accessible to each of these ESX/ESXi hosts.

The application binaries are installed on the virtual machines and the data files are installed on the non-shared VMDK or RDM disk. The VCS agents monitor the application components and services, and the storage and network components that the application uses.

Figure 1-2 Typical generic applications cluster configuration in a VMware virtual environment



During a failover, the VCS storage agents move the VMware disks to the new system. The VCS network agents bring the network components online and the application specific agents then start application services on the new system.

About the Application agent

This chapter includes the following topics:

About Generic Application

A generic application is an application which can be configured by defining:

- Start program
- Stop program
- (Optional) Force stop program
- One or more monitoring options like monitor program, list of processes, or process ID files

You can use VCS Application agent to ensure high availability of a generic application.

If an application-specific VCS agent exists, Symantec recommends the use of the specialized agent for monitoring availability. In other cases, Symantec recommends the use of the VCS Application agent.

About the Application agent for generic applications

The Application agent is a VCS bundled agent. This means that, when you install VCS on a physical or virtual machine, the VCS Application agent is automatically installed on that machine.

The VCS Application agent can be used to perform online, offline and monitor operations. Use it to specify different executables for the online, offline, and monitor routines for the different applications.

An application runs in the default context of root.

You can monitor the application in the following ways:

- Use the monitor program
- Specify a list of processes
- Specify a list of process ID files
- Any combination of the above

The Application agent is IMF-aware and uses asynchronous monitoring framework (AMF) kernel driver for IMF notification.

For more information about the VCS Application agent, including descriptions of the agent functions and attributes, see the *Symantec Cluster Server Bundled Agents Reference Guide*.

For more information about the IMF, refer to the *Symantec Cluster Server Administrator's Guide*.

Chapter 3

Configuring application monitoring for generic applications

This chapter includes the following topics:

About configuring application monitoring using the Symantec High Availability solution

Consider the following before you proceed:

- You can configure application monitoring using the Symantec High Availability Configuration wizard. In VMware environment, click **Configure application for high availability** on the **Symantec High Availability** tab to launch the wizard in the VMware vSphere Client. You can also launch the wizard through Veritas Operations Manager (VOM) UI.
- Apart from the Symantec High Availability Configuration wizard, you can also configure application monitoring using the VCS commands. For more information, refer to the *Symantec Cluster Server Administrator's Guide*.

- 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 configuring application availability, the wizard also sets up the other components required for successful application monitoring.
- In VMware environment, you must not suspend a system if an application is currently online on that machine. If you suspend a system, VCS moves the disks along with the application to another system. Later, when you try to restore the suspended system, VMware does not allow the operation because the disks that were attached before the system was suspended are no longer with the system.

Note: For details about deploying, configuring, and administering the Symantec High Availability solution in VMware environment, refer to the *Symantec High Availability Solutions Guide for VMware*.

Before configuring monitoring for generic applications

Ensure that you complete the following tasks before configuring monitoring for generic applications:

- Install Symantec Cluster Server on the physical or virtual machine on which you want to configure the application for monitoring.
- If you are going to launch the wizard from VOM, ensure that the cluster has been configured and running.
- Assign the following privileges to the logged-on user where you want to configure application monitoring:
  - When wizard is launched through vSphere client, assign **Configure Application Monitoring (Admin)** privileges.
  - When wizard is launched through VOM, the logged-on user group must be assigned the Admin role on the cluster or on the Availability perspective.
    The permission on the cluster may be explicitly assigned or inherited from a parent Organization.
- Install the application and the associated components that you want to monitor on the physical or virtual machine.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec Cluster Server installer, wizards, and services.
  Verify that the following ports are not blocked by a firewall:

VMware environment	443, 5634, 14152, and 14153
Physical environment	5634, 14161, 14162, 14163, and 14164

Note: In the physical environment, ensure that at least one of the following ports 14161, 14162, 14163, or 14164 is kept open.

- You must not select bonded interfaces for cluster communication. A bonded interface is a logical NIC, formed by grouping several physical NICs together. All NICs in a bond have an identical MAC address, due to which you may experience the following issues:
  - SSO configuration failure.
  - The wizard may fail to discover the specified network adapters.
  - The wizard may fail to discover or validate the specified system name.
- In VMware environment, verify that the disks used by the application that you want to monitor are attached to non-shared controllers so that they can be detached from the system and attached to another system.
- If you want to configure the storage dependencies of the application through the wizard, the LVM volumes or VxVM volumes used by the application should not be mounted on more than one mount point path.
- The host name of the system must be resolvable through the DNS server or locally, using `/etc/hosts` file entries.
- To review the information about the functions, attributes, and resource type definition of the VCS Application agent, refer to the *Symantec Cluster Server Bundled Agents Reference Guide*.
- If your application uses storage mount points, you must ensure that those mount points are already mounted on the physical or virtual machine from which you are configuring the application for monitoring. All the required disks must be attached and all the storage components must be available. You must launch the Symantec High Availability Configuration Wizard from the physical or virtual machine on which the application is running. The wizard discovers the disks that are attached and the storage that is currently available.

Ensure that you complete the following task if you are configuring monitoring of generic applications through VOM:

- Configure the cluster through CPI installer or manually. The wizard option is available in VOM only after the cluster is configured and running.

Ensure that you complete the following additional tasks if you are configuring monitoring for generic applications on a virtual machine:

- Verify that the boot sequence of the virtual machine is such that the boot disk (OS hard disk) is placed before the removable disks. If the sequence places the removable disks before the boot disk, the virtual machine may not reboot after an application failover. The reboot may halt with an `OS not found error`. This issue occurs because during the application failover, the removable disks are detached from the current virtual machine and are attached to the failover target system.
- Install and enable VMware Tools on the virtual machine where you want to monitor applications with VCS. Install a version that is compatible with the VMware ESX/ESXi server.
- Install the VMware vSphere Client. You can configure application monitoring from the Symantec High Availability tab in the vSphere Client.

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

  `https://VMNameorIP:5634/vcs/admin/application_health.html`

  VMNameorIP is the host name or IP address of the virtual machine on which you want to configure application monitoring.
- Install Symantec High Availability Console on a Windows system in your data center and register the Symantec High Availability plug-in with the vCenter server.
- You must not restore a snapshot on a virtual machine where an application is currently online, if the snapshot was taken when the application was offline on that virtual machine. Doing this may cause an unwanted failover. This also applies in the reverse scenario; you should not restore a snapshot where the application was online on a virtual machine, where the application is currently offline. This may lead to a misconfiguration where the application is online on multiple systems simultaneously.
- While creating a VCS cluster in a virtual environment, you must configure the cluster communication link over a public network in addition to private adapters. The link using the public adapter should be assigned as a low-priority link. This helps in case the private network adapters fail, leading to a condition where the systems cannot connect to each other, consider that the other system has faulted, and then try to gain access to the disks, thereby leading to an application fault.
- You must not attach multiple types of SCSI controllers to the virtual machines because storage dependencies of the application cannot be determined and configured.

- The term ‘shared storage’ refers to the removable disks attached to the virtual machine. It does not refer to disks attached to the shared controllers of the virtual machine.
- By default, the controller ID and port must remain the same on all cluster nodes. If you do not want the resource to have the same controller ID and port, you should localize the attribute for all cluster nodes. Localization allows all cluster nodes to have different controller IDs and port numbers. For more information about localizing an attribute, refer to the *Symantec Cluster Server Administrator’s Guide*.

Launching the Symantec High Availability Configuration wizard

In VMware or physical Linux environments, you can launch the Symantec High Availability Configuration wizard using:

- Veritas Operations Manager Client: To launch the wizard from the Veritas Operations Manager Client
- haappwizard utility: To launch the wizard using the haappwizard utility

In addition, you can also launch the wizard in a VMware environment using:

- VMware vSphere Client: To launch the wizard from the VMware vSphere Client
- A browser window: To launch the wizard from a browser window

To launch the wizard from the Veritas Operations Manager Client

1. Log in to the VOM Management Server console.
2. In the VOM home page, click the **Availability** icon from the list of perspectives.
3. In the **Data Center** tree under the **Manage** pane, locate the cluster.
4. Navigate to the **Systems** object under the cluster.
5. Locate the system on which the application is running or application prerequisites are met.
6. Right-click on the system, and then click **Configure Application**.

To launch the wizard using the haappwizard utility

The haappwizard utility allows you to launch the Symantec High Availability Configuration wizard. The utility is part of the product package and is installed in the /opt/VRTSvcs/bin directory.

◆ Enter the following command to launch the Symantec High Availability Configuration wizard:

```
happwizard [-hostname host_name] [-browser browser_name] [-help]
```

The following table describes the options of the happwizard utility:

Table 3-1 Options of the happwizard utility

–hostname	Allows you to specify the host name or IP address of the system from which you want to launch the Symantec High Availability Configuration wizard. If you do not specify a host name or IP address, the Symantec High Availability Configuration wizard is launched on the local host.
-browser	Allows you to specify the browser name. The supported browsers are Internet Explorer and Firefox. For example, enter `iexplore` for Internet Explorer and `firefox` for Firefox. **Note:** The value is case-sensitive.
-help	Displays the command usage.

To launch the wizard from the VMware vSphere Client

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

   Select the Symantec High Availability tab and in the Symantec High Availability View page, specify the credentials of a user account that has administrative privileges on the virtual machine and click **Configure**.

   The Symantec High Availability console sets up a permanent authentication for the user account on that virtual machine.
4. Depending on your setup, use one of the following options to launch the wizard:
   - If you have not configured a cluster, click the **Configure application for high availability** link.

- If you have already configured a cluster, click **Actions > Configure application for high availability** or the **Configure application for high availability** link.
- If you have already configured a cluster and configured an application for monitoring, click **Actions > Configure application for high availability**.

To launch the wizard from a browser window

1. Open a browser window and enter the following URL:

   `https://`*`VMNameorIP`*`:5634/vcs/admin/application_health.html`

   VMNameorIP is the virtual machine name or IP address of the system on which you want to configure application monitoring.
2. In the Authentication dialog box, enter the username and password of the user who has administrative privileges.
3. Depending on your setup, use one of the following options to launch the wizard:
   - If you have not configured a cluster, click the **Configure application for high availability** link.
   - If you have already configured a cluster, click **Actions > Configure application for high availability** or the **Configure application for high availability** link.
   - If you have already configured a cluster and configured an application for monitoring, click **Actions > Configure application for high availability**.

Configuring application monitoring by using the Symantec High Availability Configuration wizard

To configure a generic application for monitoring by using the Symantec High Availability Configuration Wizard:

1. Launch the Symantec High Availability Configuration Wizard.
2. Review the information on the Welcome panel and click **Next**.
3. Select **Generic Application**, and then click **Next**.
4. On the Component Selection panel, enter a name for the component and click **Add Component**.

   The component you added appears in the Component box.
5. Specify the following details to configure the component for monitoring:
   - **Start program**: The complete path of the start program script.

- **Stop program**: The complete path of the stop program script.
- **Force-stop program:**: The complete path of the program script to forcefully stop the application.
- At least one or more of the following:
  - **Monitor program**: The complete path of the monitor program script.
  - **Application-related processes to monitor**: Names of the application processes that must be monitored.
  - **Application-generated PID files**: Path names of the process ID (PID) files of your application.
- **Enable intelligent monitoring for this application**: Select or clear this option to enable or disable intelligent monitoring for the application component. This option is selected by default. Symantec recommends that you enable intelligent monitoring of the application component.
- **User**: The user name. Ensure that you specify a valid user with adequate privileges on the physical or virtual machine where you configure the application. Else, application monitoring may fail.

To remove a component from the Component box, use the Remove icon.

6 To specify more application components for monitoring, repeat steps 4 and 5. Else, click **Next**.

7 On the Storage Selection panel, select the appropriate mount points for the application instances that require storage, and click **Next**.

Note: The Storage Selection panel does not appear if shared storage is not mounted on the physical or virtual machine.

---

8 On the Define Start-Stop Order panel, to define the dependency between the components, select an application component from the **Parent Component** box and then select the components that it depends on from the **Depends on** box. When starting the application, the components are brought online in the defined order.

Note: The Define Start-Stop Order panel appears only when you have added more than one component for monitoring.

---

9 Click **Next**.

10 Skip this step if you have launched the wizard through VOM.

On the Configuration Inputs panel, use the Edit icon to specify the user name and password of the systems for the VCS cluster operations.

11 Move the required systems to the **Application failover targets** list. Use the up and down arrow keys to define the priority order of the failover systems.

- **Cluster systems** lists the systems included in the cluster configuration.
- **Application failover targets** lists the systems to which the application can fail over.

12 If you have launched the wizard through VOM, go to step 17.

13 Skip this step if you do not want to add more systems to your cluster.

To add a system to the cluster, on the Configuration Inputs panel, click **Add System**. In the Add System dialog box, specify the following details of the system that you want to add to the VCS cluster and click **OK**:

System Name or IP address	Specify the name or IP address of the system that you want to add to the VCS cluster.
User name	Specify the user account for the system. Typically, this is the root user.
Password	Specify the password for the user account mentioned.
Use the specified user account on all systems	Select to use the specified user account on all those cluster systems that have the same user name and password.

The wizard validates the details, and the system then appears in the Cluster Systems list.

To remove a system from the cluster or from the Application failover targets list, use the Remove icon.

14 Skip this step if you do not want to modify the default security settings for your cluster.

If you want to modify the security settings for the cluster, click **Advanced Settings**. In the Advanced settings dialog box, specify the following details and click **OK**.

Use single sign-on authentication	Select to configure single sign-on using VCS Authentication Service for cluster communication. This option is enabled by default.
Use VCS user privileges	Select to configure a user with administrative privileges to the cluster. Specify the username and password and click **OK**.

Note: The **Advanced Settings** link is not visible if the cluster is already created.

---

15 Click **Next**.

16 On the Network Details panel, select the type of network protocol to configure the VCS cluster network links and then specify the adapters for network communication. By default, the links are configured over Ethernet.

Note: Symantec recommends that one of the network adapters must be a public adapter. You may assign low priority to the VCS cluster communication link that uses the public adapter.

Depending on the network over which you want to configure the links, select one of the following:

- **Use MAC address for cluster communication (LLT over Ethernet)** : Select the adapter for each network communication link. You must select a different network adapter for each communication link. This communication type configures the links over the non-routed network. Choose this mode only if the failover target systems reside in the same subnet.
- **Use IP address for cluster communication (LLT over UDP)**: Select the type of IP protocol and then specify the required details for each communication link. This communication type configures the links over the routed network. Choose this mode if the failover target systems reside in the same or different subnets. The adapters that you select must have an IP address. Symantec recommends that the IP address assigned to these adapters should be in different subnets.

Select the IP protocol (IPv4 or IPv6) and then specify the following:

Network Adapter	Select a network adapter for the communication links. You must select a different network adapter for each communication link.
IP Address	Specify the IP address for cluster communication over the specified UDP port.
Port	Specify a unique port number for each link. You can use ports in the port range 49152 to 65535. A specified port for a link is used for all the cluster systems on that link.
Subnet mask (IPv4)	Displays the subnet mask details.
Prefix (IPv6)	Displays the prefix details.

By default, one of the links is configured as a low-priority link on a public network interface. The second link is configured as a high-priority link. To change a high-priority link to a low-priority link, click **Modify**. In the Modify low-priority link dialog box, select the link and click **OK**.

17 Click **Next**.

18 Skip this step if you do not want to specify a virtual IP address for the application component.

On the Virtual Network Details panel, select the IP network (IPV4 or IPv6). The IPv4 protocol is selected by default.

Select the appropriate component and specify the following details for each failover system:

Virtual IP address	Specify a unique virtual IP address. You can specify only one virtual IP address for each component.
Subnet Mask (for IPv4)	Specify the subnet mask details.
Prefix (for IPv6)	Select the prefix details.
Network Adapter	Select the network adapter that will host the virtual IP.

If you want to add another virtual IP address, click **Add virtual IP address**.

19 Click **Next**.

20 This step is not applicable if you are configuring application monitoring on a physical Linux machine.

If you selected mount points for your application in step 7, the Storage HA Inputs panel appears.

On the Storage HA Inputs panel, specify all the ESX/ESXi hosts to which virtual machines can fail over. Each ESX/ESXi host must be able to access the required shared datastores that contain visible disks.

To specify the ESX/ESXi hosts, click **Add ESX/ESXi Host** and in the Add ESX/ESXi Host dialog box, specify the following details and click **OK**:

ESX/ESXi hostname or IP address	Specify the target ESX/ESXi hostname or IP address. The virtual machines can fail over to this ESX/ESXi host during vMotion. All the additional ESX/ESXi hosts should have access to the datastore on which the disks used by the application reside.
User name	Specify a user account for the ESX/ESXi host. The user account must have administrator privileges on the specified ESX/ESXi host.
Password	Specify the password for the user account provided in the User name text box.

The wizard validates the user account and the storage details on the specified ESX/ESXi hosts.

If you want to remove an ESX/ESXi host, use the Remove icon.

21 Click **Next**.

22 On the Summary panel, review the configuration details information and then click **Next** to proceed with the configuration.

You can skip the below process if a cluster has been already configured.

If the network contains multiple clusters, the wizard verifies the cluster ID with the IDs assigned to all the accessible clusters in the network. The wizard does not validate the assigned ID with the clusters that are not accessible during the validation.

Note: Symantec recommends that you to validate the uniqueness of the assigned ID in the existing network. If the assigned ID is not unique or if you want to modify the cluster name or cluster ID, click **Edit**. In the Edit Cluster Details dialog box, modify the details as necessary and click **OK**. This function is not applicable if the cluster is already configured, and also when you launch the wizard through VOM.

---

23 On the Implementation panel, the wizard performs the following tasks:

- Creates the VCS cluster if not already created
- Configures the application for monitoring
- In VMware environment, creates cluster communication links

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

If a configuration task fails, click **Diagnostic information** to check the details of the failure. Rectify the cause of the failure and run the wizard again to configure application monitoring.

24 Click **Next** and then click **Finish** to complete the wizard workflow.

This completes the application monitoring configuration.

Note: In VMware environment, if the application status shows as not running, click **Start** to start the configured components on the system.

Appendix A

Sample configurations

This appendix includes the following topics:

- Sample configuration for an init process and generic application component
- Infrastructure service groups

Sample configuration for an init process and generic application component

This section describes a sample procedure for using the Symantec High Availability Configuration wizard launched through VMware vSphere client.

To configure monitoring for the following across two virtual machines—Machine1 and Machine2:

- an init process, such as CUPS
- a generic application, MyApplication

As part of the configuration process, the wizard configures a 2-node cluster between the machines Machine1 and Machine2 running on hosts—Host1 and Host2, respectively.

Let us assume that the generic application (MyApplication) can be started, stopped, monitored, and forcibly stopped by using the following scripts, respectively:

- `start_MyComponent`
- `stop_MyComponent`
- `monitor_MyComponent`

  The `monitor_MyComponent` script is written to comply with the MonitorProgram attribute of generic applications. For more information, see the description of the Application agent attributes in the *Symantec Cluster Server Bundled Agents Reference Guide*.

- `forcestop_MyComponent`

To configure application monitoring using the Symantec High Availability Configuration wizard

1. Launch the Symantec High Availability Configuration wizard.
2. Review the information on the Welcome panel and click **Next**.
3. Select **Generic Application**, and then click **Next**.
4. On the Component Selection panel, enter a name for the CUPS process, for example, cups_Program and click **Add Component**.

   The component you added (cups_Program) appears in the Component box.
5. Specify the following details to configure the cups_Program for monitoring:

Start program	*/etc/init.d/cups start*
Stop program	*/etc/init.d/cups stop*
Force-stop program	*Not specified*
Monitor program	*/etc/init.d/cups status* **Note:** init processes such as CUPS, do not require special monitor scripts. VCS uses the status option of the init script for monitoring. However you can also use your own program scripts to monitor such processes.
Application-related processes to monitor	*cupsd -C /etc/cups/cupsd.conf*
Application-generated PID files	*/var/run/cupsd.pid*
Enable intelligent monitoring for this application	Selected by default to enable intelligent monitoring
User	*username*. For example, root.

   Note: You must specify at least one or more of the following: Monitor program, application-related processes to monitor, application-generated PID files.

6. To configure MyApplication for monitoring, add a name for the MyApplication component, for example, MyComponent and click **Add Component**.

   The component you added (MyComponent) appears in the Component box.

7 Specify the following details to configure MyComponent for monitoring:

Start program	`/myapplication/bin/start_MyComponent`
Stop program	`/myapplication/bin/stop_MyComponent`
Force-stop program	`/myapplication/bin/forcestop_MyComponent`
Monitor program	`/myapplication/bin/monitor_MyComponent`
Application-related processes to monitor	*Not specified*
Application-generated PID files	*Not specified*
Enable intelligent monitoring for this application	Selected by default to enable intelligent monitoring
User	*username*. For example, root.

8 Click **Next**.

9 If the MyApplication application requires storage, on the Storage Selection panel, select the appropriate mount points and click **Next**.

10 On the Define Start-Stop Order panel, you can define the relationship between the CUPS process and MyApplication.

To bring the CUPS process online first and then MyApplication, in the **Parent Component** list, select ***MyComponent*** and in the **Depends on** box, select ***cups_Program***.

11 Click **Next**.

12 On the Configuration Inputs panel, the wizard lists Machine1—the machine from which you launched the wizard. The wizard also lists Machine1 in the Application failover targets list. To add Machine2 to the cluster, click **Add System**, and in the Add System dialog box, specify the following details for Machine2:

System Name or IP address	*Machine2*
User name	*username* Typically, this is the root user.
Password	*password*
Use the specified user account on all systems	Select to use the specified user account on all the cluster systems.

13 Click **Next**.

14 On the Network Details panel, select **Use MAC address for cluster communication (LLT over Ethernet)**. Specify two adapters for each machine

15 Click **Next**.

16 On the Virtual Network Details panel, select ***MyComponent***, and then select **IPv4** and specify the following details for each failover system:

Virtual IP address	*IP address*
Subnet Mask	*Subnet mask*
Network Adapter	For Machine1: *eth0* For Machine2: *eth1*

17 Click **Next**.

18 This step is applicable only if you are configuring application monitoring on a VMware virtual machine.

On the Storage HA Inputs panel, click **Add ESX/ESXi Host** to add details of ESXHost1. In the Add ESX/ESXi Host dialog box, specify the following details and click **OK**:

ESX/ESXi hostname or IP address	*ESXHost1*
User name	*esxhostuser1*
Password	*password*

The wizard validates the user account and the storage details on the specified ESX/ESXi hosts.

19 This step is applicable only if you are configuring application monitoring on a VMware virtual machine.

Click **Add ESX/ESXi Host** to add details of ESXHost2. In the Add ESX/ESXi Host dialog box, specify the following details and click **OK**

ESX/ESXi hostname or IP address	*ESXHost2*
User name	*esxhostuser2*
Password	*password*

20 Click **Next**.

21 On the Summary panel, review the VCS cluster configuration summary and then click **Next** to proceed with the configuration.

22 On the Implementation panel, the wizard creates the cluster, configures application monitoring, and creates cluster communication links. The wizard displays the status of each task. After all the tasks are complete, click **Next**.

23 Click **Finish** to complete the wizard workflow.

This completes the application monitoring configuration.

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

Infrastructure service groups

This section is applicable only if you are configuring application monitoring on a VMware virtual machine.

As part of configuring the application, the Symantec High Availability Configuration wizard:

- Configures application specific service groups and resources.
- Configures the VCS infrastructure service group (VCSInfraSG).

VCSInfraSG includes a resource called VCSNotifySinkRes. The type of this resource is Process. VCSNotifySinkRes configures and administers the notify_sink process on the guest. The notify_sink process sends the details about service groups and its attributes to the Symantec High Availability Console. This information is used for reporting purpose and is displayed on the Dashboard.

Note: VCSInfraSG is an internal service group. You must not add or delete resources from this service group.

The following are the VCSInfraSG notes:

- Before you configure the application for monitoring, ensure that SSO is configured between the Symantec High Availability Console and the guest. If SSO is not configured, VCSInfraSG fails to come online.
- If VCSInfraSG or VCSNotifySinkRes faults, ensure that SSO is configured between the Symantec High Availability Console and the guest. Clear the faults and bring the resource online again.
- VCSInfraSG or VCSNotifySinkRes must not be taken offline because it affects the information displayed on the Dashboard.

Sample scripts for generic application

This appendix includes the following topics:

Sample scripts to start, stop, and monitor a generic application

You can write your own scripts for the VCS Application agent to bring a generic application online, take the application offline, and monitor the status of the application.

You can also modify the following sample scripts and use them to start, stop, and monitor the application.

- Sample script to start a generic application:

  ```
  #!/bin/sh
  touch /tmp/sampleapp # add any steps, if required
  exit 0
  ```

  You can modify the sample start script to suit the application requirements. If you save the start script with the name startsampleapp, then to bring the application online, the agent function runs the following command:

  ```
  su - user -c startsampleapp
  ```

- Sample script to stop a generic application:

```
#!/bin/sh
rm -f /tmp/sampleapp # add any steps, if required
exit 0
```

You can modify the sample stop script to suit the application requirements. If you save the stop script with the name stopsampleapp, then to bring down the application, the agent function runs the following command:

```
su - user -c stopsampleapp
```

Note: The value of the return code for the start and stop scripts must be 0. No other return codes are supported.

- Sample script to monitor a generic application:

```
#!/bin/sh
APPLICATION_IS_ONLINE=110
APPLICATION_IS_OFFLINE=100
if [ -f /tmp/sampleapp ] ; then # add any steps, if required
exit $APPLICATION_IS_ONLINE
else
exit $APPLICATION_IS_OFFLINE
fi
```

If you save the monitor script with the name monitorsampleapp, then to monitor the application, the agent function runs the following command:

```
su - user -c monitorsampleapp
```

About the monitor script exit codes

Custom monitor scripts use exit codes to let VCS know the status of the resource or process that is being monitored. The values that VCS expects as return values are:

- 1 or 100 - indicates that the resource is offline.
- 101 to 109 - indicates that the resource is online and has a confidence level of less than 100.
- 0 or 110 - indicates that the resource is online and has a confidence level of 100.

If the exit value returned is not one of the values listed above, then the status is considered unknown (typically a value of 99 is used).