Symantec™ High Availability Solution Guide for Custom Application in VMware Environment

Windows

6.1

December 2014



Symantec™ High Availability Solution Guide for Custom Application in VMware Environment

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 0

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

About Symantec Connect

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

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

Documentation

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

doc_feedback@symantec.com

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

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

Contents

Technical Support 4

Chapter 1 Introducing the Symantec High Availability solution for VMware 10

How the Symantec High Availability solution works in a VMware environment 10
How the VMwareDisks agent communicates with the vCenter Server instead of the ESX/ESXi host 12
Typical VCS cluster configuration in a virtual environment 13
Supported VMware versions 14
Managing storage 15

Chapter 2 Configuring application high availability- Local site VMware environment 16

About setting up the Symantec High Availability solution– Local site VMware environment 16
About configuring application monitoring with Symantec High Availability solution for VMware 18
Before configuring application monitoring 21
Assigning privileges for non-administrator ESX/ESXi user account 22
Configuring application monitoring 25
Configuring the VCS cluster 26
Configuring the application 37
Modifying the ESXDetails attribute 52

Chapter 3 Configuring application high availability- VMware SRM environment 54

About setting up the Symantec High Availability solution– VMware SRM environment 55
Prerequisites 57
Encrypting the recovery site vCenter Server password 58
Configuring SSO between the protected and the recovery site 60
Updating the SRM recovery plan 61

Encrypting the ESX password 63
Modifying the attributes for the application and its component dependency group 64
Copying the script files 65
Configuring the SRM service 65
About executing the test recovery plan 66
Sample VCS_Site_Info.xml file 67

Chapter 4 Administering application availability 68

Administering application monitoring using the Symantec High Availability tab 68
Understanding the Symantec High Availability tab work area 69
To configure or unconfigure application monitoring 72
To start or stop applications 73
To switch an application to another system 75
To add or remove a failover system 75
To suspend or resume application monitoring 80
To clear Fault state 81
To resolve a held-up operation 81
To determine application state 82
To remove all monitoring configurations 82
To remove VCS cluster configurations 82
Administering application monitoring settings 83
Administering application availability using Symantec High Availability dashboard 84
Understanding the dashboard work area 85
Accessing the dashboard 88
Monitoring applications across a data center 89
Monitoring applications across an ESX cluster 90
Monitoring applications running on Symantec ApplicationHA guests 90
Searching for application instances by using filters 90
Selecting multiple applications for batch operations 91
Starting an application using the dashboard 91
Stopping an application by using the dashboard 92
Entering an application into maintenance mode 92
Bringing an application out of maintenance mode 93
Switching an application 93
Resolving dashboard alerts 94
Deleting stale records 95

Appendix A Troubleshooting 96

Troubleshooting application monitoring configuration issues 96
Symantec High Availability Configuration Wizard displays blank panels 96
The Symantec High Availability Configuration wizard displays the "hadiscover is not recognized as an internal or external command" error 97
Running the 'hastop –all' command detaches virtual disks 97
Troubleshooting Symantec High Availability tab view issues 97
Tab displays only HAD-related error and Unconfigure VCS Cluster link 97
An alert icon appears in the Symantec High Availability tab 98
High Availability tab not visible from a cluster node 98
Symantec High Availability tab does not display the application monitoring status 99
Symantec High Availability tab may freeze due to special characters in application display name 99
In the Symantec High Availability tab, the Add Failover System link is dimmed 100
Troubleshooting dashboard issues 100
Task-specific panels launched from dashboard, do not display description for alerts 100
Reporting on the Dashboard 100
About error logging- VMware SRM environment 101
All VCS cluster systems fail to start at the same time- VMware SRM environment 101

Chapter 1

Introducing the Symantec High Availability solution for VMware

This chapter includes the following topics:

- How the Symantec High Availability solution works in a VMware environment
- Supported VMware versions
- Managing storage

How the Symantec High Availability solution works in a VMware environment

The Symantec High Availability solution for VMware employs Symantec Cluster Server (VCS) and its agent framework to monitor the state of applications and their dependent components running on the virtual machines that use non-shared storage. Specific agents are available to monitor the application, storage, and network components. Together, these agents monitor the overall health of the configured applications by running specific commands, tests, or scripts.

The storage configuration in the VMware virtual environment determines how VCS functions differently in a non-shared virtual environment. The non-shared storage configuration in the VMware virtual environment involves the VMware VMDK and RDM disks that reside on the shared datastore. This datastore is accessible to multiple virtual machines. However, the disks are attached to a single virtual machine at any given point of time. VCS provides a new storage agent “VMwareDisks” that communicates with the VMware ESX/ESXi hosts to perform the disk detach and

attach operations to move the storage disk between the virtual machines, in a VCS cluster.

Note: By default the VMwareDisks agent communicates with the ESX/ESXi host to perfom the disk deatch and attach operations. However, instead of the ESX/ESXi hosts you can choose to communicate with the vCenter Server to perform these operations.

See "How the VMwareDisks agent communicates with the vCenter Server instead of the ESX/ESXi host" on page 12.

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, they initiate an application fail over to the failover target system. During the fail over, the VMwareDisks agent moves the storage disk to the failover target system, the network agents bring the network components online, and the application-specific agents then start the application services on the failover target system.

In case of a virtual machine fault, the VCS agents begin to fail over the application to the failover target system. The VMwareDisks agent sends a disk detach request to the ESX/ESXi host. After the detach operation is successful, the agent proceeds to attach the disks to the new failover target system.

In a scenario where the ESX/ESXi host itself faults, the VCS agents begin to fail over the application to the failover target system that resides on another host. The VMwareDisks agent communicates with the new ESX/ESXi host and initiates a disk detach operation on the faulted virtual machine. The agent then attaches the disk to the new failover target virtual machine.

In event of a failure in a site recovery configuration, the following tasks are performed for application monitoring continuity:

- The virtual machines at the protected site are failed over to the recovery site.
- The pre-online script defined in the form of a command in the SRM recovery plan applies the specified attribute values for the application components.
- The status monitoring script retrieves the application status.
- The network agents bring the network components online and the application-specific agents 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 the application agents, refer to the application-specific agent guide.

For details on the storage agents, refer to the *VCS Bundled Agents Reference Guide*.

How the VMwareDisks agent communicates with the vCenter Server instead of the ESX/ESXi host

In addition to the ESX hosts the VMwareDisks agent can also communicate the disk deatch and attach operations with the vCenter Server to which the virtual machines belong.

In this scenario, in event of a failure, the VMwareDisks agent sends the disk detach and attach requests to the vCenter Server (instead of the ESX hosts). The vCenter Server then notifies the ESX host for these operations. Since the communication is directed through the vCenter Server, the agent successfully detaches and attaches the disks even if the ESX host and the virtual machines reside in a different network.

In a scenario where the host ESX/ESXi itself faults, the VMareDisks agent from the target virtual machine sends a request to the vCenter Server to detach the disks from the failed virtual machine. However, since the host ESX has faulted, the request to detach the disks fails. The VMwareDisks agent from the target virtual machine now sends the disk attach request. The vCenter Server then processes this request and disks are attached to the target virtual machine. The application availability is thus not affected.

See “Modifying the ESXDetails attribute” on page 52.

Limitation

The configuration of VMwareDisks agent to communicate with the vCenter Server has the following limitation:

If VMHA is not enabled and the host ESX faults, then even after the disks are attached to the target virtual machine they remain attached to the failed virtual machine. This issue occurs because the request to detach the disks fails since the host ESX itself has faulted. The agent then sends the disk attach request to the vCenter Server and attaches the disks to the target virtual machine.

Even though the application availability is not impacted, the subsequent power ON of the faulted virtual machine fails. This issue occurs because of the stale link between the virtual machine and the disks attached. Even though the disks are now attached to the target virtual machine the stale link with the failed virtual machine still exists.

Workaround

As a workaround, you must manually detach the disks from the failed virtual machine and then power ON the machine.

About the vCenter Server user account privileges

You must have the administrative privileges or must be a root user to communicate the disk detach and attach operations through the vCenter Server. If the vCenter Server user account fails to have the administrative privileges or is not a root user, then the disk detach and attach operation may fail, in event of a failure.

If you do not want to use the administrator user account or the root user, then you must create a role and add the following privileges to the created role:

- "Low level file operations" on datastore
- "Add existing disk" on virtual machine
- "Change resource" on virtual machine
- "Remove disk" on virtual machine

After you create a role and add the required privileges, you must add a local user to the created role. You can choose to add an existing user or create a new user.

Refer to the VMware product documentation for details on creating a role and adding a user to the created role.

Typical VCS cluster configuration in a virtual environment

A typical VCS cluster configuration for services, processes, and mount points, 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 host or could reside on separate ESX hosts. If the virtual machines reside on separate ESX 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 hosts.

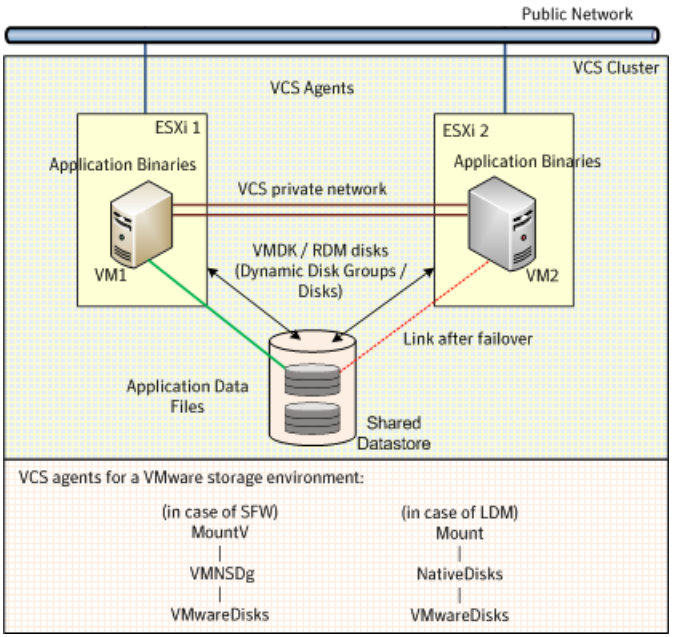
The application binaries are installed on the virtual machines and the data files are installed on the VMware disk drive. The VCS agents monitor the application components and services, and the storage and network components that the application uses.

During a failover, the VCS storage agents (MountV-VMNSDg-VMwareDisks in case of SFW storage, Mount-NativeDisks-VMwareDisks in case of LDM strorage) move the VMware disks to the new system. The VCS network agents bring the network components online, and the application-specific agents then start the application services on the new system.

In a site recovery environment, Symantec High Availability solution additionally provides script files for the following tasks. These files are invoked when the SRM recovery plan is executed.

- Set up communication between the vCenter Server and the SRM Server at the recovery site and the virtual machines at the protected site.
- Assign a SiteID to both the sites.
- Specify attribute values for the application components at the respective site.
- Retrieve the application status in the SRM recovery report, after the virtual machine is started at the recovery site.

Figure 1-1 Typical services, processes, and mount points cluster configuration in a VMware virtual environment



Supported VMware versions

For the latest list of supported VMware Servers and Management Clients refer to the software compatibilty list (SCL) at:

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

Managing storage

Configure the storage disks to save the application data.

VMware virtualization manages the application data by storing it on SAN LUNs (RDM file), or creating virtual disks on a local or networked storage attached to the ESX host using iSCSI, network, or Fibre Channel. The virtual disks reside on a datastore or a raw disk that exists on the storage disks used.

For more information, refer to the VMware documentation.

The application monitoring configuration in a VMware environment requires you to use the RDM or VMDK disk formats. During a failover, these disks can be deported from a system and imported to another system.

Consider the following to manage the storage disks:

- Use a networked storage and create virtual disks on the datastores that are accessible to all the ESX servers that hosts the VCS cluster systems.
- In case of virtual disks, create non-shared virtual disks (Thick Provision Lazy Zeroed).
- Add the virtual disks to the virtual machine on which you want to start the configured application.
- Create volumes on the virtual disks.

Note: If your storage configuration involves NetApp filers that are directly connected to the systems using iSCSI initiator, you cannot configure application monitoring in a virtual environment with non-shared disks.

The following VCS storage agents are used to monitor the storage components involving non-shared storage:

- If the storage is managed using SFW, the MountV, VMNSDg, and VMwareDisks agents are used.
- If the storage is managed using LDM, the Mount, NativeDisks, and VMwareDisks agents are used.

Before configuring the storage, you can review the resource types and attribute definitions of these VCS storage agents. For details refer to the *Symantec Cluster Server Bundled Agents Reference Guide*.

Chapter 2

Configuring application high availability- Local site VMware environment

This chapter includes the following topics:

- About setting up the Symantec High Availability solution– Local site VMware environment
- About configuring application monitoring with Symantec High Availability solution for VMware
- Before configuring application monitoring
- Configuring application monitoring
- Modifying the ESXDetails attribute

About setting up the Symantec High Availability solution– Local site VMware environment

Table 2-1 describes the tasks for setting up the Symantec High Availability solution in a VMware virtualization environment.

Table 2-1 Tasks for setting up Symantec High Availability in a VMware virtualization environment

Task	Description
Install the Symantec High Availability Console	Install the Symantec High Availability Console on a system identified to serve as a Console server. This installation registers the Symantec High Availability plugin on the vCenter Server. For more details refer to the *Symantec High Availability Console Installation and Upgrade Guide*. **Note:** If you are deploying a disaster recovery setup and plan to configure Symantec High Availability for application high availabilty, you must install the Console host at both, the protected site and the recovery site. After the installation is complete, the Symantec High Availability tab, Symantec High Availability dashboard, and the Symantec High Availability home page are added to the vSphere client. The Symantec High Availability tab is visible when you select a virtual machine from the VMware vCenter Server inventory. The Symantec High Availability dashboard is visible when you select a VMware cluster or a datacenter from the VMware vCenter Server inventory. The Symantec High Availability home page is added as an vSphere Client extension under its Solutions and Applications pane. Use the Symantec High Availability home page to perform any of the following tasks: ■ Install guest components ■ Manage licenses ■ Configure SSO for disaster recovery Use the Symantec High Availability tab to configure and control application monitoring on virtual machines that are managed from the VMware vCenter Server. You can perform these operations per virtual machine. Use the Symantec High Availability dashboard to administer the configured applications on virtual machines in a VMware cluster/datacenter. You can perform these operations at a VMware cluster or datacenter level. For details, refer to the *Symantec High Availability Console Installation and Upgrade Guide*.

Table 2-1 Tasks for setting up Symantec High Availability in a VMware virtualization environment *(continued)*

Task	Description
Install Symantec High Availability guest components	Install the Symantec High Availability guest components on all the systems where you wish to configure the application for high availability. This installs the infrastructure, application, and replication agents and the configuration wizards on the systems. For more details refer to the *Symantec High Availability Solutions Guide for VMware* **Note:** Before you install the guest components, you must install the Console.
Configure SSO	Configure single sign-on between the system where you installed the guest components and the Console host. **Note:** You need to manually configure SSO, if you have installed the guest components using the product installer or CLI. The Guest Components installer launched using the vSphere Client menu configures SSO after the guest components installation is complete. SSO provides secure communications between the system and the Console. It uses digital certificates for permanent authentication and uses SSL to encrypt communications. The single sign-on authentication is required for all VCS cluster operations on the system. It is also required so that the vCenter server does not prompt you for a user name and password each time you log on to the vSphere Client and click on a system to view the application status. For details refer to the *Symantec High Availability Solutions Guide for VMware*.
Manage storage	Configure the storage disks to save the application data. See "Managing storage" on page 15.
Configure application monitoring	Run the Symantec High Availability configuration wizard to configure application monitoring. See "About configuring application monitoring with Symantec High Availability solution for VMware" on page 18.

About configuring application monitoring with Symantec High Availability solution for VMware

Consider the following before you proceed:

- You can configure application monitoring on a virtual machine using the Symantec High Availability Configuration Wizard for VMware. The wizard is launched when you click **Configure application for high availability** on the Symantec High Availability tab in VMware vSphere Client.
  Apart from the Symantec High Availability Configuration Wizard, you can also configure application monitoring using the Symantec Cluster Server (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 the application monitoring configuration, the wizard also sets up the other components required for successful application monitoring.
- After configuring services, processes, and mount points for monitoring, if you create another service, process, or mount point, then these new components are not monitored as part of the existing configuration.
  In this case, you can either use the VCS commands to add the components to the configuration or unconfigure the existing configuration and then run the wizard again to configure all the components.
- In case the VMwareDisks agent resource is configured manually, care should be taken not to add the operating system disk in the configuration. The VMwareDisks agent does not block this operation. This might lead to a system crash during failover.
- If VMware vMotion is triggered at the same time as an application fails over, the VMwareDisks resource may either fail to go offline or may report an unknown status. The resource will eventually failover and report online after the vMotion is successful and the application is online on the target system.
- VMware snapshot operations may fail if VMwareDisks agent is configured for a physical RDM type of disk. Currently only virtual RDM disks are supported.
- Non-shared disks partitioned using GUID Partition Table (GPT) are not supported. Currently only Master Boot Record (MBR) partition is supported.
- VMwareDisks agent does not support disks attached to the virtual machine using IDE controllers. The agent resource reports an unknown if IDE type of disks are configured.
- In case VMware HA is disabled and the ESX itself faults, VCS moves the application to the target failover system on another ESX host. VMwareDisks agent registers the faulted system on the new ESX host. When you try to power on the faulted system, you may see the following message in the vSphere Client:

```
This virtual machine might have been moved or copied.
In order to configure certain management and networking features,
VMware ESX needs to know if this virtual machine was moved or copied.
If you don't know, answer "I copied it".
```

You must select “I moved it” (instead of the default “I copied it”) on this message prompt.

- 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 fail over.
  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.
- If you want to suspend a system on which an application is currently online, then you must first switch the application to a failover target system.
  If you suspend the system without switching the application, then 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.
- While creating a VCS cluster in a virtual environment, you must configure one of the cluster communication link over a public adapter in addition to the link configured over a private adapter. To have less VCS cluster communication over the link using the public adapter, you may assign it low priority. This keeps the VCS cluster communication intact even if the private network adapters fail. If the cluster communication is configured over the private adapters only, the cluster systems may fail to communicate with each other in case of network failure. In this scenario, each system considers that the other system has faulted, and then try to gain access to the disks, thereby leading to an application fault.
- VMware Fault Tolerance does not support adding or removing of non-shared disks between virtual machines. During a failover, disks that contain application data cannot be moved to alternate failover systems. Applications that are being monitored thus cannot be brought online on the failover systems.
- For cluster communication, you must not select the teamed network adapter or the independently listed adapters that are a part of the teamed NIC.
  A teamed network adapter is a logical NIC, formed by grouping several physical NICs together. All NICs in a team have an identical MAC address, due to which you may experience the following issues:
  - SSO configuration failure

- The application monitoring configuration wizard may fail to discover the specified network adapters
- The application monitoring configuration wizard may fail to discover/validate the specified system name

Before configuring application monitoring

Note the following prerequisites before configuring application monitoring:

- Verify that you have installed the Symantec High Availability console and guest components.
- 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 on the failover target system.
- 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
  ```

  A prompt for the user account details will be displayed. You must enter the system user account details.
- Verify that all the systems on which you want to configure application monitoring belong to the same domain.
- Verify that the ESX/ESXi host user account has administrative privileges or is a root user.
  If the ESX/ESXi user account fails to have the administrative privileges or is not a root user, then in event of a failure the disk deattach and attach operation may fail.

If you do not want to use the administrator user account or the root user, then you must create a role, add the required privileges to the created role and then add the ESX user to that role.

See "Assigning privileges for non-administrator ESX/ESXi user account" on page 22.

- Verify that the logged-on user has administrative privileges on the virtual machine where you want to configure application monitoring.
- If you want to monitor storage managed using Symantec Storage Foundation for Windows (SFW), ensure that the volumes and mount points are created on dynamic disk groups.
  Symantec High Availability does not support monitoring for volumes and mount points created on cluster disk groups.
- If you want to monitor the mount points, ensure that the volumes or mounts selected during configuration do not have multiple paths or drive letters assigned to it.
  The Symantec High Availability Configuration wizard fails to configure monitoring if the selected mount points or a volume has multiple drive letters or paths are assigned to it.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec High Availability installer, wizard, and services.

Assigning privileges for non-administrator ESX/ESXi user account

The application monitoring configuration in a VMware virtual environment using non-shared disks involves the VMwareDisks agent. In event of a failure, the VMwareDisks agent sends a disk detach request to the ESX/ESXi host and then attaches it to the new failover target system.

To enable the VMwareDisks agent to communicate with the ESX/ESXi host, we need to specify the ESX user account details during the application configuration workflow. This ESX user account must have the administrative privileges or should be a root user. If the ESX user account does not have these privileges, you must perform the following tasks:

- Create a role having the following privileges
  - Low level file operations
  - Add existing disk
  - Change resource
  - Remove disk

  See "Creating a role" on page 23.

- Integrate with the existing authentication mechanism
  See "Integrating with Active Directory or local authentication" on page 23.
- Add the ESX user to the created role
  See "Adding a user to the role" on page 25.

Note: If you do not want to add the existing user, you can create a new user and then add the same to the created role

See "Creating a new user" on page 24.

Creating a role

Perform the following steps to create the role

1. Using the VMware vSphere Client, log on to the ESX host, and navigate to**Home** > **Administration** > **Roles**.
2. Click **Add Role**.
3. On the Add New Role panel, specify a name for the new role. For example, "ESX/ESXi User Role for Application Monitoring".
4. In the Privileges tree, click the following check boxes to assign the required privileges:
   - **All Privileges** > **Datastore** > **Low level file operations**
   - **All Privileges** > **Virtual Machine** > **Configuration** > **Adding existing disk**
   - **All Privileges** > **Virtual Machine** > **Change resource**
   - **All Privileges** > **Virtual Machine** > **Configuration** > **Remove disk**
5. Click **Ok**.

Integrating with Active Directory or local authentication

To integrate with Active Directory or local authentication

1. Create a domain user in the Active Directory.
2. Using the VMware vSphere Client, log on to the ESX host, and navigate to**Home** > **Inventory**
3. Click the ESX host.
4. In the right pane, click **Configuration**.
5. In the Software panel, click **Authentication Services**.

6 Review the Directory Services Configuration.

If the Directory Service Type is not Active Directory, and you do not want to integrate with Active Directory, proceed to the section,

See "Adding a user to the role" on page 25.

If the Directory Service Type is not Active Directory, and you want to integrate with Active Directory, in the top right corner, click **Properties**.

7 In the Directory Service Configuration panel, from the Select Directory Service Type drop down list, select **Active Directory**.

8 In the Domain Settings area, specify the **Domain**, and click **Join Domain**.

Alternatively, configure vSphere Authentication proxy.

9 Enter the user name and password of a directory service user that has permissions to join the host to the domain, and click **OK**.

Creating a new user

You must perform this task only if you do not want to add the existing user to the created role.

Perform the following steps to create a new user

1 Using the VMware vSphere Client, log on to the ESX host, and navigate to**Home** > **Inventory**.

2 Click the ESX host.

3 In the right pane, click **Local Users & Groups**.

The Users list appears by default.

4 If the Users list is not displayed, on the View bar, click **Users**.

Alternatively, if the Users list is displayed, right-click any existing user and then click **Add**.

5 In the Add New User panel, specify a Login and Password to define a new user account.

To confirm the password, retype the password.

To define the new user account, you can also specify a descriptive User Name and user ID (UID). If you do not specify the UID, the vCenter server automatically assigns one.

6 Click **Ok**.

Adding a user to the role

To add a user to the role

1. Using the VMware vSphere Client, log on to the ESX host, and navigate to**Home** > **Inventory**.
2. Click the ESX host.
3. In the right pane, click **Permissions**.
4. In the Permissions tab, right-click the blank space, and click **Add Permission**.
5. In the Assign Permissions panel, click **Add**.
6. In the Users and Groups frame of the Select Users and Groups panel, specify the user(s) that you want to assign the new role.

   Press Ctrl and click to select multiple users, if required, and then click **Add**and click **OK**.
7. In the Assigned Role drop down list, click the new role and then click **OK**.

Configuring application monitoring

Configuring an application for monitoring involves the following tasks:

1. Configuring the VCS cluster

   This task involves selecting the virtual machines on which you want to configure monitoring and setting up the network communication links between those virtual machines.

   See “Configuring the VCS cluster” on page 26.
2. Configuring the application

   This task involves configuring the application in one of the following modes:

   - Start/stop mode on a single system: In the event of a failure, the application is restarted on a virtual machine for a configured number of times.
   - Failover mode on multiple systems: In the event of a failure, the application is first restarted on a virtual machine for a configured number of times. If the application does not restart, the virtual machine fails over to another ESX host.
     When you configure an application in the failover mode, you need to select the ESX hosts where the virtual machines can fail over.

   See “Configuring the application” on page 37.

Configuring the VCS cluster

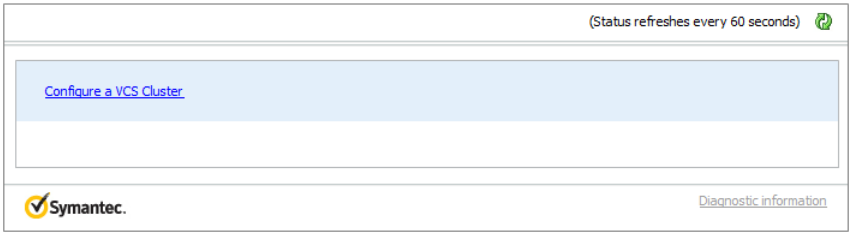
VCS cluster configuration involves selecting the virtual machines on which you want to configure monitoring and setting up the network communication links between the selected virtual machines.

To configure the VCS cluster

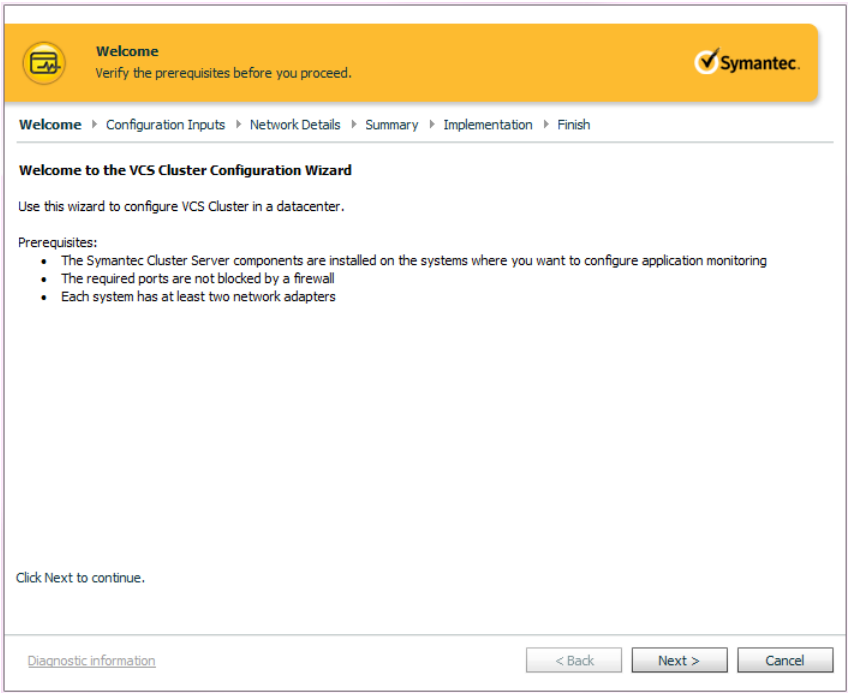
1. Launch the vSphere Client and connect to the vCenter Server that manages the virtual machine. On the Inventory view of the vCenter Server, in the left pane, select the virtual machine where you want to configure application monitoring. Then, in the right pane, select the Symantec High Availability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

   On the Symantec High Availability view, specify the credentials of a user account that has administrative privileges on the system and then click **Configure**.

   The single sign-on configuration enables the Symantec High Availability Console to set up a permanent authentication for the user account. After the authentication is successful, the Symantec High Availability view refreshes and displays the link to configure the VCS cluster.
3. On the Symantec High Availability view, click **Configure a VCS Cluster**. This launches the VCS cluster configuration wizard. Unless you configure a cluster, you cannot configure an application for monitoring.



4 On the Welcome panel, review the pre-requisites and then click **Next**.



5 On the Configuration Inputs panel, specify the systems for the VCS cluster operations and the user account details for each system.

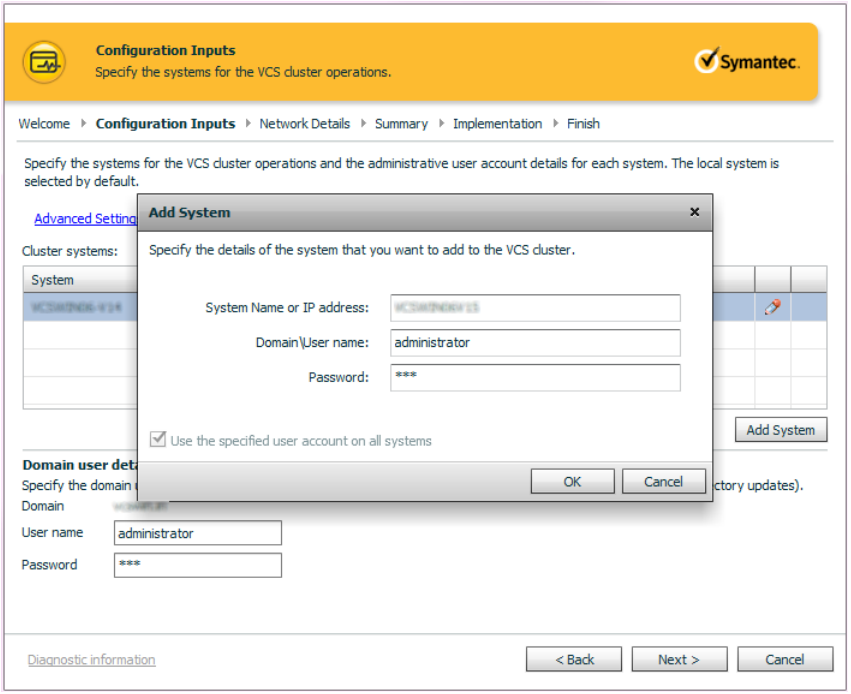
Note: The specified user account must have administrative privileges on the system.

The **Cluster systems** lists the systems that are included in the cluster configuration. The local system is selected by default.

To add more systems, click **Add System** and then on the Add System dialog box, specify the following details of the system that you want to add to the VCS cluster.

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. The user name must be in the domain.com\username. **Note:** The specified user must be a domain user having administrative privileges on all the selected system.
Password	Specify the password for the user account mentioned.
Use the specified user account on all systems	Uses the specified user account on all the cluster systems. This option is selected by default.

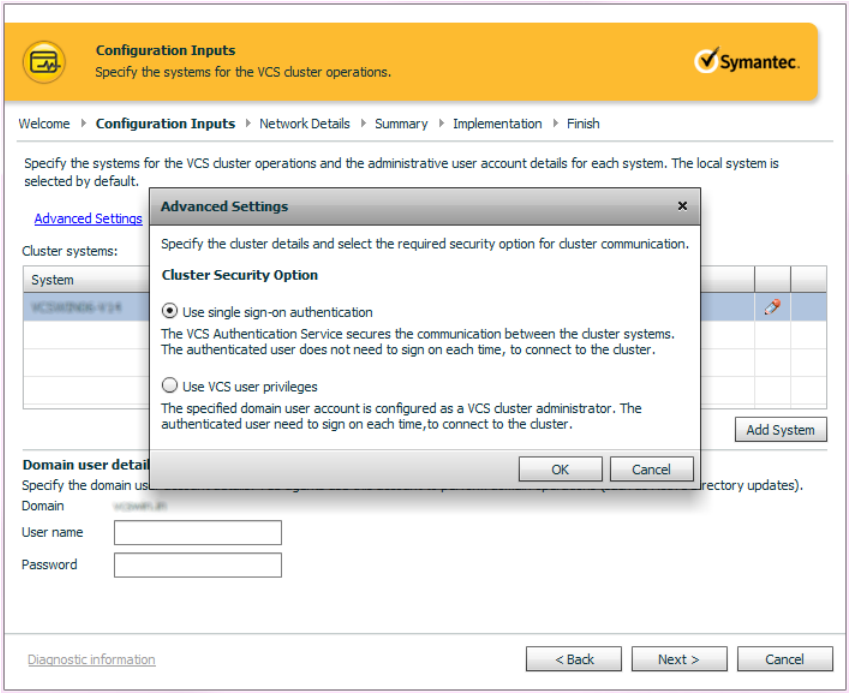
The wizard validates the system details and then adds the system to VCS cluster system list.


Configuration Inputs
Specify the systems for the VCS cluster operations.
Symantec.
Welcome
Configuration Inputs
Network Details
Summary
Implementation
Finish
Specify the systems for the VCS cluster operations and the administrative user account details for each system. The local system is selected by default.
Advanced Setting
Cluster systems:
System
Add System
Domain user det
Specify the domain
Domain
User name
administrator
Password
***
Diagnostic information
< Back
Next >
Cancel
Add System
Specify the details of the system that you want to add to the VCS cluster.
System Name or IP address:
Domain\User name:
administrator
Password:
***
Use the specified user account on all systems
OK
Cancel

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

To modify the security settings for the cluster, on the Configuration Inputs panel, click **Advanced Settings** . In the Advanced settings dialog box, specify the following details and then click **OK**.

Use Single Sign-on	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 user name and password and click OK.



7 On the Network Details panel, select the type of communication for the VCS cluster and then select the adapters to configure the communication links.

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

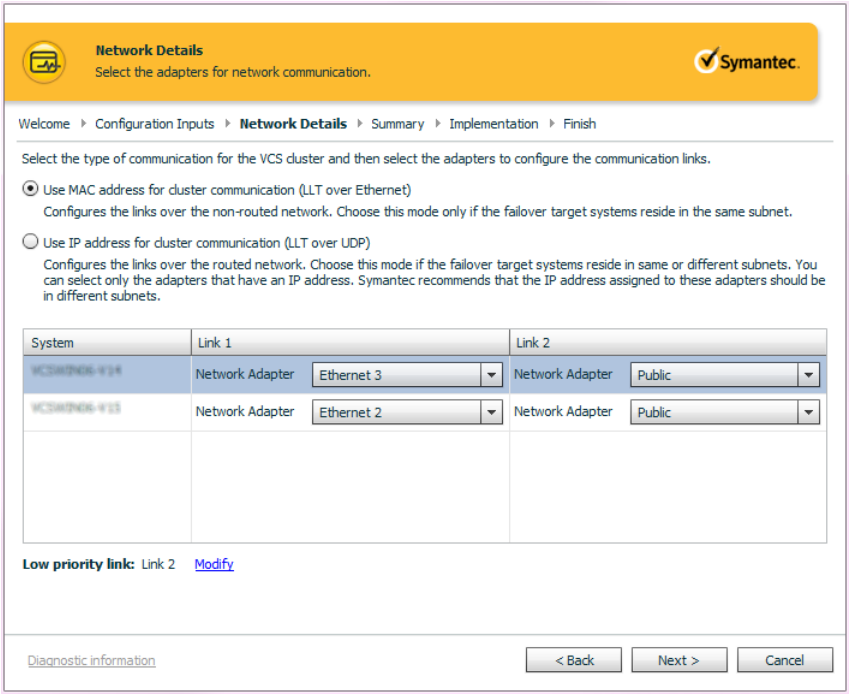
- **Use MAC address for cluster communication (LLT over Ethernet)** : The LLT over Ethernet communication configures the links over the non-routed network. Choose this mode only if the failover target systems reside in the same subnet.
- **Use IP address for cluster communication (LLT over UDP)**: The LLT over UDP communication configures the links over the routed network. You choose this mode regardless of whether the failover target systems reside in the same subnet or in different subnets. You can select only those adapters that have an IP address.

You must select a minimum of two adapters per system.

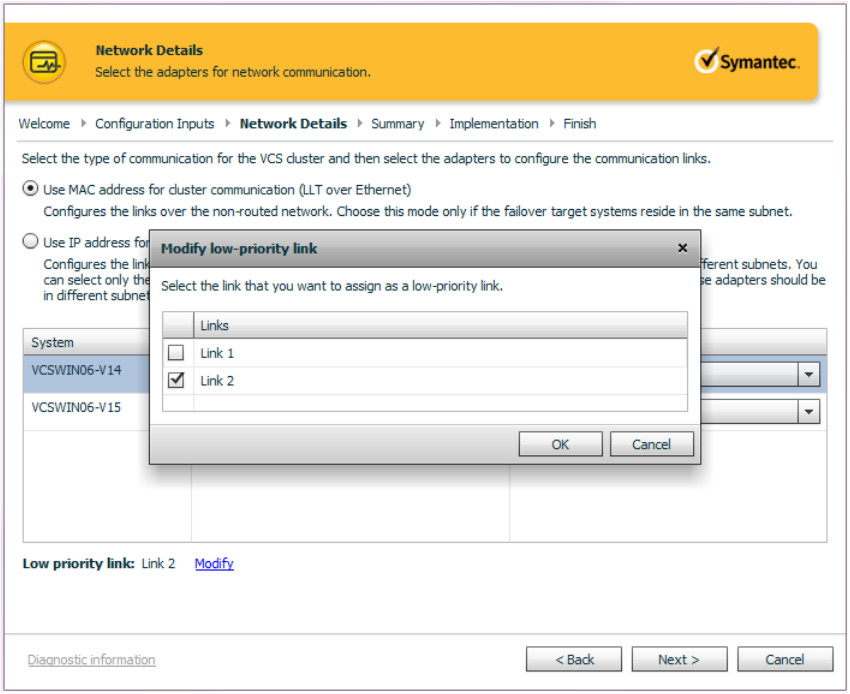
Symantec recommends the following:

- IP addresses that are assigned to the selected adapters should be in different subnets.
- 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.

Network Adapter	Select a network adapter for the communication links. You must select a different network adapter for each communication link. To configure links over UDP, select the type of IP protocol and then specify the required details for each communication link. **Note:** Do not select the teamed network adapters and the independently listed adapters that are a part of the teamed NIC.
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 range 49152 to 65535. A specified port for a link is used for all the cluster systems on that link.
Subnet mask	Displays the subnet masks to which the specified IP belongs.



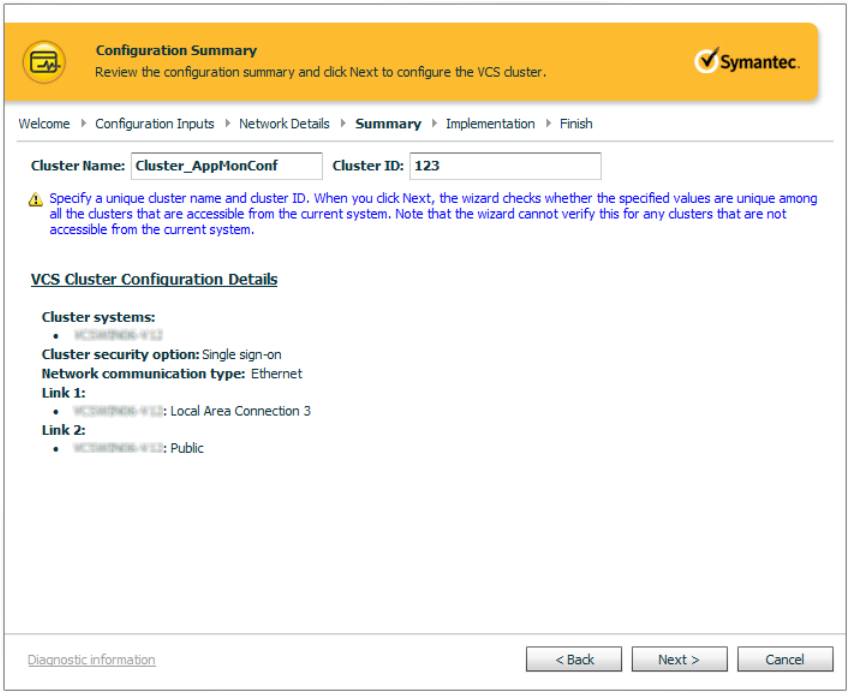
By default, the VCS cluster communication link that uses the public adapter is configured as low-priority link. To change the priority, click **Modify**. In the Modify low-priority link dialog box, select the link and click **OK**.



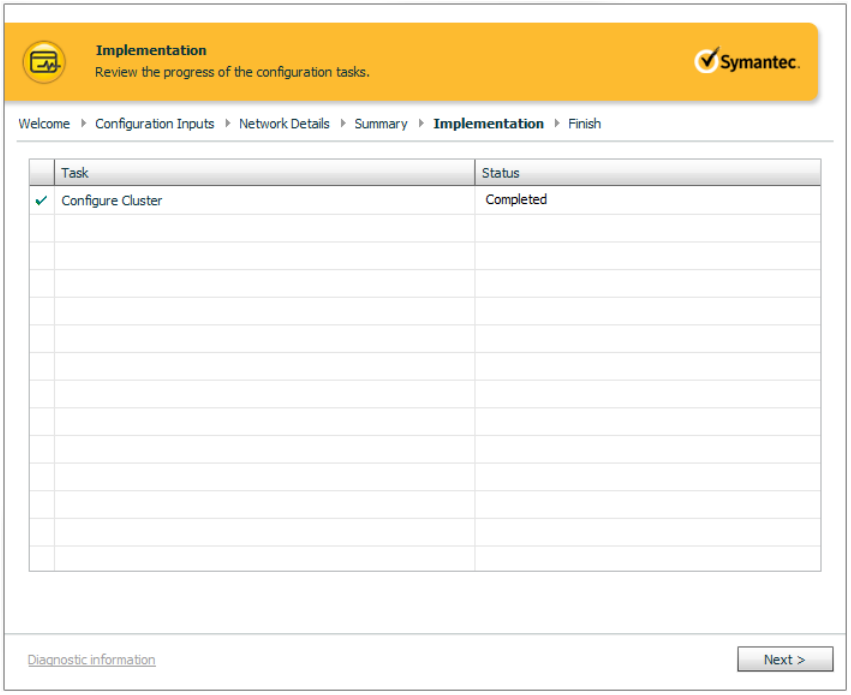
For information about adding or changing the selected network links after the configuration workflow is complete, see the *Symantec Cluster Server Administrator's Guide*.

8 On the Configuration Summary panel, specify a cluster name and a cluster ID of your choice. Review the VCS cluster configuration details and then click **Next** to initiate the configuration.

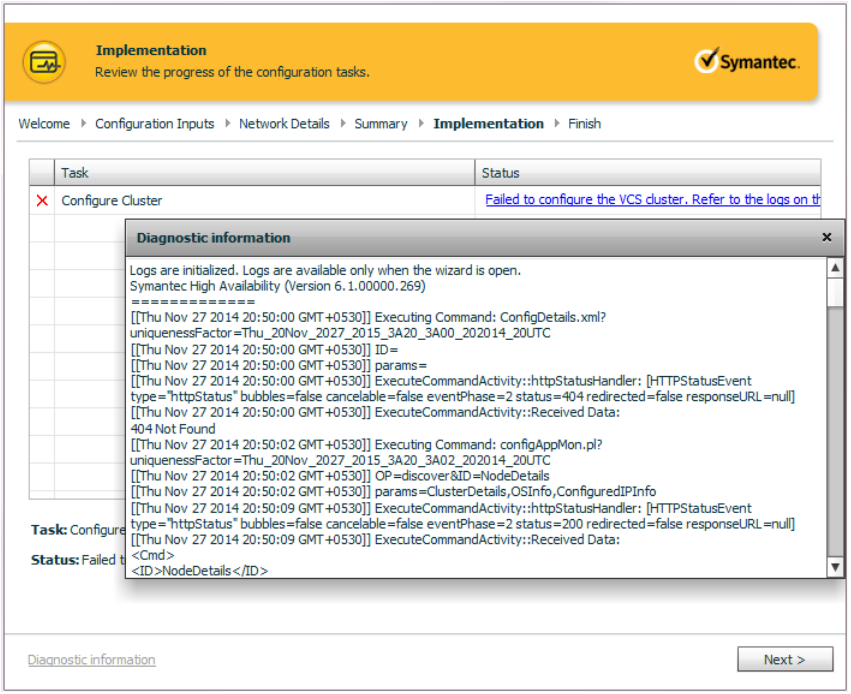
If the network contains multiple clusters, the wizard verifies the cluster ID with the IDs assigned to all the accessible clusters in the network. The wizard does not validate the assigned ID with the clusters that are not accessible during the validation. Symantec recommends you to validate the uniqueness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



9 On the Implementation panel, the wizard displays the VCS cluster configuration tasks and the status of each task. After all the tasks are complete, click **Next**.

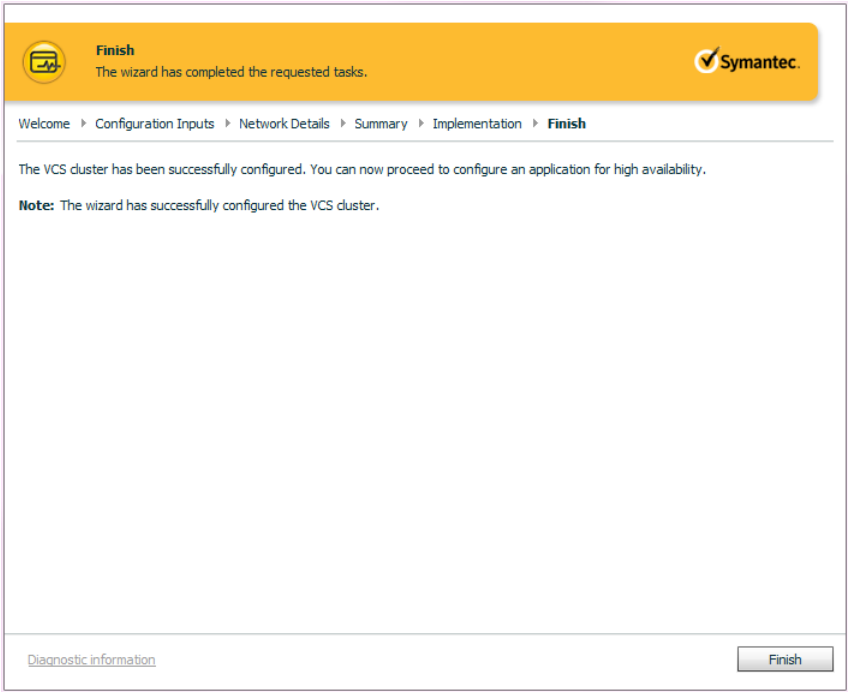


If the configuration tasks fail, click **Diagnostic information** to check the details of the failure.


Implementation
Review the progress of the configuration tasks.
Symantec.
Welcome ▸ Configuration Inputs ▸ Network Details ▸ Summary ▸ Implementation ▸ Finish
Task
Status
Configure Cluster
Failed to configure the VCS cluster. Refer to the logs on th
Diagnostic information
Logs are initialized. Logs are available only when the wizard is open.
Symantec High Availability (Version 6.1.00000.269)
==========
[[Thu Nov 27 2014 20:50:00 GMT+0530]] Executing Command: ConfigDetails.xml?
uniquenessFactor=Thu_20Nov_2027_2015_3A20_3A00_202014_20UTC
[[Thu Nov 27 2014 20:50:00 GMT+0530]] ID=
[[Thu Nov 27 2014 20:50:00 GMT+0530]] params=
[[Thu Nov 27 2014 20:50:00 GMT+0530]] ExecuteCommandActivity::httpStatusHandler: [HTTPStatusEvent
type="httpStatus" bubbles=false cancelable=false eventPhase=2 status=404 redirected=false responseURL=null]
[[Thu Nov 27 2014 20:50:00 GMT+0530]] ExecuteCommandActivity::Received Data:
404 Not Found
[[Thu Nov 27 2014 20:50:02 GMT+0530]] Executing Command: configAppMon.pl?
uniquenessFactor=Thu_20Nov_2027_2015_3A20_3A02_202014_20UTC
[[Thu Nov 27 2014 20:50:02 GMT+0530]] OP=discover&ID=NodeDetails
[[Thu Nov 27 2014 20:50:02 GMT+0530]] params=ClusterDetails,OSInfo,ConfiguredIPInfo
[[Thu Nov 27 2014 20:50:09 GMT+0530]] ExecuteCommandActivity::httpStatusHandler: [HTTPStatusEvent
type="httpStatus" bubbles=false cancelable=false eventPhase=2 status=200 redirected=false responseURL=null]
[[Thu Nov 27 2014 20:50:09 GMT+0530]] ExecuteCommandActivity::Received Data:
<Cmd>
<ID>NodeDetails</ID>
Task: Configure
Status: Failed t
Diagnostic information
Next >

Rectify the cause of the failure and run the wizard again to configure the VCS cluster.

10 On the Finish panel, click **Finish** to complete the wizard workflow. This step completes the VCS cluster configuration.



The Symantec High Availability view now displays the link to configure an application for high availability.

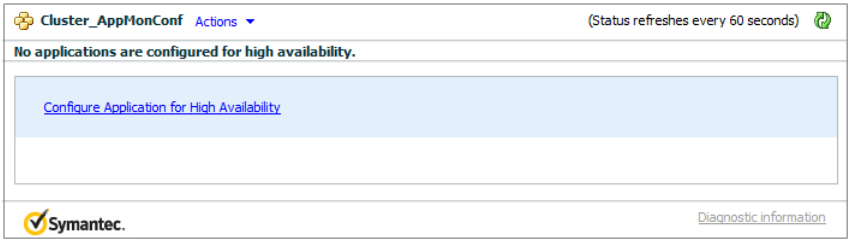
Configuring the application

Perform the following steps to configure monitoring for services, processes, and mount points using the Symantec High Availability Configuration Wizard.

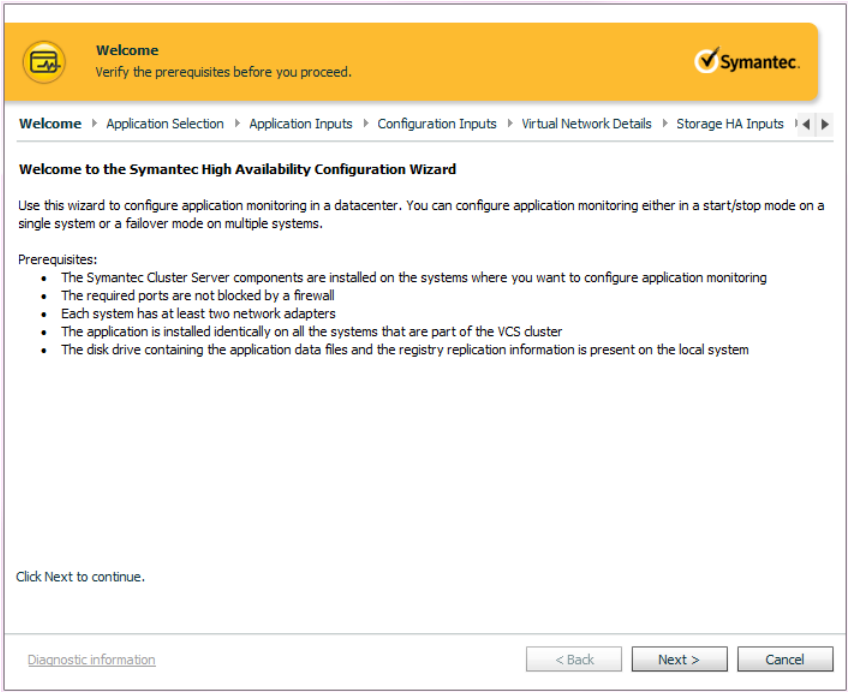
Note: You can configure monitoring for multiple services and processes in a single wizard workflow. However, you cannot configure multiple applications simultaneously. To configure another application, run the wizard again.

To configure the application

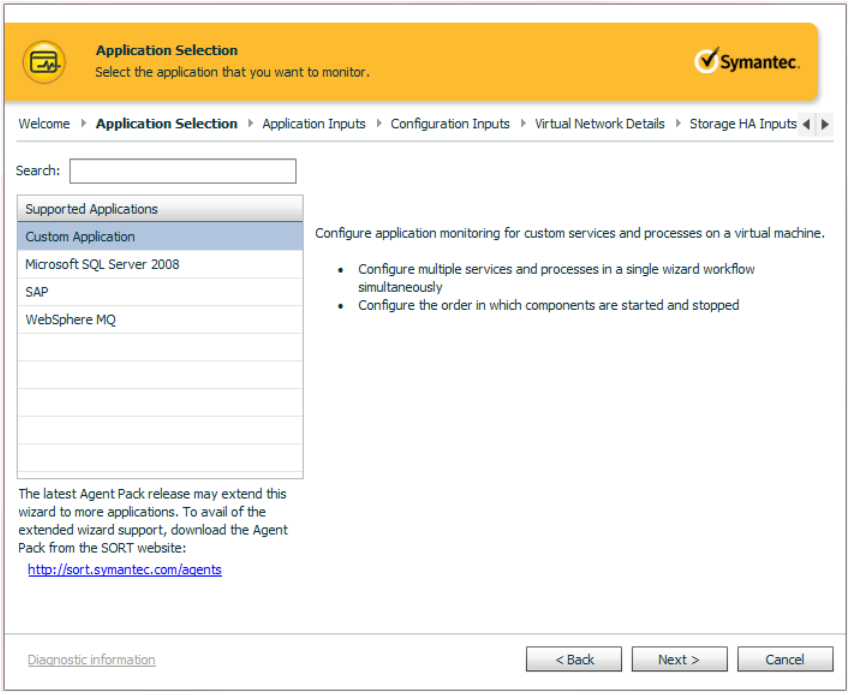
1. Launch the vSphere Client and connect to the vCenter Server that manages the virtual machine. On the Inventory view of the vCenter Server, in the left pane, select the virtual machine where you want to configure application monitoring. Then, in the right pane, select the Symantec High Availability tab.
2. On the Symantec High Availability tab, click **Configure Application for High Availability**. This option is available only after a cluster has been configured. Unless you configure a cluster, you cannot configure an application for monitoring.



3 On the Welcome panel of the Symantec High Availability Configuration wizard, review the pre-requisites and then click **Next**.



4 On the Application Selection panel, select services, processes, and mount points from the Supported Applications list and then click **Next**.



Alternatively, you can use the **Search** box to find the application and then click **Next**.

If you want to download any of the Symantec High Availability agents, click the **Download Application Agents (SORT)** link to download the agents from the Symantec Operations Readiness Tools (SORT) site.

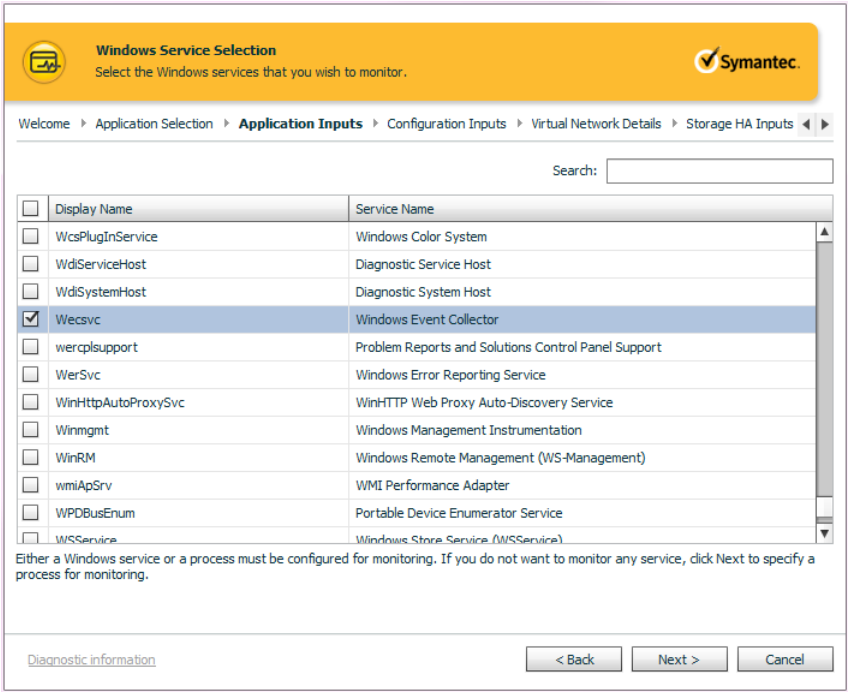
https://sort.symantec.com/agents

5 On the Windows Service Selection panel, select the services that you want to monitor and then click **Next**.

Alternatively, you can use the **Search** box to find the service and then click **Next**.

The wizard automatically discovers the services on the system. If a selected service depends on some other services, you must also select those services. You can define the dependencies between those services on the Define Start-Stop Order panel later.

If you do not want to monitor any services, click **Next** without selecting any service.



6 On the Windows Process Selection panel, specify the processes that you want to monitor.

To specify a process, click **Add Process**.

On the Process Parameters dialog box, select the type of monitoring that you want to configure, specify the required details, and then click **OK**.

For direct process monitoring, specify the following details:

Process Full Path	Specify the complete path of the process executable file including its extension.
Arguments	Specify the command line arguments, if any, for the process to be monitored.
Run process in local system account context	By default the specified process runs in the context of the local system account.
Run process in specified user account context	Select to run the process in a different user's context, and then specify the user name and password in the respective fields. The user name must be in the format user@domain.com or domain.com\username. **Note:** Ensure that you specify a valid user name and that the user account has adequate privileges on the system where you want to configure application monitoring. Otherwise, application monitoring may fail.

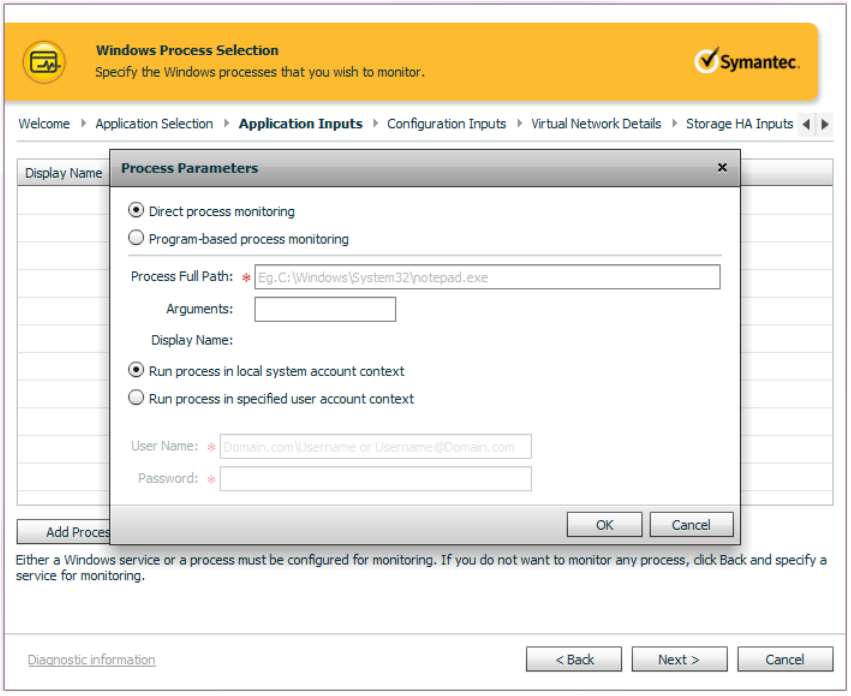
For program-based process monitoring, specify the following details:

Start program	Specify the full path of the program that starts the process to be configured for monitoring.
Arguments	Specify the command line arguments, if any, for the start program.
Monitor program	Specify the full path of the program that monitors the process to be configured for monitoring.
Arguments	Specify the command line arguments, if any, for the monitor program.
Stop program	Specify the full path of the program that stops the process to be configured for monitoring.
Arguments	Specify the command line arguments, if any, for the stop program.

Run process in local system account context	By default the specified process runs in the context of the local system account.
Run process in specified user account context	Select to run the process in a different user's context, and then specify the user name and password in the respective fields. The user name must be in the format user@domain.com or domain.com\username. **Note:** Ensure that you specify a valid user name and that the user account has adequate privileges on the system where you want to configure application monitoring. Otherwise, application monitoring may fail.

The process or the programs that you add is displayed on the Windows Process Selection panel. Repeat this step for all the processes that you want to configure for monitoring.

If you do not want to monitor any processes, click **Next** without specifying any process.



7 On the Mount Point Selection panel, select the mount points that you want to monitor and then click **Next**.

If you do not want to monitor any mount points, click **Next** without selecting any mount points.

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

To define the dependency between the components, select an application component from the **Parent Component** box and then select the components from the **Depends on** box.

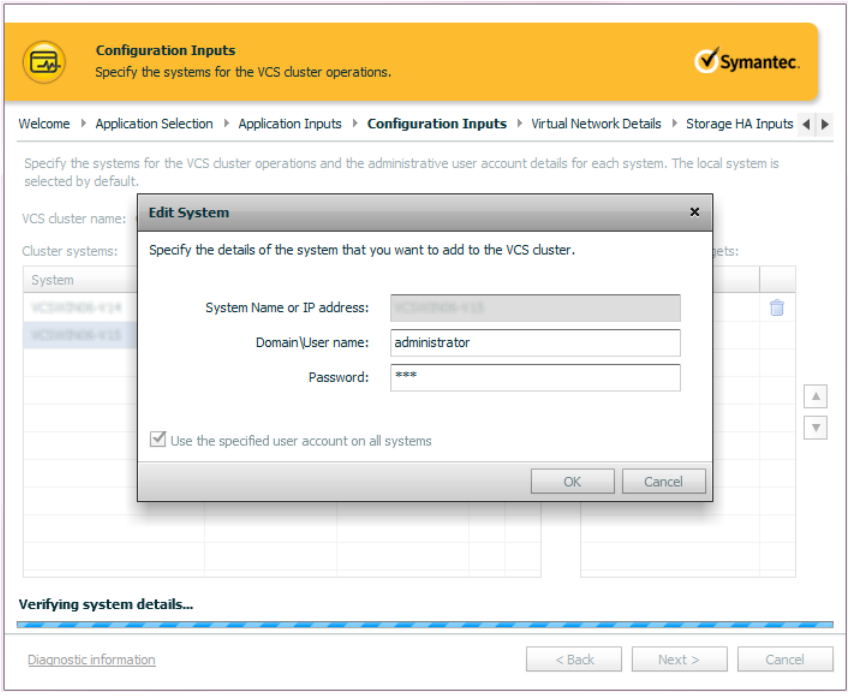
While starting the service or process, the components are brought online in the defined order. For example, if a service is dependent on a mount point, then while starting the service, the mount point is first brought online and then the service itself.

Click **Next** to proceed with the configuration.

9 On the Configuration Inputs panel, select the VCS cluster systems on which you want to configure the application for high availability and move them to the **Application failover targets** list. The local system is selected by default.

Using the up-down arrow keys, you can define the priority order for the failover systems.

For each system that you assign as a failover target, you must specify the domain user account details in the appropriate fields on the Edit System dialog box. The VCS agents use these details to perform domain operations (such as Active Directory updates).

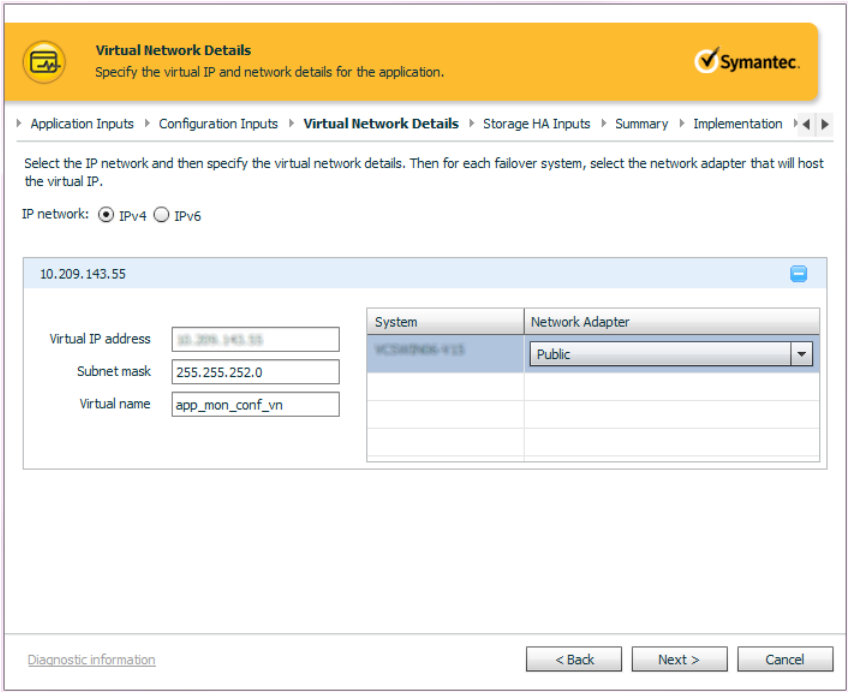


10 On the Virtual Network Details panel, specify the virtual IP and the network details for the application to be configured and then click **Next**.

To specify the virtual IP and network details, select the IP protocol and then specify the following details for each failover system:

Note: You must select the same IP protocol as the one that was selected during the VCS cluster configuration.

Virtual IP address	Specify a unique virtual IP address.
Subnet mask	Specify the subnet mask to which the IP address belongs.
Virtual name	Specify a virtual name.
Network Adapter column	Select the network adapter that will host the virtual IP.

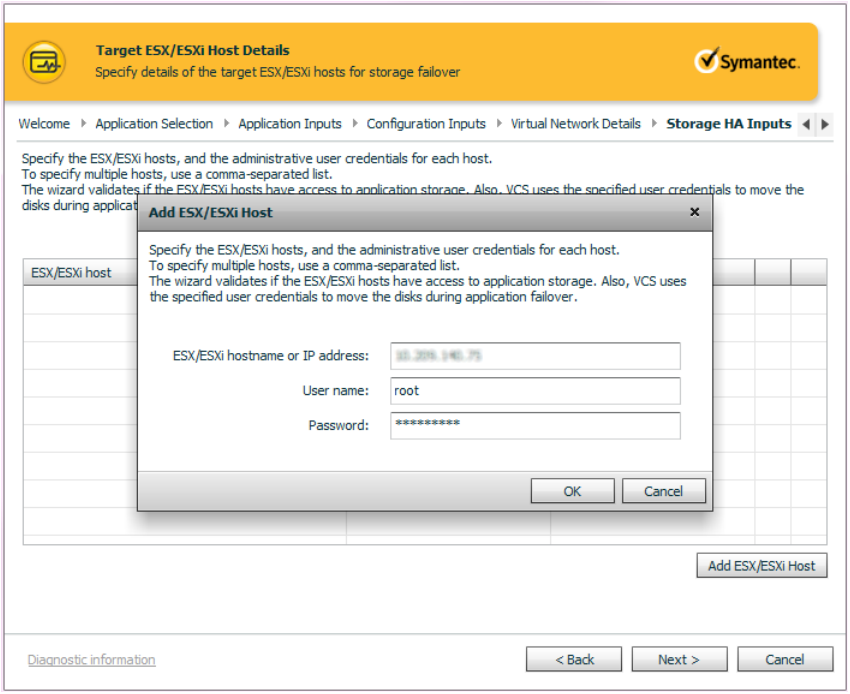


11 On the Storage HA Inputs panel, specify the ESX/ESXi hosts and the administrative user account details for each host, and then click **Next**.

Note: This panel appears only if you have specified a mount point, or multiple application failover targets, or both for the selected custom application.

To specify the ESX/ESXi hosts, click **Add ESX/ESXi Host** and on the Add ESX/ESXi Host dialogue box, specify the following details:

ESX/ESXi hostname or IP address	Specify the target ESX hostname or IP address. The virtual machines will fail over on this ESX host during vMotion. The mount points configured on the ESX host where the application is currently running must be available on the target ESX host.
User name	Specify a user account for the ESX host. The user account must have administrator privileges on the specified ESX host.
Password	Specify the password for the user account provided in the User name text box.



Note: By default, the wizard sets up a communication link with the ESX/ESXi server. You can modify the configuration to set up the communication link with vCenter Server instead. To set up a link with a vCenter Server, you must modify the ESXDetails attribute after this application monitoring configuration workflow is complete.

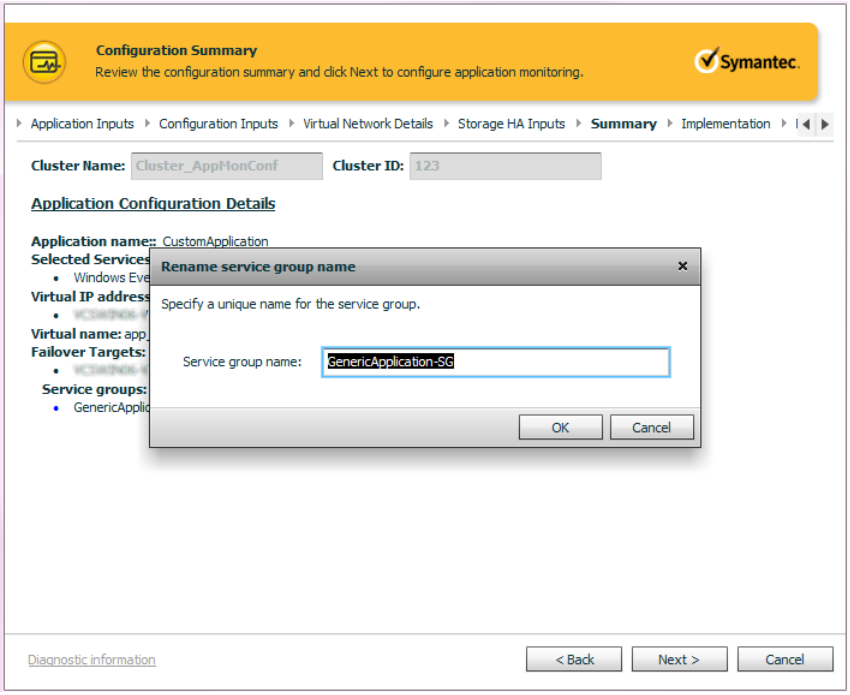
See "Modifying the ESXDetails attribute" on page 52.

---

12 On the Configuration Summary panel, review the application configuration details.

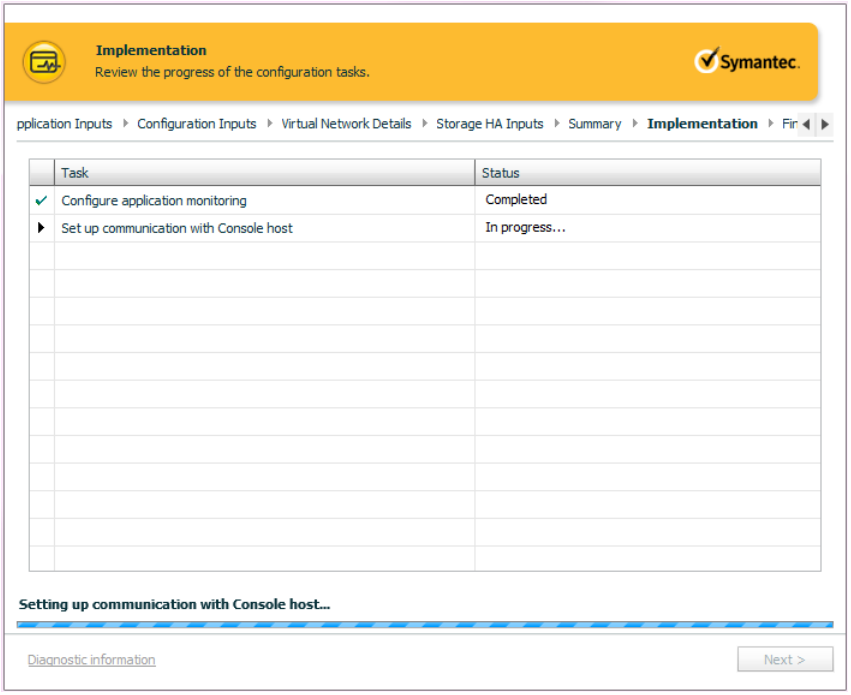
The wizard assigns a unique name to the application service group. Click **Rename** to rename the service group.

Click **Next** to initiate the application monitoring configuration.



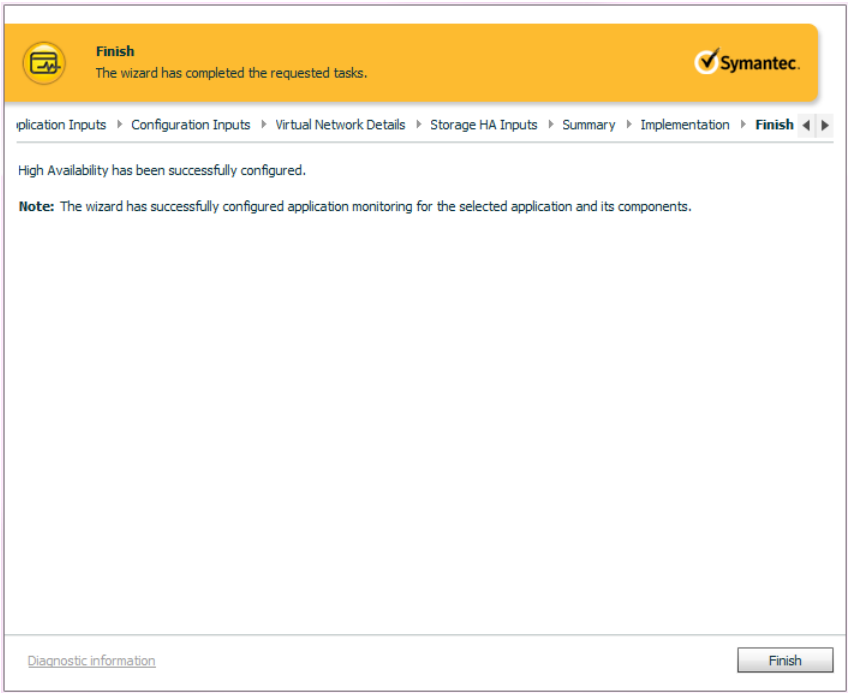
13 On the Implementation panel, the wizard performs the application configuration tasks.

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



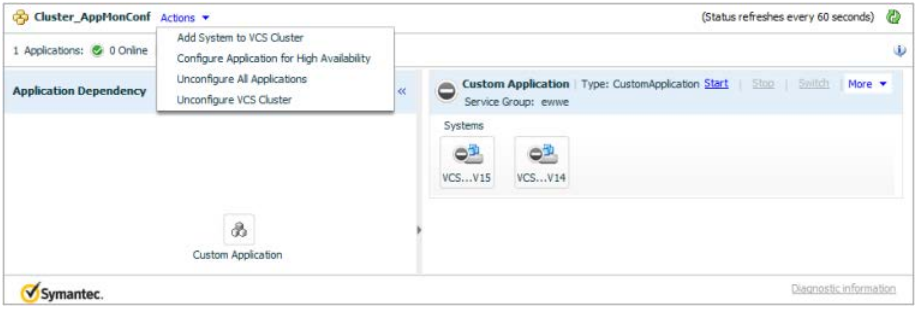
If the configuration tasks fail, click **Diagnostic information** to check the details of the failure. Rectify the cause of the failure, and run the wizard again to configure application monitoring.

14 On the Finish panel, click **Finish** to complete the wizard workflow. This configures the application for high availability on the selected VCS cluster systems.



The Symantec High Availability view now displays the application status and its component dependency.

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



Modifying the ESXDetails attribute

You must modify the value of the "ESXDetails" attribute (of the VMwareDisks agent) if you want the VMwareDisks agent to communicate with the vCenter Server (instead of the ESX/ESXi host) for the disk detach and attach operations.

By default the “ESX Details” attribute of the VMwareDisks agent used the hostnames or IP addresses and the user account details of the ESX hosts on which the virtual machines are configured. To enable the VMwareDisks agent to communicate with the vCenter Server, you must modify the ESXDetails attribute and provide the hostname or IP address and the user account details of the vCenter Server to which the virtual machines belong.

Use the Cluster Manager (Java Console) or the Command Line to modify the attribute values.

To modify the attribute from Cluster Manager

1. From the Cluster Manager configuration tree, select the VMwareDisks resource and then select the **Properties** tab.
2. On the Properties tab, click the Edit icon next to the ESX Details attribute.
3. On the Edit Attribute dialogue box, select all the entries specified under the Key-Value column and press “-“ to delete them.
4. Encrypt the password of the vCenter Server user account.
   - From the command prompt, run the following command:
     ```
     Vcsencrypt –agent
     ```
   - Enter the vCenter Server user account password.
   - Re-enter the specified password
     The encrypted value for the specified password is displayed.
5. On the Edit Attribute dialogue box, click “+” to specify the values under the Key-Value column.
6. Under the Key column, specify the vCenter Server hostname or the IP address.
7. Under the Value column, specify the encrypted password of the vCenter Server user account (from step 4)
8. Click **Ok** to confirm the changes.
9. Repeat the steps for all VMwareDisks resources from the Cluster Manager configuration tree.
10. Save and close the configuration.

To modify/specify the attribute from Command Line

1. Change the VCS configuration to read/write mode.

   ```
   Haconf -makerw
   ```

2. Delete the existing details of the ESX Server.

   ```
   hares -modify VMwareDIsks ResourceName ESXDetails -delete -keys
   ```

3. Encrypt the password of the vCenter Server user account.

   - From the command prompt, run the following command:

     ```
     Vcsencrypt -agent
     ```

   - Enter the vCenter Server user account password.
   - Re-enter the specified password.
     The encrypted value for the specified password is displayed.

4. Specify the vCenter Server details.

   ```
   hares -modify <VMwareDIsks ResourceName> ESXDetails
   -add <vCenter IP address or hostname> <UserName>=<encrypted password>
   ```

Chapter 3

Configuring application high availability- VMware SRM environment

This chapter includes the following topics:

- About setting up the Symantec High Availability solution– VMware SRM environment
- Prerequisites
- Encrypting the recovery site vCenter Server password
- Configuring SSO between the protected and the recovery site
- Updating the SRM recovery plan
- Encrypting the ESX password
- Modifying the attributes for the application and its component dependency group
- Copying the script files
- Configuring the SRM service
- About executing the test recovery plan
- Sample VCS_Site_Info.xml file

About setting up the Symantec High Availability solution– VMware SRM environment

The following table lists the tasks to be performed for setting up the Symantec High Availability solution in a VMware SRM environment.

Verify the pre-requisites	Review the pre-requisites before you begin to deploy the Symantec High Availability Solution in VMware SRM environment. See "Prerequisites" on page 57.
Configure SSO between the Symantec High Availability Console at the recovery site and the protection group virtual machines (at the protected site)	The SSO configuration enables communication between the protected site virtual machines, and the recovery site Symantec High Availability Console. This configuration maintains continuity between the virtual machine and Console communication even after failover. See "Configuring SSO between the protected and the recovery site" on page 60.
Copy the provided script files	Copy the following script files to invoke or execute various functions: ■ preonline.pl ■ setSiteID The script files are available in the `Resource\SRM` folder, in the product software disc. See "Copying the script files" on page 65.
Update the SRM recovery plan	Modify the SRM recovery plan to define the action for application monitoring continuity. See "Updating the SRM recovery plan" on page 61.

Encrypt the recovery site vCenter Server password	This is an optional task. Execute the `EncryptvCenterPassword.ps1` script to encrypt the recovery site vCenter Server password. You must perform this task only if you plan to set up the communication with the recovery site vCenter Server, using the encrypted password . Alternatively, you can configure the "VMware vCenter Site Recovery Manager Server" service or then provide the vCenter Server password in the command that needs to be added to the SRM Recovery Plan. See "Encrypting the recovery site vCenter Server password" on page 58.
Encrypt the recovery site ESX password	Use the vcsencrypt utility to encrypt the recovery site ESX password. You need to specify this encrypted password in the VCS_Site_Info.xml See "Encrypting the ESX password" on page 63.
Modify the attributes for the application components	Update the attribute values in the VCS_Site_Info.xml. This file lists the attributes and their corresponding values for the application components. The attributes and their values must be specified for both, the protected and the recovery site. See "Modifying the attributes for the application and its component dependency group" on page 64.
Configure the "VMware vCenter Site Recovery Manager Server" service	This is an alternative task. You must perform this task only if you have not executed the `EncryptvCenterPassword.ps1` script but plan to encrypt the secondary site vCenter Server password. You can configure the "VMware vCenter Site Recovery Manager Server" service only if the SRM Server and the vCenter Server are present in the same domain. You must perform this tasks before you execute the recovery plan. See "Configuring the SRM service " on page 65.

Prerequisites

Review the following pre-requisites before you begin to deploy the Symantec High Availability Solution in VMware SRM environment:

Set up the VMware SRM environment	Ensure that you have performed the following tasks while you set up the SRM environment: ■ Install and configure VMware SRM and vCenter Server at both, the primary and the recovery site ■ At the protected site, set up a protection group for the virtual machines on which you want to configure appliaction monitoring ■ Create a SRM recovery plan ■ In the SRM recovery plan, verify if the virtual machines in the protection group are included in the same priority group. This required to ensure that all the virtual machines in a VCS cluster are failed over at the same time. ■ Install the vSphere PowerCLI on the SRM Servers. For more details on performing each of these tasks, refer to VMware product documentation.
Install Symantec High Availability Console	Ensure that the Symantec High Availability Console is installed at both, the protected and the recovery site. For more details refer to, *Symantec High Availability Console Installation and Upgrade Guide*.
Install the Symantec High Availability Guest Components	Install VCS or SFW HA, as part of the Symantec High Availability guest components installation. Install these components on all the virtual machines (at the protected site) where you want to configure application monitoring. These virtual machines must be a part of the protection group. For details refer to the *Symantec High Availability Solutions Guide for VMware*.
Configure SSO	Configure SSO between the Symantec High Availability Console and the guest machine on the respective sites. For more details refer to *Symantec High Availability Solutions Guide for VMware*.

Verify that the user account privileges and the ports are enabled	■ The vCenter logged-on user must have the Symantec High Availability 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. ■ Ports 5634, 14152, and 14153 are not blocked by a firewall on the Console hosts and the virtual machines.
Verify if the required services are running on the Symantec High Availability Console at both the sites	■ Symantec ApplicationHA Service (ApplicationHA Console) ■ Veritas Storage Foundation Messaging Service (xprtld) ■ Symantec Authentication Service
Others	■ Ensure that the virtual machines can access the Console host at both the sites. ■ Ensure that the virtual machines can access the Console host at recovery site using the fully qualified host name. ■ Ensure that the clock times on the protected site virtual machines and the recovery site ApplicationHA Console are within 30 minutes of one another.
Configure application monitoring	At the protected site, ensure that application monitoring is configured on the virtual machines and the VCS cluster is formed. For more details on configuring application monitoring, refer to the respective application configuration guides. **Note:** For application monitoring continuity in a VMware SRM environment, you must configure the VCS cluster communication links using the MAC address (LLT over Ethernet option). If you use IP address (LLT over UDP option) to configure the cluster communication links, then the VCS cluster fails to start after the virtual machines are failed over to the recovery site.

Encrypting the recovery site vCenter Server password

This is an optional task.

You must perform this task only if you plan to encrypt the recovery site vCenter Server user account password (that is; if you do not want to specify the vCenter

Server user account password in the command step that must be added to the SRM Recovery Plan for application monitoring continuity).

Alternatively, you can avoid providing the password in the command step by configuring the VMware vCenter Site Recovery Manager Server service (only if the SRM Server and the vCenter Server are in the same domain).

The EncryptvCenterPassword.ps1 script stores the vCenter Server user account credentials at a specified or the default location. These details are then used by the command step that you add to update the recovery plan.

To encrypt the vCenter Server user account password

1. From the product software disc navigate to the following path and copy the EncryptvCenterPassword.ps1 script to a temporary location on the SRM Server at the recovery site.

   `Resource\SRM`

2. From the command prompt run the following command:

   `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted c:\encryptVCenterPasswd.ps1 [-CredPath]`

   Where,

   CredPath is the path where you want to save the vCenter Server user account credentials. For example, *c:\users\administrator\VCenterUserInfo.xml*

   Note: Ensure that the path is specified in ‘ ‘ (single quotes) and that it does not contain the character ‘&’ in it.

   The encryptVCenterPasswd.ps1 script fails to save the vCenter Server user account details at a specified path, if the path is specified in “ “ (double quotes) and contains a space. Also, if the path contains a character ‘&’ in it the script displays an error indicating that the specified path does not exists.

   If you do not specify the FileName, then the user account credentials are saved at the following location by default:

   `C:\ProgramData\Veritas\VCenterUserInfo.xml` is used.

   After you run the command, a dialogue box to specify the vCenter Server user account details is displayed.

Configuring SSO between the protected and the recovery site

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

To configure the single sign-on

1. On the recovery site, using the vSphere Client, connect to the vCenter Server and navigate to **Home** > **Solutions and Applications** > **Symantec High Availability**.
2. On the Symantec High Availability 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 Symantec High Availability Console and the vCenter Server at the protected site.

   The wizard uses these details to set up a link with the protected site virtual machines and the Symantec High Availability Console at the recovery site. 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.

7 The Implementation panel displays the SSO configuration progress for each virtual machine. 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 Symantec High Availability Console at the following location:

```
%AllUsersProfile%\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 Symantec High Availability Console at the recovery site.

Updating the SRM recovery plan

After you have configured SSO between the recovery site Symantec High Availability 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 the form of an Symantec High Availability recovery command that must be added to the SRM recovery plan.

Note: You must perfom these steps on all the virtual machines.

To update the SRM recovery plan

1 Using the vSphere Client, navigate to **Home** > **Solutions and Applications** > **Site Recovery**

In the left pane, select **Recovery Plan**.

2 From the list of recovery plans, select the recovery plan to be updated.

3 In the recovery plan, select the virtual machine, right-click and click **Configure**.

4 On the VM Recovery Properties panel, select **Pre-power On Steps** in the left pane and click **Add** in the right pane.

5 On the Add Pre-power On Step panel, perform the following tasks:

- Select **Command on SRM Server**
- In the Name text box, specify a name for the command step to be added
- In the Content text box, specify the following command

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-ExecutionPolicy Unrestricted c:\setSiteID.ps1 -vCenter <IP address>
-SiteId <ID> -VM 'VirtualMachine HostName'
-U Administrator -P Password
-UseFileCred 0/1
-CredPath CredFilePath
```

Where,

- IP address = The IP address of recovery site vCenter Server. If you do not specify the IP address, then the vCenter Server hostname is considered by default.
- ID= Specify an ID for the recovery site
  This is required when you modify the vcs_site_info.xml file.
  If you do not specify an ID, the hostname of recovery site SRM Server is used.
- VirtualMachine HostName= Host name of the local machine as that specified in the vCenter server inventory

  Note: Ensure that the hostname does not contain any special characters. If the hostname contains any special characters, then the "setSiteID.ps1" script that is used to assign a site ID to the respective sites fails to assign these IDs.

- Administrator= User account name for the recovery site vCenter Server
- Password= Password for the user account specified
- UseFileCred= Specify a value for this argument depending on whether or not you have encrypted the vCenter Server user account password, using the encryptVCenterPassword.ps1 script.
  0= The vCenter Server password is not encrypted and you need to specify the password in the command.
  1= The vCenter Server password is encrypted and is saved at a temporary location.

  Note: You need not specify this argument if you plan to configure the SRM service. This service configuration helps to automatically establish a connection with the vCenter Server.

- CredFilePath= File path where the vCenter Server user account credentials are saved

You need to specify this variable only if you have specified '1' for UseFileCred variable.

Note: User account details are required only if you intend to encrypt the vCenter Server user account password. To encrypt the password, you must execute the EncryptvCenterPassword.ps1 script. This script saves the user account details at the specified or default location. The CredPath specified is applied only if the UseFileCred argument value is 1.

- Click **Ok**.

6 On the VM Recovery Properties panel, from the left panel, select **Post Power On Steps** and click **Add**.

7 On the Add Post Power On Step panel, perform the following:

- Select **Command on Recovered VM**
- In the Name text box, specify a name for the command step to be added
- In the Content text box, specify the following command step

  ```
  "%vcs_home%\bin\getAppStatus.bat"
  ```

  This script retrieves the application status after it is started at the recovery site.
- Click **Ok**.

Encrypting the ESX password

Before you specify passwords in the XML configuration file, you must encrypt them by using the vcsencrypt utility.

Perform these steps for all the passwords to be specified in the XML file.

To encrypt a password

1 Run the vcsencrypt utility by typing the following on the command line.

```
C:\> vcsencrypt -agent
```

2 The utility prompts you to enter the password twice. Enter the password and press **Enter**.

```
Enter New Password:

Enter Again:
```

3 The utility encrypts the password and displays the encrypted password.

4 Specify this encrypted password in the XML file.

Modifying the attributes for the application and its component dependency group

The VCS_Site_Info.xml file saves a site ID for both, the protected and the recovery site. It also lists the attributes for the configured application components. Each attribute must have a corresponding value on both the sites.

During a disaster, when the virtual machines fail over to the recovery site, VCS considers these attribute values and then starts the application.

Note: You must perform this task on all the virtual machines that are a part of the protection group.

To modify the attribute values

1 Copy the vcs_site_info.xml file and save it to the following location on a virtual machine in the protection group:

%VCS_Home%\conf

2 Modify the xml file to specify a SiteID for the protected and the recovery site. Also, update the required resource names and attribute values for the respective sites.

Note: Ensure that the specified attribute values do not contain any of these special characters ", < and >". If the attribute values contain any of these characters, then the preonline.pl script fails to appliy the specified attributes to the respective sites.

---

3 Copy and save this modified XML file on all the virtual machines.

4 Using the VCS Java Console, perform the following tasks:

- Select the application dependency group and set its "PreOnline Trigger" attribute to "True".
- Ensure that the "AutoStartList" attribute includes all the virtual machines that were specified in the Failover Target System List of the application dependency group.

Note: You must perform this step for each application dependency group from any virtual machine in the protection group.

Copying the script files

Copy the "preonline.pl" and the "setSiteID.ps1" files from the following location on the product software disc:

`Resource\SRM folder`

You must copy these files to the recovery site SRM Server or the local virtual machine.

The following table provides the details on the function of the respective file and the destination folder where the file should be copied:

preonline.pl	This script executes the vcs_site_info.xml and applies the specified attribute values for the respective site. Copy this script on all the virtual machines at the following location: %vcs_home%\bin\Triggers
setSiteID.ps1	This script applies or assigns a SiteID to both the sites. Copy this script to a temporary location on the SRM Server at the recovery site. This script is executed when the command specified in the Pre-power On Step of a virtual machine is run.

Configuring the SRM service

This is an alternative task.

You must perform this task only if you have not executed the EncryptvCenterPassword.ps1 script, but want to encrypt the secondary site vCenter Server user account password (do not want to specify the vCenter Server user account password in the command step to be added to the recovery plan).

You can configure the "VMware vCenter Site Recovery Manager Server" service only if the SRM Server and the vCenter Server are present in the same domain.

Perform this task before you execute the recovery plan.

To configure the SRM service

1. On the SRM Server at the recovery site, launch the Windows Services panel.
2. Select and double-click on the "VMware vCenter Site Recovery Manager Server" service.
3. On the service dialog box that appears, select the **Log On** tab.
4. On the Log On tab, select **This account** and browse or specify the vCenter Server user account details.
5. Click **Ok**.

About executing the test recovery plan

After you have configured the sites for disaster recovery, you can test the recovery plan to verify the fault-readiness by mimicking a failover from the protected site to the recovery site. This procedure is done without affecting application monitoring.

When you run a test recovery plan, the virtual machines specified in the plan appear in the isolated network at the recovery site.

For details, refer to, VMware product documentation.

For test recovery, Symantec recommends you to modify your network settings such that,

- The recovery site vCenter Server and Symantec High Availability Console is able to communicate with the test virtual machines.
- Create a dedicated network for the test virtual machines to failover. The target ESX console port should be accessible over this virtual network.
  To create this network, you must select "Auto" as the Test Network while you create the SRM Recovery Plan.
- Configure the test virtual machines such that they are accessible over the virtual network created.

Note: If you do not set up a dedicated network for the test virtual machines to failover, the virtual machines failover in an isolated network. During the failover the VMwareDisk agent successfully, deports and imports the VMware disk to the target virtual machine and the application dependency group is successfully brought online. However, the VMwaredisk agent goes in to an "Unknown" state.

Sample VCS_Site_Info.xml file

The following sample xml depicts the VCS_Site_Info.xml file. This file lists the attribute values for the configured application components, on both the sites.

```
<SiteInfo>
<site name="SiteB">
<attr resname="GenericApplication-SG-Lanman"
attrname="VirtualName" type="scalar">
<value data="LanmanName_SiteB"/>
</attr>
<attr resname="GenericApplication-SG-VMWareDisks"
attrname="ESXDetails" type="assoc">
<value data="ESXIP_SiteB" rvalue="root=ESXPassword_encrypted
ByVCS_SiteB"/>
</attr>
<attr resname="GenericApplication-SG-IP" attrname="Address" type="scalar">
</attr>
</site>
<site name="SiteA">
<attr resname="GenericApplication-SG-Lanman"
attrname="VirtualName" type="scalar">
</attr>
<attr resname="GenericApplication-SG-VMWareDisks"
attrname="ESXDetails" type="assoc">
<value data="ESXIP_SiteA" rvalue="root=ESXPassword_encrypted
ByVCS_SiteA"/>
</attr>
<attr resname="GenericApplication-SG-IP" attrname="Address" type="scalar">
</attr>
</site>
</SiteInfo>
```

Chapter 4

Administering application availability

This chapter includes the following topics:

- Administering application monitoring using the Symantec High Availability tab
- Administering application monitoring settings
- Administering application availability using Symantec High Availability dashboard

Administering application monitoring using the Symantec High Availability tab

Symantec Cluster Server provides you with 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.

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 for multiple applications on multiple systems in a data center. For more information on the later:

See "Administering application availability using Symantec High Availability dashboard" on page 84.

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

- To configure and unconfigure application monitoring
- To unconfigure the VCS cluster

- To start and stop configured applications
- To add and remove failover systems
- To enter and exit maintenance mode
- To switch an application
- To determine the state of an application (components)
- To resolve a held-up operation
- To modify application monitoring settings
- To view application dependency
- To view component dependency

To view the Symantec High Availability tab, launch the VMware vSphere Client, select a system from the inventory and then click the **Symantec High Availability** tab.

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

Note: You can also perform the application monitoring operations directly from a browser window using the following URL:
https://<*VMNameorIP*>:5634/vcs/admin/application_health.html?priv=ADMIN
where <*VMNameorIP*> is the virtual machine name or the IP address of the system from where you want to access the tab.

A prompt for user account details will be displayed. You must enter the system user account details.

Understanding the Symantec High Availability tab work area

The Symantec High Availability tab displays the consolidated health information for applications running in a Symantec Cluster Server (VCS) cluster. The cluster may include one or more systems.

When you click a system in the inventory view of the VMware vSphere client, the Symantec High Availability tab displays application information for the entire VCS cluster, not just the selected system.

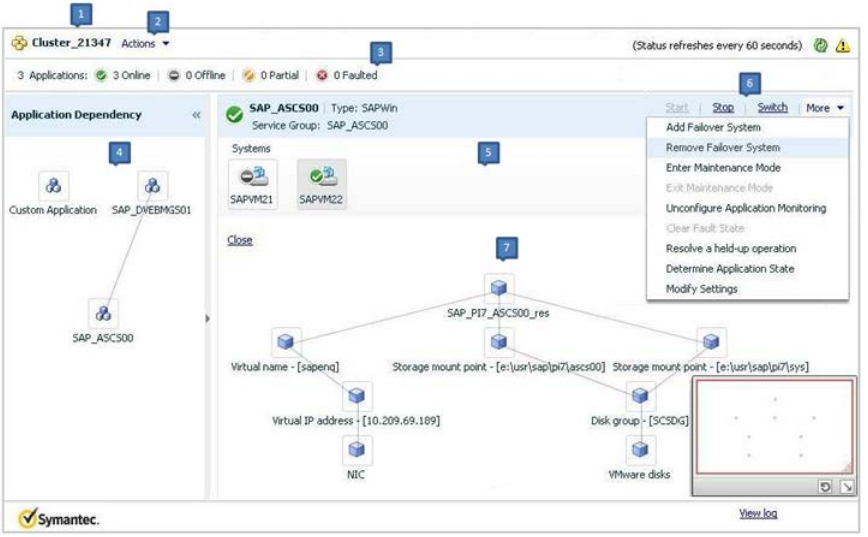
Note: If you do not configure any application for monitoring in the VCS cluster, then the Symantec Application High Availability tab displays only the following link: **Configure an application for high availability**.

The Symantec High Availability tab uses icons, color coding, dependency graphs, and tool tips to report the detailed status of an application.

The Symantec High Availability tab displays complex applications, for example SAP Netweaver, in terms of multiple interdependent instances of that application. These interdependent instances represent component groups of the application. The component groups are also known as "service groups" in VCS terminology.

Each service group in turn includes several critical components of the application. The components are known as "resources" in VCS terminology.

The following figure displays two instances of SAP running in the Symantec High Availability tab:



1. Title bar

2. Actions menu

3. Aggregate Status Bar

4. Application dependency graph

5.Application table

6. Application-specific task menu

7. Component dependency graph

The Symantec High Availability tab graphic user interface (GUI) includes the following components:

- Title bar: Displays the name of the VCS cluster, the Actions menu, the Refresh icon, the Alert icon. Note that the Alert icon appears only if the communication between Symantec High Availability Console and the system fails, and the Symantec High Availability tab fails to display the system, or displays stale data.

- Actions menu: Includes a drop-down list of operations that you can perform with effect across the cluster. These include: Configuring an application for high availability; Unconfigure all applications; and Unconfigure VCS cluster.
- Aggregate status bar: Displays a summary of applications running in the cluster. This includes the total number of applications, and the state-wise breakdown of the applications in terms of the Online, Offline, Partial, and Faulted states.
- Application dependency graph: Illustrates the order in which the applications or application instances, must start or stop.

  If an application must start first for another application to successfully start, the former application appears at a lower level. A line connects the two applications to indicate the dependency. If no such dependency exists, all applications appear in a single horizontal line.
- Application table: Displays a list of all applications configured in the VCS cluster that is associated with the system you selected in the inventory view of the vSphere Client GUI.

  Each application is listed in a separate row. Each row displays the systems where the application is configured for monitoring.

  The title bar of each row displays the following entities to identify the application or application instance (service group):

  - Display name of the application (for example, Payroll application)
  - Type of application (for example, Custom)
  - Service group name
- Application-specific task menu: Appears in each application-specific row of the application table. The menu includes application-specific tasks such as Start, Stop, Switch, and a dropdown list of more tasks. The More dropdown list includes tasks such as Add a failover system, and Remove a failover system.
- Component dependency graph: Illustrates the order in which application components (resources) must start or stop for the related application or application instance to respectively start or stop. The component dependency graph by default does not appear in the application table. To view the component dependency graph for an application, you must click a system on which the application is running.

  The track pad, at the right-bottom corner helps you navigate through complex component dependency graphs.

  If you do not want to view the component dependency graph, in the top left corner of the application row, click **Close**.

To view the status of configured applications

In the application dependency graph, click the application for which you want to view the status. If the appropriate row is not already visible, the application table automatically scrolls to the appropriate row. The row displays the state of the application for each configured failover system in the cluster for that application.

If you click any system in the row, a component dependency graph appears. The graph uses symbols, color code, and tool tips to display the health of each application component. Roll the mouse over a system or component to see its health details.

The health of each application/application component on the selected system is displayed in terms of the following states:

Table 4-1 Application states

State	Description
Online	Indicates that the configured application or application components are running on the virtual machine. If the application is offline on at least one other failover system, an alert appears next to the application name.
Offline	Indicates that the configured application or its components are not running on the virtual machine.
Partial	Indicates that either the application or its components are being started on the virtual machine or Symantec Cluster Server was unable to start one or more of the configured components If the application is offline on at least one other failover system, an alert appears next to the application name.
Faulted	Indicates that the configured application or its components have unexpectedly stopped running.

To configure or unconfigure application monitoring

Use the Symantec High Availability tab to configure or unconfigure an application for monitoring in a cluster under Symantec Cluster Server (VCS) control.

The tab provides you with specific links to perform the following configuration tasks:

- Configure the first application for monitoring in a VCS cluster:
  If you have not configured any application for monitoring in the cluster, the Symantec High Availability tab appears blank except for the link **Configure an application for high availability**.

Click the link to launch the Symantec High Availability Application Monitoring Configuration Wizard. Use the wizard to configure application monitoring.

- Unconfigure monitoring of an application:
  In the appropriate row of the application table, click **More** > **Unconfigure Application Monitoring** to delete the application monitoring configuration from the VCS.
  Note that this step does not remove VCS from the system or the cluster, this step only removes the monitoring configuration for that application.
  Also, to unconfigure monitoring for an application, you can perform one of the following procedures: unconfigure monitoring of all applications, or unconfigure VCS cluster.
- Unconfigure monitoring of all applications:
  Click **Actions** > **Unconfigure all applications**. This step deletes the monitoring configuration for all applications configured in the cluster.
- Unconfigure VCS cluster:
  Click **Actions** > **Unconfigure VCS cluster**. This step stops the VCS cluster, removes VCS cluster configuration, and unconfigures application monitoring.

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 or component groups (application instances).

Note that the **Start** and **Stop** links are dimmed in the following cases:

- If you have not configured any associated components or component groups (resources or service groups) for monitoring
- If the application is in maintenance mode
- If no system exists in the cluster, where the application is not already started or stopped as required.

To start an application

1. In the appropriate row of the application table, click **Start**.
2. If the application (service group) is of the failover type, on the Start Application panel, click **Any system**. VCS uses pre-defined policies to decide the system where to start the application.

   If the application (service group) is of the parallel type, on the Start Application panel, click **All systems**. VCS starts the application on all required systems, where the service group is configured.

   Note: Based on service group type, either the Any system or the All Systems link automatically appears.

   To learn more about policies, and parallel and failover service groups, see the *VCS Administrator's Guide*.

   If you want to specify the system where you want to start the application, click **User selected system**, and then click the appropriate system.
3. If the application that you want to start requires other applications or component groups (service groups) to start in a specific order, then check the **Start the dependent components in order** check box, and then click **OK**.

To stop an application

1. In the appropriate row of the application table, click **Stop**.
2. If the application (service group) is of the failover type, in the Stop Application Panel, click **Any system**. VCS selects the appropriate system to stop the application.

   If the application (service group) is of the parallel type, in the Stop Application Panel click **All systems**. VCS stops the application on all configured systems.

   Note: Based on service group type, either the Any system or the All Systems link automatically appears.

   To learn more about parallel and failover service groups, see the *VCS Administrator's Guide*.

   If you want to specify the system, where you want to stop the application, click **User selected system**, and then click the appropriate system.
3. If the application that you want to stop requires other applications or component groups (service groups) to stop in a specific order, then check the **Stop the dependent components in order** check box, and then click **OK**.

To switch an application to another system

If you want to gracefully stop an application on one system and start it on another system in the same cluster, you must use the Switch link. You can switch the application only to a system where it is not running.

Note that the Switch link is dimmed in the following cases:

- If you have not configured any application components for monitoring
- If you have not specified any failover system for the selected application
- If the application is in maintenance mode
- If no system exists in the cluster, where the application can be switched
- If the application is not in online/partial state on even a single system in the cluster

To switch an application

1. In the appropriate row of the application table, click **Switch**.
2. If you want VCS to decide to which system the application must switch, based on policies, then in the Switch Application panel, click **Any system**, and then click **OK**.

   To learn more about policies, see the *Symantec Cluster Server Administrator's Guide*.

   If you want to specify the system where you want to switch the application, click **User selected system**, and then click the appropriate system, and then click **OK**.

   Symantec Cluster Server stops the application on the system where the application is running, and starts it on the system you specified.

To add or remove a failover system

Each row in the application table displays the status of an application on systems that are part of a VCS cluster in a VMware environment. The displayed system/s either form a single-system Symantec Cluster Server (VCS) cluster with application restart configured as a high-availability measure, or a multi-system VCS cluster with application failover configured. In the displayed cluster, you can add a new system as a failover system for the configured application.

The system must fulfill the following conditions:

- Symantec Cluster Server 6.1 is installed on the system.
- The system is not part of any other VCS cluster.

- The system has at least two network adapters.
- The required ports are not blocked by a firewall.
- The application is installed identically on all the systems, including the proposed new system.

To add a failover system, perform the following steps:

Note: The following procedure describes generic steps to add a failover system. The wizard automatically populates values for initially configured systems in some fields. These values are not editable.

To add a failover system

1. In the appropriate row of the application table, click **More** > **Add Failover System**.
2. Review the instructions on the welcome page of the Symantec High Availability Configuration Wizard, and click **Next**.

3 If you want to add a system from the Cluster systems list to the Application failover targets list, on the Configuration Inputs panel, select the system in the Cluster systems list. Use the Edit icon to specify an administrative user account on the virtual machine. You can then move the required system from the Cluster system list to the Application failover targets list. Use the up and down arrow keys to set the order of systems in which VCS agent must failover applications.

If you want to specify a failover system that is not an existing cluster node, on the Configuration Inputs panel, click **Add System**, and in the Add System dialog box, specify the following details:

System Name or IP address	Specify the name or IP address of the system that you want to add to the VCS cluster.
Domain/Username	Specify the user name with administrative privileges on the system. Specify the user name must be in the *domain.com\username format*. If you want to specify the same user account on all systems that you want to add, check the **Use the specified user account on all systems** box.
Password	Specify the password for the account you specified.
Use the specified user account on all systems	This options is by default checked. You cannot modify this setting.

The wizard validates the details, and the system then appears in the Application failover target list.

4 Specify the user name and that VCS agents must use to perform domain operations such as Active Directory updates.

5 If you are adding a failover system from the existing VCS cluster, the Network Details panel does not appear.

If you are adding a new failover system to the existing cluster, on the Network Details panel, review the networking parameters used by existing failover systems. Appropriately modify the following parameters for the new failover system.

Note: The wizard automatically populates the networking protocol (UDP or Ethernet) used by the existing failover systems for Low Latency Transport communication. You cannot modify these settings.

- To configure links over ethernet, select the adapter for each network communication link. You must select a different network adapter for each communication link.
- To configure links over UDP, specify the required details for each communication link.

Network Adapter	Select a network adapter for the communication links. You must select a different network adapter for each communication link. Symantec recommends that one of the network adapters must be a public adapter and the VCS cluster communication link using this adapter is assigned a low priority. **Note:** Do not select the teamed network adapter or the independently listed adapters that are a part of teamed NIC.
IP Address	Select the IP address to be used for cluster communication over the specified UDP port.
Port	Specify a unique port number for each link. You can use ports in the range 49152 to 65535. The specified port for a link is used for all the cluster systems on that link.
Subnet mask	Displays the subnet mask to which the specified IP belongs.

6 If a virtual IP is not configured as part of your application monitoring configuration, the Virtual Network Details page is not displayed. Else, on the Virtual Network Details panel, review the following networking parameters that the failover system must use, and specify the NIC:

Virtual IP address	Specifies a unique virtual IP address.
Subnet mask	Specifies the subnet mask to which the IP address belongs.
Virtual name	Specifies a virtual name.
NIC	For each newly added system, specify the network adaptor that must host the specified virtual IP.

7 If the newly added failover system is associated with a different ESX host as compared to other systems, then on Target ESX Details page, specify the ESX host of the newly added failover system. Also specify the administrative user account details associated with the ESX host.

Note: If the application for which you are adding a failover system does not use storage attached directly to the ESX host, the wizard does not display this page.

If the new failover system runs on a different ESX host, or is configured to failover to another ESX host, specify that ESX host. To specify the ESX host, click **Add ESX Host** and on the Add ESX Host dialogue box, specify the following details, and then click **Next**:

ESX hostname or IP address	Specify the target ESX hostname or IP address. The virtual machines can fail over to this ESX host during vMotion. Specify an ESX host that has the same mount points as those currently used by the application.
User name	Specify a user account for the ESX host. The user account must have administrator privileges on the specified ESX host.
Password	Specify the password associated with the user name you specified.

The wizard validates the user account and the storage details on the specified ESX host, and uses this account to move data disks during vMotion.

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

9 On the Implementation panel, the wizard adds the specified system to the VCS cluster, if it is not already a part. It then adds the system to the list of failover targets. The wizard displays a progress report of each task.

- If the wizard displays an error, click **View Logs** to review the error description, troubleshoot the error, and re-run the wizard from the Symantec High Availability tab.
- Click **Next**.

10 On the Finish panel, click **Finish**. This completes the procedure for adding a failover system. You can view the system in the appropriate row of the application table.

Similarly you can also remove a system from the list of application failover targets.

Note: You cannot remove a failover system if an application is online or partially online on the system.

To remove a failover system

1. In the appropriate row of the application table, click **More** > **Remove Failover System**.
2. On the Remove Failover System panel, click the system that you want to remove from the monitoring configuration, and then click **OK**.

Note: This procedure only removes the system from the list of failover target systems, not from the VCS cluster. To remove a system from the cluster, use VCS commands. For details, see the *Symantec Cluster Server Administrator's Guide*.

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 Cluster Server (VCS) 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, VCS freezes the application configuration.

The **Enter Maintenance Mode** link is automatically dimmed if the application is already in maintenance mode. Conversely, if the application is not in maintenance mode, the **Exit Maintenance Mode** link is dimmed.

The Symantec High Availability tab provides the following options:

To enter maintenance mode

1. In the appropriate row, click **More**> **Enter Maintenance Mode**.

   During the time the monitoring is suspended, Symantec high availability solutions do 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, VCS takes no action.

2. While in maintenance mode, if a virtual machine restarts, if you want application monitoring to remain in maintenance mode, then in the Enter Maintenance Mode panel, check the **Suspend the application availability even after reboot** check box, and then click **OK** to enter maintenance mode.

To exit the maintenance mode

1. In the appropriate row, click **More**> **Exit Maintenance Mode**, and then click **OK** to exit maintenance mode.
2. Click the Refresh icon in the top right corner of the Symantec High Availability tab, to confirm that the application is no longer in maintenance mode.

To clear Fault state

When you fix an application fault on a system, you must further clear the application Faulted state on that system. Unless you clear the Faulted state, VCS cannot failover the application on that system.

You can use the Symantec High Availability tab to clear this faulted state at the level of a configured application component (resource).

The Clear Fault link is automatically dimmed if there is no faulted system in the cluster.

To clear Fault state

1. In the appropriate row of the application table, click **More** > **Clear Fault state**.
2. In the Clear Fault State panel, click the system where you want to clear the Faulted status of a component, and then click **OK**.

To resolve a held-up operation

When you try to start or stop an application, in some cases, the start or stop operation may get held-up mid course. This may be due to VCS detecting an incorrect internal state of an application component. You can resolve this issue by using the resolve a held-up operation link. When you click the link, VCS appropriately resets the internal state of any held-up application component. This process prepares

the ground for you to retry the original start or stop operation, or initiate another operation.

To resolve a held-up operation

1. In the appropriate row of the application table, click **More** > **Resolve a held-up operation**.
2. In the Resolve a held-up operation panel, click the system where you want to resolve the held-up operation, and then click **OK**.

To determine application state

The Symantec High Availability tab displays the consolidated health information of all applications configured for monitoring in a VCS cluster. The tab automatically refreshes the application health information every 60 seconds.

If you do not want to wait for the automatic refresh, you can instantaneously determine the state of an application by performing the following steps:

To determine application state

1. In the appropriate row of the Application table, click **More** > **Determine Application State**.
2. In the Determine Application State panel, select a system and then click **OK**.

Note: You can also select multiple systems, and then click **OK**.

To remove all monitoring configurations

To discontinue all existing application monitoring in a VCS cluster, perform the following step:

- On the Symantec High Availability tab, in the Title bar, click **Actions** > **Unconfigure all applications**. When a confirmation message appears, click **OK**.

To remove VCS cluster configurations

If you want to create a different VCS cluster, say with new systems, a different LLT protocol, or secure communication mode, you may want to remove existing VCS cluster configurations. To remove VCS cluster configurations, perform the following steps:

Note: The following steps deletes all cluster configurations, (including networking and storage configurations), as well as application-monitoring configurations.

- On the Title bar of the Symantec High Availability tab, click **Actions** >**Unconfigure VCS cluster**.
- In the Unconfigure VCS Cluster panel, review the Cluster Name and Cluster ID, and specify the User name and Password of the Cluster administrator.
  For non-secure clusters, specify the user name and password credentials of a domain user with local administrative privileges on each VCS cluster node, and then click **OK**.

Administering application monitoring settings

The Symantec High Availability tab lets you define and modify settings that control application monitoring with Symantec Cluster Server (VCS). You can define the settings on a per application basis. The settings apply to all systems in a VCS cluster, where that particular application is configured for monitoring.

The following settings are available:

- **App.StartStopTimeout**: When you click the **Start Application** or **Stop Application**, or **Switch Application** links in the Symantec High Availability tab, VCS initiates an application start or stop, respectively. This option defines the number of seconds that VCS must wait for the application to start or stop, after initiating the operation. You can set a value between 0 and 300 seconds for this attribute; the default value is 30 seconds.
  If the application does not respond in the stipulated time, the tab displays an alert. The alert states that the operation may take some more time to complete and that you must check the status after some time. A delay in the application response does not indicate that the application or its dependent component has faulted. Parameters such as workload, system performance, and network bandwidth may affect the application response. VCS continues to wait for the application response even after the timeout interval elapses.
  If the application fails to start or stop, VCS takes the necessary action depending on the other configured remedial actions.
- **App.RestartAttempts**: This setting defines the number of times that VCS must try to restart a failed application. The value of App.RestartAttempts may vary between 0 and 5; the default value is 0. If an application fails to start within the specified number of attempts, VCS fails over the application to a configured failover system.
- **App.DisplayName**: This setting lets you specify an easy-to-use display name for a configured application. For example, Payroll Application. VCS may internally

use a different application name to uniquely identify the application. However, the internal string, for example OraSG2, may not be intuitive to understand, or easy to recognize while navigating the application table.

Moreover, once configured, you cannot edit the application name, while you can modify the application display name as required. Note that the Symantec High Availability tab displays both the application display name and the application name.

Administering application availability using Symantec High Availability dashboard

The Symantec High Availability Dashboard is a consolidated graphic user interface that lets you administer application monitoring on systems in a VMware vCenter-administered data center.

The dashboard is fully integrated with the VMware vSphere Client GUI. The dashboard appears in the Symantec High Availability tab of the VMware vSphere Client GUI. To view the dashboard, select a data center or an ESX cluster in the inventory, and then click the Symantec High Availability tab.

Note: To administer application availability using the dashboard, single sign-on between the system and Symantec High Availability Console must be configured. Also, the application-specific agent must be appropriately configured.

For more information, see the *Symantec High Availability Solution Guide for VMware*.

On the dashboard, you can view the aggregate health statistics for monitored applications across a data center. You can also drill down to an ESX cluster and view monitored applications running in that cluster.

To understand how to navigate across the dashboard:

See "Understanding the dashboard work area" on page 85.

You can drill down to an individual application and perform the following administrative actions:

- Start application
- Stop application
- Enter maintenance mode
- Exit maintenance mode
- Switch application (to another system)

Apart from applications on systems running Symantec Cluster Server, the Symantec High Availability Dashboard also displays applications running on Symantec ApplicationHA guests (versions 6.0 and 5.1 SP2).

For more information on monitoring applications running on Symantec ApplicationHA guests:

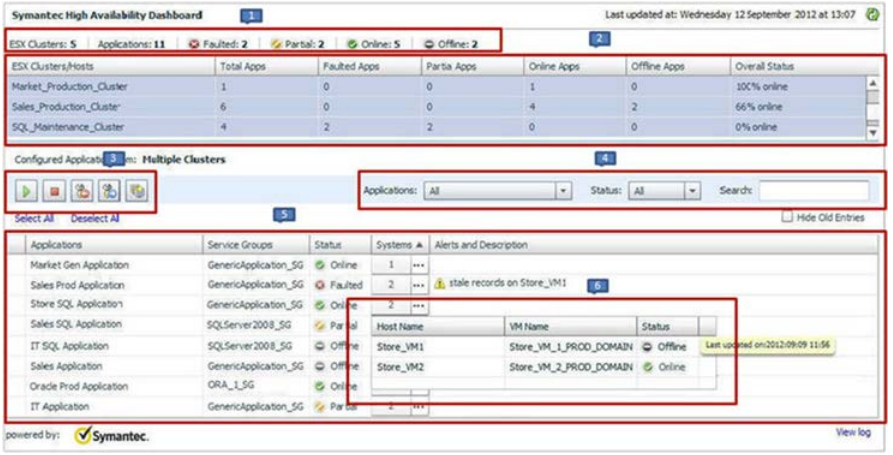
See "Monitoring applications running on Symantec ApplicationHA guests" on page 90.

Understanding the dashboard work area

The Symantec High Availability dashboard displays the aggregate application health status information for a datacenter or an ESX cluster.

Depending on whether you click a datacenter or a VMware cluster in the inventory view (left pane) of the VMware vSphere Client GUI, the dashboard displays the aggregate application status information. Apart from the application table described in detail below, the dashboard uses color code and tool tips to indicate the status of an application.

The following figure illustrates the dashboard work area. Note that the red boxes highlight the key GUI elements:



In the above figure, the labels stand for the following elements of the dashboard

1	Aggregate status bar	**2**	ESX cluster/host table	**3**	Taskbar
4	Filters menu	**5**	Application table	**6**	Systems table (dropdown)

Aggregate status bar

The aggregate status bar of the dashboard displays the following details:

- Number of ESX clusters that have applications configured for monitoring with VCS
- Number of configured applications in the selected data center
- Number of faulted applications
- Number of applications in partial state
- Number of online applications
- Number of offline applications

ESX cluster/host table

The Symantec High Availability dashboard displays this table only if you click a datacenter in the inventory view of the vSphere Client, and then click the Symantec High Availability tab.

The cluster table lists the following statistics per ESX cluster (or independent ESX host) in the data center:

- Number of configured applications
- Number of faulted applications
- Number of applications in partial state
- Number of online applications
- Number of offline applications
- Overall status (percentage of healthy applications)

If you click a row in the ESX cluster/host table, the application table of the dashboard displays monitored applications running on systems hosted by the selected ESX cluster or ESX host (an ESX server that is not part of an ESX cluster).

Note: This is the only method to navigate to applications running on systems hosted by standalone ESX hosts, by using the Symantec High Availability dashboard.

Taskbar

The taskbar displays icons for various administrative tasks. A tool tip highlights the task that each icon represents.

The dashboard supports the following tasks:

- Start Application: Starts a configured application
- Stop Application: Stops a configured application
- Enter Maintenance Mode: Suspends application monitoring of the configured application. In maintenance mode, VCS does not monitor the state of the application, and its dependent components.
- Exit Maintenance Mode: Resumes application monitoring for a configured application.
- Switch Application: Switches and an application gracefully from one system to another.

Filters menu

The filters menu lets you dynamically filter the applications that are displayed in the applications table. You can filter the applications by the following parameters:

- Application name
- Application status
- Search (by a string)

Application table

If you click an ESX cluster in the ESX cluster/host table, or in the inventory view of the VMware vSphere Client, then the list of applications running in that ESX cluster appears in the application table of the dashboard.

If you click an ESX host (an ESX server that is not part of an ESX cluster) in the ESX cluster/host table, then the list of applications that are configured on systems hosted by that ESX server appears. Note that this is the only route to navigate to such applications through the dashboard

The following table lists each column in the application table and its description:

Column	Description
Applications	Indicates the application name.
Service Groups	Indicates the group of critical application components that VCS uses to determine the health of a monitored application. Service group is a VCS term. The equivalent term in Symantec ApplicationHA terminology is “component group”. VCS may use more than one service group to monitor a complex application. The dashboard displays each service group of such an application as a separate instance of that application.

Column	Description
Status	This column indicates the effective status of an application in a VCS cluster. It does not indicate the state of the application on per member system. For example, in a two-system cluster, if the application has faulted on one system but has failed over to another system, then this column states the state of the application as Online. Indicates one of the following states of an application: ■ Online ■ Offline ■ Faulted ■ Partial **Note:** After you perform an administrative task such as starting or stopping an application, or entering or exiting maintenance mode, it takes a few seconds for the dashboard to reflect the revised status of the configured application.
Systems	Indicates the number of systems where the application is configured for monitoring. To view more information about all such systems, click the **(…)** icon. The System table (dropdown) appears, listing the ESX host name of each configured system, the VM name (system name), and the status of the application on each system.
Alerts and description	Displays a triangular alert icon **(!)** and describes the reason for the alert. This column displays alerts in two cases: a) If the application status record is stale; b) If the application has faulted on a system. For stale records, the column includes the timestamp of the last received health record. In case of application fault, the column provides details of the system where the fault occurred.

Accessing the dashboard

You can use the Symantec High Availability dashboard to perform one of the following actions:

- Identify all instances and failover systems of one or more applications running in a data center
- Drill down to a specific application, and perform an administrative action on the application
- View alerts for faulted applications and stale application health reports

Prerequisites for accessing the dashboard

Before you access the Symantec High Availability dashboard to administer an application, ensure:

- Single sign-on is configured between the Symantec High Availability Console and the systems hosting the monitored applications
- Symantec High Availability Console is able to communicate with Symantec High Availability guest components on designated port (port 5634).
- The application that you want to administer is configured for application monitoring with Symantec High Availability

How to access the dashboard

When you install Symantec High Availability guest components, the product installation script or wizard automatically installs the required dashboard components. As a result, the Symantec High Availability Dashboard appears in the **Symantec High Availability** tab of the vSphere Client.

You must, however, ensure that Symantec High Availability is successfully installed and that you have adequate user privileges to access the dashboard.

To access dashboard

Perform the following step:

- In the inventory view (left pane) of the vSphere Client, click a datacenter or a VMware cluster. In the right pane, to view the Symantec High Availability dashboard, click the Symantec High Availability tab.

Who can access the dashboard

To access High Availability dashboard, the VMware vCenter administrator must assign one the following roles to you:

- Guest: View application state
- Operator: View application state and perform administrative actions
- Admin: View application state and perform administrative actions. You can also configure application availability monitoring in this role, but not from the dashboard.

Monitoring applications across a data center

If you click a data center in the inventory view of the VMware vSphere Client, and then click the Symantec High Availability tab, the dashboard appears, displaying the aggregate health information of applications running inside various ESX clusters.

You can use filters to drill down from all applications running across the data center and view a single application and its various instances in the data center.

Monitoring applications across an ESX cluster

If you click an ESX cluster in the inventory view of the VMware vSphere Client, and then click the tab, the dashboard displays the consolidated information on the systems and applications running in the ESX cluster. The dashboard also displays the application health and application monitoring information.

You can use filters to drill down from all applications running in the ESX cluster, to view a single application and its various instances in the ESX cluster.

Monitoring applications running on Symantec ApplicationHA guests

Symantec High Availability dashboard displays applications running on Symantec ApplicationHA guests as well as those running on Symantec Cluster Server systems. The dashboard presents a unified view of monitored applications on the two types of systems in a data center.

For easy application monitoring, the dashboard displays an application-centric view, not a product-centric view. You cannot therefore always determine which application is under the control of which Symantec High Availability product.

However, you can conclude that applications configured for failover are under VCS control. Applications configured for monitoring without a failover system may either be under VCS control or under ApplicationHA control.

Searching for application instances by using filters

The High Availability dashboard lets you search for all instances of a particular application in the selected datacenter or an ESX cluster. Various filters enable to search for the application that you want to monitor. You can use multiple filters simultaneously to search for an application.

The following table lists each field in the filter menu and its description:

Field	Description
Application	Lets you specify the name of the application that you want to filter in the application table. A drop-down list displays all the applications that are configured in the datacenter or ESX cluster. Click to select the name of the application that you want to filter.

Field	Description
Status	Lets you specify the status of the application by which you want to filter the application table. A drop-down list displays the following status values: Online, Offline, Faulted, and Partial.
Search	Lets you search for an application by using a string or pattern of characters. Enter the string using which you want to filter applications. As you enter the string in the Search box, the dashboard dynamically filters the applications. **Note:** The dashboard searches for the specified string in the Systems column.

Selecting multiple applications for batch operations

You can select one or more instances of an application for administering by using the dashboard as follows:

- To select one application instance, click inside the row of that application instance.
- To select various instances, keep the **Control** key pressed and then click inside the row of each instance.
- To select a batch of consecutive entries in the application table, keep the **Shift** key pressed, click inside the row of the first instance, and then click inside the row of the last instance. Alternatively, you can keep the **Shift** key pressed and drag the mouse to mark a block of consecutive entries.
- To select all instances in the application table, click **Select All**.

Starting an application using the dashboard

To start an application, perform the following steps in the application table of the dashboard.

To start an application

1. Filter the applications that you want to start.

   See "Searching for application instances by using filters" on page 90.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to perform a batch operation.

   See "Selecting multiple applications for batch operations" on page 91.

3 To start the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

4 In the Start Application panel, click the systems where you want to start the application. Note that you can start the application on any of the systems displayed for each application.

Click **OK**.

Stopping an application by using the dashboard

To stop an application on one or more virtual machines, perform the following steps in the application table of the High Availability dashboard.

To stop an application

1 Filter the applications that you want to stop.

See "Searching for application instances by using filters" on page 90.

The application table displays all the instances of the filtered applications.

2 If required, select multiple applications or instances to perform a batch operation.

See "Selecting multiple applications for batch operations" on page 91.

3 To stop the application, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

4 In the Stop Application panel, from the dropdown list, click the systems where you want to stop the application.

Click **OK**.

Entering an application into maintenance mode

You may need to intentionally take an application offline for maintenance purposes, without triggering a corrective response from Symantec Cluster Server (VCS).

To enter an application into maintenance mode, perform the following steps in the application table of the High Availability dashboard.

Note: The maintenance mode configuration is application-specific, not system-specific.

To enter maintenance mode

1. Filter the application that you want to gracefully take offline for maintenance.

   See "Searching for application instances by using filters" on page 90.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to perform a batch operation.

   See "Selecting multiple applications for batch operations" on page 91.
3. To enter maintenance mode, in the taskbar, click the appropriate icon for entering maintenance mode (use the tool tip to recognize the appropriate icon).
4. If a system restarts while the application is in maintenance mode, and you want the application to remain in maintenance mode, then in the Enter Maintenance Mode panel, check the **Suspend the application availability even after reboot**.
5. On the Enter Maintenance Mode panel, click **OK**.

Bringing an application out of maintenance mode

To bring an application out of maintenance mode on one or more systems, perform the following steps in the application table of the High Availability dashboard.

To exit maintenance mode

1. Filter the applications that you want to bring out of maintenance mode.

   See "Searching for application instances by using filters" on page 90.

   The application table displays all the instances of the filtered applications.
2. If required, select multiple applications or instances to bring out of maintenance mode.

   See "Selecting multiple applications for batch operations" on page 91.
3. To bring the applications out of maintenance mode, in the taskbar, click the appropriate icon for exiting maintenance mode (use the tool tip to recognize the appropriate icon).
4. In the Exit Maintenance Mode panel, click **OK**.

Switching an application

To gracefully switch an application from one system to another, perform the following steps in the application table of the dashboard.

Note: You can switch an application only if the application monitoring configuration includes one or more failover systems.

To switch an application

1. Filter the applications that you want to switch to another node.

   See "Searching for application instances by using filters" on page 90.

   The application table displays all the instances of the filtered applications.

2. If required, select multiple applications or instances to perform a batch operation.

   See "Selecting multiple applications for batch operations" on page 91.

3. To switch the applications, in the taskbar, click the appropriate icon (use the tool tip to recognize the appropriate icon).

4. In the Switch Application panel, select the systems where you want to switch the applications, and then click **OK**. Symantec Cluster Server takes the applications offline on the existing systems, and brings them online on the systems that you specified.

Resolving dashboard alerts

The Alerts and Description column in the application table of the High Availability dashboard marks application alerts with the alert **(!)** icon. This occurs in the following cases:

- Stale entries: Stale entries occur either due to a system (virtual machine) issues or connectivity issues. When this occurs, the system fails to send application heartbeats to the dashboard. If the system fails to send the heartbeat for two consecutive heartbeat intervals, the dashboard displays the alert icon.

  Note: You can filter stale entries using the **Search** option and searching with the string "stale".

- Application faults: Application faults may occur due to reasons beyond Symantec Cluster Server (VCS) control, such as storage failure. In such cases, you must investigate and appropriately resolve the issue, and then clear the Faulted status of the application. To view only application fault alerts, in the Alerts and Description column, click the **Hide Old Entries** check box.

Note: It is important that you fix application faults, and then clear the Fault status. Else, the VCS cannot fail over applications to the faulted system, and application availability may be compromised. For more information, See "To clear Fault state" on page 81.

Deleting stale records

VCS uses a heartbeat mechanism to monitor the health of a configured application. If a system fails to send two consecutive heartbeats for an application, VCS marks the health status of that application as stale. The Alerts and Description column of the High Availability Dashboard indicates the time elapsed since the last valid health status was recorded.

After troubleshooting the heartbeat failure, you can delete such stale records from the High Availability database.

To delete stale records

1. On the Console host, navigate to the home directory.

   For example:

   ```
   C:\Program Files\Veritas\
   ```

   Where C:\ is the system drive.

2. Run the following command:

   ```
   C:\Program Files\Veritas\VRTSsfmh\bin>perl.exe C:\Program
   Files\Veritas\ApplicationHA
   \bin\delete_stale_records.pl<TimeInterval>
   ```

   Where Time Interval, in minutes, indicates how stale the records must be, for them to be deleted. By default, the script deletes all records that are older than 60 minutes

Appendix A

Troubleshooting

This appendix includes the following topics:

- Troubleshooting application monitoring configuration issues
- Troubleshooting Symantec High Availability tab view issues
- Troubleshooting dashboard issues
- About error logging- VMware SRM environment
- All VCS cluster systems fail to start at the same time- VMware SRM environment

Troubleshooting application monitoring configuration issues

This section lists common troubleshooting scenarios that you may encounter while or after configuring application monitoring.

Symantec High Availability Configuration Wizard displays blank panels

The Symantec High Availability Configuration Wizard may fail to display the wizard panels. The window may appear blank.

Verify that the Symantec ApplicationHA Service is running on the Symantec High Availability Console host and then launch the wizard again.

The Symantec High Availability Configuration wizard displays the "hadiscover is not recognized as an internal or external command" error

While configuring application monitoring the Symantec High Availability Configuration wizard may display the "hadiscover is not recognized as an internal or external command" error, after you click Next on the Application Selection panel.

This issue occurs if you launch the wizard from a system where you have reinstalled the Symantec High Availability guest components.

Workaround: Exit the wizard, restart the Veritas Storage Foundation Messaging Service and then re-run the wizard.

Running the ‘hastop –all’ command detaches virtual disks

The 'hastop –all' command takes offline all the components and components groups of a configured application, and then stops the VCS cluster. In the process, the command detaches the virtual disks from the VCS cluster nodes. (2920101)

Workaround: If you want to stop the VCS cluster (and not the applications running on cluster nodes), instead of the “hastop –all”, use the following command:

```
hastop -all -force
```

This command stops the cluster without affecting the virtual disks attached to the VCS cluster nodes.

Troubleshooting Symantec High Availability tab view issues

This section lists common troubleshooting scenarios that you may encounter when using the Symantec High Availability tab.

Tab displays only HAD-related error and Unconfigure VCS Cluster link

The Symantec High Availability tab appears blank except for the following HAD-related error message:

```
Unable to retrieve the VCS cluster details.
The cluster is either not responding or is not accepting
the client connection requests.
You may have to unconfigure the cluster and then configure
it again.
```

The Unconfigure VCS Cluster link also appears in the tab. (2828764)

Workaround: Click the **Unconfigure VCS Cluster** link, and then proceed with the steps. For more information on this procedure:

See "To remove VCS cluster configurations" on page 82.

You can then freshly configure the VCS cluster and application monitoring to monitor application availability.

An alert icon appears in the Symantec High Availability tab

An Alert icon appears in the title bar of the Symantec High Availabiity tab of the vSphere Client GUI only if the communication between Symantec High Availability Console and a failover system fails. As a result, the Symantec High Availability dashboard fails to display the system, or displays stale application health data for the system.

Workaround:

Perform the following steps

1. Configure single sign-on between the Symantec High Availability Console host and the system.

   For information on configuring single sign-on, see the *Symantec High Availability Console Installation and Upgrade Guide*.

2. Bring the VCSInfraSG group online:

   ```
   # hagrp -online VCSInfraSG -any
   ```

High Availability tab not visible from a cluster node

If you click a system in the inventory view of the VMware vSphere client GUI, then the Symantec High Availability tab displays the cluster view (consolidated cluster-level health information of the configured application/s running on the selected system). In some multi-node cluster, the view is not visible from at least one of the cluster nodes.

This behavior occurs if connectivity of the configured LLT links fail. This may be a networking error. (2863649)

Workaround

Ensure that valid LLT links are configured for the affected cluster node, and then retry.

Symantec High Availability tab does not display the application monitoring status

The Symantec High Availability tab in the vSphere Client console may either display a HTTP 404 Not Found error or may not show the application health status at all.

Verify the following conditions and then refresh the Symantec High Availability tab in the vSphere Client console:

- Verify that the Symantec High Availability Console host is running and is accessible over the network.
- Verify that the VMware Web Service is running on the vCenter Server.
- Verify that the VMware Tools Service is running on the guest virtual machine.
- Verify that the Veritas Storage Foundation Messaging Service (xprtld process) is running on the Symantec High Availability Console and the virtual machine. If it is stopped, type the following on the command prompt:

  ```
  net start xprtld
  ```
- Verify that ports 14152, 14153, and 5634 are not blocked by a firewall.
- Log out of the vSphere Client and then login again. Then, verify that the Symantec High Availability plugin is installed and enabled.

Symantec High Availability tab may freeze due to special characters in application display name

For a monitored application, if you specify a display name that contains special characters, one or both of the following symptoms may occur:

- The Symantec high availability tab may freeze
- The Symantec high availability tab may display an Adobe exception error message

  Based on your browser settings, the Adobe exception message may or may not appear. However, in both cases the tab may freeze. (2923079)

  Workaround: Reset the display name using only those characters that belong to the following list:

  - any alphanumeric character
  - space
  - underscore

  Use the following command to reset the display name:

  hagrp -modify *sg name* UserAssoc -update Name *modified display name without special characters*

In the Symantec High Availability tab, the Add Failover System link is dimmed

If the system that you clicked in the inventory view of the vSphere Client GUI to launch the Symantec High Availability tab is not part of the list of failover target systems for that application, the Add Failover System link is dimmed. (2932281)

Workaround: In the vSphere Client GUI inventory view, to launch the Symantec High Availability tab, click a system from the existing list of failover target systems for the application. The Add Failover System link that appears in the drop-down list if you click **More**, is no longer dimmed.

Troubleshooting dashboard issues

This section lists common troubleshooting scenarios that you may encounter when using the Symantec High Availability Dashboard:

Task-specific panels launched from dashboard, do not display description for alerts

When you perform administrative tasks such as starting or stopping an application using the Symantec High Availability Dashboard, a task-specific panel appears. In the panel, you can specify the system where you want to perform the administrative task. For some the configured systems listed in the panel, an alert icon appears. However, no description for the reason of the alert is displayed.

The alert icon (!) typically appears when a system reports a stale application health record, or an application fault. Without known such information about the alert, it may be difficult to select the appropriate system for the administrative task. (2919069)

Workaround

Navigate to the appropriate row in the Application table of dashboard. Alert details, such as time stamp of the stale record, are displayed in the Alerts and Description column.

Reporting on the Dashboard

The Dashboard may not report one or more configured failover systems. This can happen:

- If one or more failover systems have MAC addresses that are already in use by other virtual machines in the same datacenter.
  Workaround: Ensure that the cluster systems have unique MAC addresses.

- If one or more cluster systems have not established single sign-on (SSO) with Symantec High Availability Console.
  Workaround: Perform the following steps:
  - a) In the Inventory view of the vSphere Client GUI, navigate to the required virtual machine.
  - Click the Symantec High Availability tab.
  - Enter the username and password of the virtual machine to configure SSO with the Symantec High Availability Console.

About error logging- VMware SRM environment

The error log "healthview_A.txt " is generated for the errors that may occur while executing the application monitoring command step in the SRM recovery plan.

The log file is located at the following path on the virtual machine:

```
C:\Program Files\Veritas\cluster server\log
```

All VCS cluster systems fail to start at the same time- VMware SRM environment

In a SRM recovery plan, Symantec recommends to add all the VCS cluster systems under the same priority order. This ensures that all the virtual machines are started at the same time and the application dependency group is brought online successfully.

However, if due to any network issues all the VCS cluster systems do not start at the same time, then VCS cluster fails to start and the application monitoring continuity is lost.

Workaround: You must manually seed the VCS cluster.

For more details on seeding a cluster, refer to the *Veritas™ Cluster Server Administrator's Guide*.