Symantec™ High Availability Agent for WebSphere MQ Installation and Configuration Guide

Windows

6.1

December 2014

Symantec

Symantec High Availability Agent Symantec Agent Pack for WebSphere MQ Installation and Configuration Guide

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

Agent 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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Contents

Technical Support 4

Chapter 1 Introducing the Symantec High Availability Agent for WebSphere MQ 10

About the Symantec High Availability agent for WebSphere MQ 10
Supported software 11
Agent functions 11
Online 11
Offline 11
Monitor 11
Clean 12

Chapter 2 Installing, upgrading, and removing the agent for WebSphere MQ 13

Before you install the agent for WebSphere MQ 13
Installing the VCS agent for WebSphere MQ 13
Removing the VCS agent for WebSphere MQ 15
Upgrading the agent for WebSphere MQ 16

Chapter 3 Configuring the agent for WebSphere MQ 18

About configuring the agent for WebSphere MQ 18
Agent attributes for WebSphere MQ 18
Executing a custom monitor program 22

Chapter 4 Configuring the service group for WebSphere MQ using the Symantec High Availability Configuration wizard 23

Typical VCS cluster configuration in a virtual environment 24
About configuring application monitoring using the Symantec High Availability solution for VMware 25
Getting ready to configure VCS service groups using the wizard 26
Before configuring application monitoring 27
Launching the Symantec High Availability Configuration wizard 28

Configuring the WebSphere MQ queue manager for high availability 29
Configuring the VCS cluster 30
Configuring the application 41
Understanding service group configurations 52
Resource dependency 53
Service group dependency 53
Infrastructure service groups 53
Understanding configuration scenarios 54
Configuring a single instance/multiple instances in VCS 54
Configuring multiple WebSphere MQ Queue Manager instances in VCS using multiple runs of the wizard 54
Configuring multiple applications 55
Symantec High Availability Configuration wizard limitations 55
Troubleshooting 56
Symantec High Availability Configuration wizard displays blank panels 56
The Symantec High Availability Configuration wizard displays the "hadiscover is not recognized as an internal or external command" error 56
Running the `hastop -all` command detaches virtual disks 56
Log files 56
Sample configurations 57
Sample VCS configuration file for single WebSphere MQ Queue Manager instance (VxVM) 57

Chapter 5 Configuring the service groups for WebSphere MQ Queue Manager 63

About configuring a service group for the agent for WebSphere MQ 63
Configuring a WebSphere MQ resource 63
Active-Passive configuration 64
Active-Active configuration 64
Configuring a WebSphere MQ Listener 66

Chapter 6 Troubleshooting the agent for WebSphere MQ 67

Using correct software and operating system versions 67
Meeting prerequisites 67
Configuring WebSphere MQ Queue Manager resources 68
Starting the WebSphere MQ Queue Manager outside a cluster 68
Monitoring WebSphere MQ Queue Manager processes 68
Reviewing error log files 69

Reviewing VCS log files 69
Using WebSphere MQ log files 69
Using trace level logging 69

Appendix A Sample Configurations 71

About the sample configuration for the agent for WebSphere MQ 71
Sample agent type definition 71
Sample configuration for WebSphere MQ 72
Sample service group configuration for WebSphere MQ 74

Index 75

Chapter 1

Introducing the Symantec High Availability Agent for WebSphere MQ

This chapter includes the following topics:

- About the Symantec High Availability agent for WebSphere MQ
- Supported software
- Agent functions

About the Symantec High Availability agent for WebSphere MQ

Symantec High Availability agents monitor specific resources within an enterprise application, determine the status of these resources, and start or stop them according to external events.

The Symantec High Availability agent for WebSphere MQ manages the WebSphere MQ Queue Managers in a clustered environment. The agent can bring a specific WebSphere MQ Queue Manager online and monitor the state of the Queue Manager. The agent can also detect failures and can shut down the Queue Manager in case of a failure.

Supported software

For information on the software versions that the Symantec High Availability agent for WebSphere MQ supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Agent functions

Online

The online function performs the following tasks:

- Verifies that the WebSphere MQ Queue Manager is not already online.
- Uses an IBM provided start command to start the WebSphereMQ using the name of the Queue Manager.
- Ensures that the WebSphere MQ Queue Manager is up and running successfully. The function uses the wait period that the OnlineTimeout attribute specifies to enable the Queue Manager to initialize fully before allowing the monitor function to probe the resource.

Offline

The offline function performs the following tasks:

- Verifies that the WebSphere MQ Queue Manager is not already offline.
- Uses an IBM-provided stop command to stop the WebSphere MQ Queue Manager using the name of the Queue Manager.
- Ensures that the WebSphereMQ Queue Manager is given enough time to go offline successfully. The function uses a wait period that the OfflineTimeout attribute specifies, to allow the WebSphereMQ Queue Manager to complete the offline sequence before allowing further probing of the resource.

Monitor

The monitor function monitors the states of the WebSphere MQ Queue Managers running on all nodes within the cluster. The monitor function can monitor the following WebSphere MQ Queue Manager components:

- Queue Manager
- Channel Initiator
- Command Server (If the CommandServer attribute is set to 1)

The monitor function performs the following tasks:

- The first level check searches for all system processes that must be running for a WebSphereMQ Queue Manager. If the first level check does not find these processes running on the node, the check exits immediately, and reports the Queue Manager as OFFLINE.
- If the SecondLevelMonitor attribute is set to greater than 0, the monitor function performs a second level check to determine the status of the WebSphereMQ Queue Manager.
  The second level check executes the runmqsc command and pings the Queue Manager to see if the manager is up and running. This check ensures that the processes are truly available for MQ Queue processing.
- Depending upon the MonitorProgram attribute, the monitor function can perform a customized check using a user-supplied monitoring utility. For details about executing a custom monitor program:
  See "Executing a custom monitor program" on page 22.

Clean

In case of a failure or after an unsuccessful attempt to online or offline WebSphereMQ Queue Manager, the clean function removes any Queue Manager processes remaining in the system. The clean function performs the following tasks:

- Attempts to gracefully shut down the WebSphereMQ Queue Manager.
- If a graceful shutdown fails, the clean function looks for all the processes running for the WebSphereMQ Queue Manager, and cleans the processes.
- If the CommandServer attribute is set to 1 for WebSphere version 6.0, the clean function kills the Command Server processes associated with the WebSphere MQ Queue Manager.

Chapter 2

Installing, upgrading, and removing the agent for WebSphere MQ

This chapter includes the following topics:

- Before you install the agent for WebSphere MQ
- Installing the VCS agent for WebSphere MQ
- Removing the VCS agent for WebSphere MQ
- Upgrading the agent for WebSphere MQ

Before you install the agent for WebSphere MQ

Ensure that you install and configure Symantec Cluster Server before installing the agent for WebSphere MQ.

Installing the VCS agent for WebSphere MQ

Use the Product Installer to install the agent for WebSphere MQ.

Note: Ensure that you have uninstalled the previous version of this agent, if installed.

To install the VCS agent for WebSphere MQ

1. Log on to any node in the cluster.

   Ensure that the logged on user has the domain administrative privileges.

2. Download the Agent Pack from the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

   You can download the complete Agent Pack tar file or the individual agent tar file.

3. Uncompress the file to a temporary location.

4. If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

Windows 2003	`cd1\windows\w2k3\application\webspheremq_agent\`
	`vcs_version\version_agent\`
	`webspheremq_agt.5.0-GA_w2k3`

Windows 2003 (IA64)	`cd1\windows\w2k3IA64\vcs\application\webspheremq_agent\`
	`vcs_version\version_agent\`
	`webspheremq_agt.version-GA_w2k3IA64\Pkgs`

Windows 2003 (x64)	`cd1\windows\w2k3x64\vcs\application\webspheremq_agent\`
	`vcs_version\version_agent\`
	`webspheremq_agt.version-GA_w2k3x64\Pkgs`

Windows 2008 (x64)	For VCS 5.1:
	`cd1\windows\w2k8x64\vcs\application\webspheremq_agent\`
	`5.1\version_agent\version_agent\Pkgs`
	For VCS 6.0 and later:
	`cd1\windows\w2k8x64\vcs\application\webspheremq_agent\`
	`vcs_version\version_agent\Pkgs`

Windows 2012 (x64)	`cd1\windows\w2k12x64\vcs\application\webspheremq_agent\` `6.1\version_agent\Pkgs`

5 Double-click **vrtsvcswebspheremq.msi**.

Follow the instructions that the install program provides, to complete the installation of the Symantec High Availability agent for WebSphere MQ.

6 If you want to configure a WebSphere MQ queue manager for high availability, download and install the **vrtsvcswiz.msi** package from the following location:

```
cd1\windows\win\vcs\6.1\Pkgs\vrtsvcswiz.msi
```

Warning: Symantec recommends that if you have installed the VCS for Windows Agent Pack, you should *not* uninstall `vrtsvcswiz.msi`. Uninstalling this package removes the Symantec High Availability Configuration wizard files, and so, you cannot use the wizard to configure applications for high availability.

Removing the VCS agent for WebSphere MQ

Perform the following procedure to uninstall the agent for WebSphere MQ from a cluster. Perform these steps while the cluster is active.

To uninstall the VCS agent for WebSphere MQ

1 Ensure that all clustered VCS resources are offline.

2 From the cluster, remove all the resources that use the agent for WebSphere MQ.

3 Perform the following steps on each node from which you want to uninstall the agent. Ensure that you have a user with administrative privileges.

- Click **Start > Settings > Control Panel**.
  - On Windows 2008: Navigate to **Programs and Features**
  - On Windows 2008R2/2012: Navigate to **Programs**>**Programs and Features**
- From the list of programs, select **vrtsvcswebspheremq.msi**.

4 Click **Change/Remove**.

5 Follow the instructions that the uninstall program provides, to complete the uninstallation of the agents for WebSphere MQ.

Upgrading the agent for WebSphere MQ

Perform the following steps to upgrade the agent with minimal disruption, in a VCS environment.

To upgrade the agent in a VCS environment

1. Login as domain administrator.
2. Verify that your path is *drive*:\Program Files\Veritas\Cluster Server\bin
3. Persistently freeze all the service groups that host the application:

   ```
   C:\> hagrp –freeze GroupName -persistent
   ```

4. Stop the cluster services forcibly:

   ```
   C:\> hastop -all –force
   ```

5. Ensure that the agent operations are stopped on all the nodes.
6. Take a back up of the main.cf and types.cf files:

   ```
   C:\> copy drive:\> Program Files\Veritas\Cluster
   Server\conf\config\main.cf drive:\>backup\main.cf
   ```

   ```
   C:\> copy drive:\> Program Files\Veritas\Cluster
   Server\conf\config\types.cf drive:\>backup\types.cf
   ```

7. Uninstall the agent package from all the nodes.

   See “Removing the VCS agent for WebSphere MQ” on page 15.

8. Install the new agent on all the nodes.

   See “Installing the VCS agent for WebSphere MQ” on page 13.

9. Navigate to *drive*:\> Program Files\Veritas\Cluster Server\conf\config\types.cf file and verify if any duplicate type definitions exists for WebSphere MQ on all the nodes.

   If duplicate type definitions exist, remove old type definition from types.cf file and save the file.

   Note: To identify the old type definition, compare the new type definition file with the old (backed up) types.cf file.

10 Check for the changes in the resource values required, if any, due to the new agent types definition.

Note: To note the list of changed attributes, compare the new type definition file with the old type definition file.

---

11 Start VCS on all nodes in the cluster:

```
C:\> hastart
```

12 Start the agent on all nodes:

```
C:\> haagent -start WebSphereMQ -sys SystemName
```

13 Unfreeze the service groups once all the resources come to an online steady state:

```
C:\> hagrp -unfreeze GroupName -persistent
```

Chapter 3

Configuring the agent for WebSphere MQ

This chapter includes the following topics:

- About configuring the agent for WebSphere MQ
- Agent attributes for WebSphere MQ
- Executing a custom monitor program

About configuring the agent for WebSphere MQ

After installing the agent for WebSphere MQ, you can create and configure a WebSphere MQ Queue Manager resource. Before you configure a resource, review the attributes table that describes the WebSphere MQ Queue Manager resource type and its attributes.

Agent attributes for WebSphere MQ

Table 3-1 shows the required attributes for configuring a WebSphere MQ Queue Manager.

Table 3-1 Required attributes

Required attributes	Description
Home	The absolute path to the WebSphereMQ installation directory. This attribute is used to locate programs executed by the agent, such as strmqm.exe. Type and dimension: string-scalar Default: No default value Example: c:\Program Files\IBM\WebSphere MQ
Domain	Specifies the Windows domain name to which the specified user belongs. If the attribute value for User does not belong to a Windows domain, use VCS localization settings to specify the local computer name for each system. Type and dimension: string-scalar Default: No default value Example: ISV-DOMAIN
Password	Password for the user. Use the vcsencrypt -agent command to encrypt the password. If you are using the VCS GUI, the GUI automatically encrypts the password. Refer to the VCS documentation for more information about VCSEncrypt. Type and dimension: string-scalar Default: No default value
CommandServer	Decides whether the monitor operation must monitor the command server process or not. This attribute is applicable for WebSphere version 6.0 only. If you set this attribute to 1, the agent for WebSphere MQ monitors the command server process, amqpcsea. If this process faults, the agent for WebSphere MQ restarts the process. If you set this attribute to 0, the agent for WebSphere MQ does not monitor the amqpcsea process. Type and dimension: string-scalar Default: 0 Example: 1

Table 3-1 Required attributes *(continued)*

Required attributes	Description
User	Windows user name of the owner of the WebSphere MQ directories and executables. The agent operations use this name to execute all WebSphere MQ commands. This user name does not have to be unique within a cluster. Do not include the domain name when specifying this attribute; use the Domain attribute to specify domain requirements. Type and dimension: string-scalar Default: mqm Example: mqusr1
MQVer	Version of the WebSphere MQ Queue Manager. Supported version is 6.0. Type and dimension: string-scalar Default: 6.0
QueueManager	Name of the WebSphere MQ Queue Manager that the cluster server manages. You must uniquely define this attribute for each Queue Manager within the cluster. This attribute also uniquely identifies the processes running for a specific WebSphere MQ Queue Manager. Type and dimension: string-scalar Default: No default value Example: venus.queue.manager

Table 3-1 Required attributes *(continued)*

Required attributes	Description
ResLogLevel	Specifies the logging detail performed by the agent for the resource. Valid values are: ■ INFO: Logs error messages. ■ TRACE: Logs error and trace messages. TRACE is very verbose and should only be used during initial configuration or for troubleshooting and diagnostic operations. To see trace messages while agent entry point is executing, add value DBG_21 to LogDbg attribute of WebSphereMQ resource type and set ResLogLevel attribute value to TRACE. Type and dimension: string-scalar Default: INFO Example: TRACE

Table 3-2 shows the optional attributes for configuring a WebSphere MQ Queue Manager.

Table 3-2

Optional attributes	Description
MonitorProgram	Absolute path name of an external, user-supplied monitor executable. For information about setting this attribute: See "Executing a custom monitor program" on page 22. Type and dimension: string-scalar Default: No default value
SecondLevelMonitor	Specifies if second-level monitor is enabled and how frequently it is performed. Second-level monitor is a deeper, more thorough state check of the configured WebSphere MQ resource, performed by executing the runmqsc.exe utility. Type and dimension: integer-scalar Default: 0 Example: 1

Executing a custom monitor program

The monitor function executes a custom monitor program to perform a user-defined WebSphere MQ Queue Manager state check.

The monitor function executes the MonitorProgram if the following conditions are true:

- The specified utility is a valid executable file.
- The first level process check indicates that the WebSphere MQ Queue Manager is online.
- The SecondLevelMonitor attribute is either set to 0 or 1, and the second level check indicates that the WebSphere MQ Queue Manager is online.
- The SecondLevelMonitor attribute is set to greater than 1, but the second level check is deferred for this monitoring cycle.

The monitor operation interprets the program exit code as follows:

110 or 0	WebSphere MQ Queue Manager is ONLINE
100 or 1	WebSphere MQ Queue Manager is OFFLINE
99	WebSphere MQ Queue Manager is UNKNOWN
Any other value	WebSphere MQ Queue Manager is UNKNOWN

To ensure that the custom monitor program is always available to the agent application, Symantec recommends storing the file in a shared directory that is available on an online node.

Chapter 4

Configuring the service group for WebSphere MQ using the Symantec High Availability Configuration wizard

This chapter includes the following topics:

- Typical VCS cluster configuration in a virtual environment
- About configuring application monitoring using the Symantec High Availability solution for VMware
- Getting ready to configure VCS service groups using the wizard
- Before configuring application monitoring
- Launching the Symantec High Availability Configuration wizard
- Configuring the WebSphere MQ queue manager for high availability
- Understanding service group configurations
- Understanding configuration scenarios
- Symantec High Availability Configuration wizard limitations
- Troubleshooting
- Sample configurations

Typical VCS cluster configuration in a virtual environment

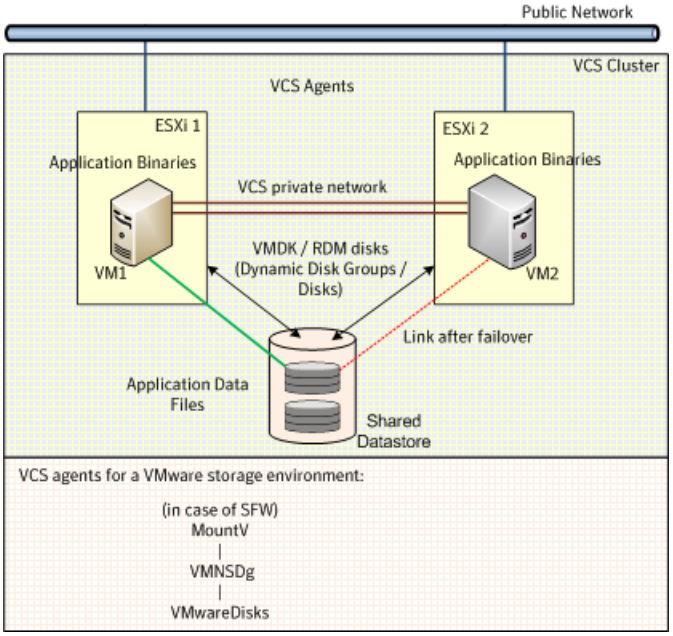
A typical VCS cluster configuration for WebSphere MQ Queue Manager, in a VMware virtual environment involves two or more virtual machines. The virtual machine on which the application is active, accesses a non-shared VMware VMDK or RDM disk that resides on a VMware datastore.

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.

Figure 4-1 Typical WebSphere MQ Queue Manager cluster configuration in a VMware virtual environment



About configuring application monitoring using the Symantec High Availability solution for VMware

Consider the following before you proceed:

- You can configure monitoring for WebSphere MQ 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 configuring application availability, the wizard also sets up the other components required for successful application monitoring.

- You must not suspend a system if an application is currently online on that machine. If you suspend a system, VCS moves the disks along with the application to another system. Later, when you try to restore the suspended system, VMware does not allow the operation because the disks that were attached before the system was suspended are no longer with the system. To suspend a virtual machine, ensure that the application being monitored is not online on that system.

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

Getting ready to configure VCS service groups using the wizard

Ensure that you complete the following tasks before configuring application monitoring on a virtual machine:

- Install the VMware vSphere Client.
- Install and enable VMware Tools on the virtual machine, where you want to monitor applications with VCS. Install a version that is compatible with the VMware ESX server.
- Install Symantec High Availability console on a Windows system in your data center and register the Symantec High Availability plug-in with the vCenter server.
- Assign Configure Application Monitoring (Admin) privileges to the logged-on user on the virtual machine where you want to configure application monitoring.
- Install Symantec Cluster Server.
- Install the application and the associated components that you want to monitor on the virtual machine.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by the Symantec High Availability installer, wizards, and services. Refer to the *Symantec High Availability Solutions Guide for VMware* for a list of ports and services used.

Before configuring application monitoring

Note the following prerequisites before configuring application monitoring on a virtual machine:

- The Symantec High Availability Configuration wizard discovers the disks that are attached and the storage that is currently mounted. Ensure that the shared storage used by the application is mounted before you launch the wizard.
- For all the WebSphere MQ Queue Managers that you want to configure, the DataPath, LogPath, and InstallationPath directories must be accessible from the node from where you invoke the Symantec High Availability Configuration wizard.
- You must not restore a snapshot on a virtual machine where an application is currently online, if the snapshot was taken when the application was offline on that virtual machine. Doing this may cause an unwanted failover. This also applies in the reverse scenario; you should not restore a snapshot where the application was online on a virtual machine, where the application is currently offline. This may lead to a misconfiguration where the application is online on multiple systems simultaneously.
- While creating a VCS cluster in a virtual environment, you must configure the cluster communication link over a public network in addition to private adapters. The link using the public adapter should be assigned as a low-priority link. This helps in case the private network adapters fail, leading to a condition where the systems are unable to connect to each other, consider that the other system has faulted, and then try to gain access to the disks, thereby leading to an application fault.
- You must not select teamed network adapters for cluster communication. If your configuration contains teamed network adapters, the wizard groups them as "NIC Group #N" where "N" is a number assigned to the teamed network adapters. 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 wizard may fail to discover the specified network adapters.
  - The wizard may fail to discover/validate the specified system name.
- 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 the disks used by the application that you want to monitor are attached to non-shared controllers so that they can be deported from the system and imported to another system.
- If multiple types of SCSI controllers are attached to the virtual machines, then storage dependencies of the application cannot be determined and configured.
- The term 'shared storage' refers to the removable disks attached to the virtual machine. It does not refer to disks attached to the shared controllers of the virtual machine.
- If you want to configure the storage dependencies of the application through the wizard, the VxVM volumes used by the application should not be mounted on more than one mount point path.
- Verify that the following packages are installed:
  - `vrtsvcswebspheremq.msi`
    This package contains the WebSphere MQ agent files.
  - `vrtsvcswiz.msi`
    This package contains the configuration wizard files.

Launching the Symantec High Availability Configuration wizard

You can launch the Symantec High Availability Configuration wizard from:

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

You must launch the Symantec High Availability Configuration wizard from the system where the disk residing on the shared datastore is attached.

To launch the wizard from the VMware vSphere Client

1. Launch the VMware vSphere Client and connect to the VMware vCenter Server that hosts the virtual machine.
2. From the vSphere Client's Inventory view in the left pane, select the virtual machine where you want to configure application monitoring.

3 Skip this step if you have already configured single sign-on during guest installation.

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

The Symantec High Availability console sets up a permanent authentication for the user account on that virtual machine.

4 Depending on your setup, use one of the following options to launch the wizard:

- If you have not configured a cluster, click the **Configure a VCS Cluster** link.
- If you have already configured a cluster, click **Actions > Configure application for high availability** or the **Configure application for high availability** link.
- If you have already configured a cluster and configured an application for monitoring, click **Actions > Configure application for high availability**.

To launch the wizard from a browser window

1 Open a browser window and enter the following URL:

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

<*VMNameorIP*> is the virtual machine name or IP address of the system on which you want to configure application monitoring.

2 In the Authentication dialog box, enter the username and password of the user who has administrative privileges.

3 Depending on your setup, use one of the following options to launch the wizard:

- If you have not configured a cluster, click the **Configure a VCS Cluster** link.
- If you have already configured a cluster, click **Actions > Configure application for high availability** or the **Configure application for high availability** link.
- If you have already configured a cluster and configured an application for monitoring, click **Actions > Configure application for high availability**.

Configuring the WebSphere MQ queue manager for high availability

Configuring an application for high availability 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 the selected virtual machines.

   See "Configuring the VCS cluster" on page 30.

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 configuring 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 41.

Configuring the VCS cluster

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

To configure the VCS cluster

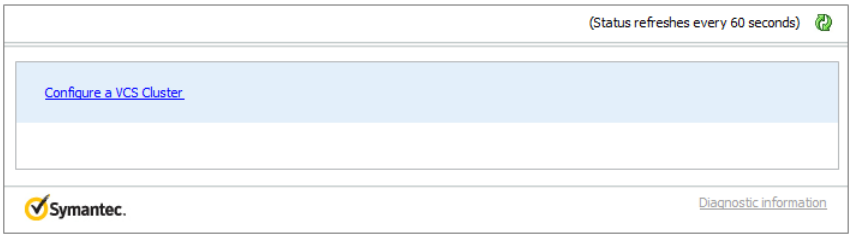
1 Launch the vSphere Client and connect to the vCenter Server that manages the virtual machine. On the Inventory view of the vCenter Server, in the left pane, select the virtual machine where you want to configure application monitoring. Then, in the right pane, select the Symantec High Availability tab.

2 Skip this step if you have already configured the single sign-on during the guest installation.

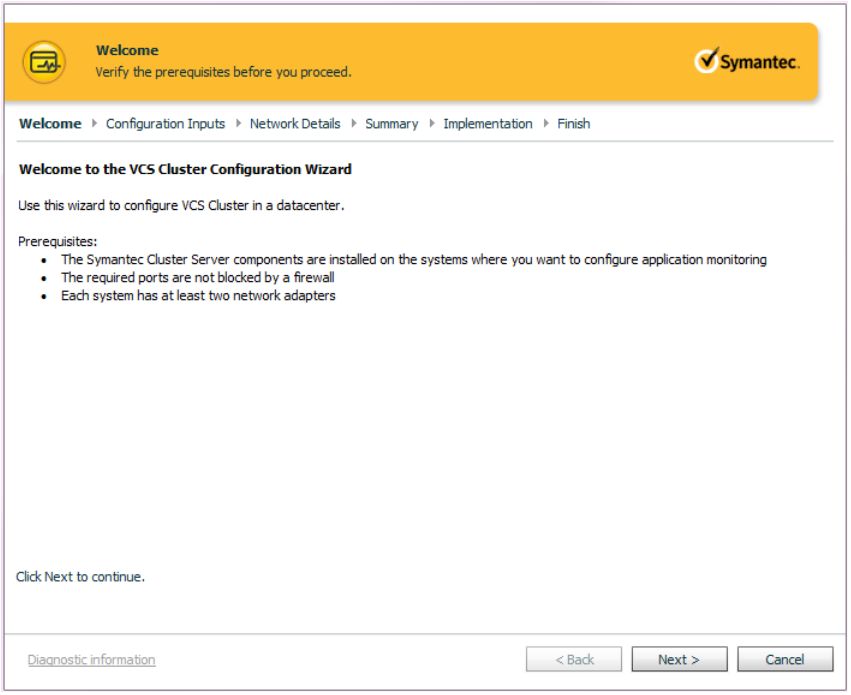
On the Symantec High Availability view, specify the credentials of a user account that has administrative privileges on the system and then click **Configure**.

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.

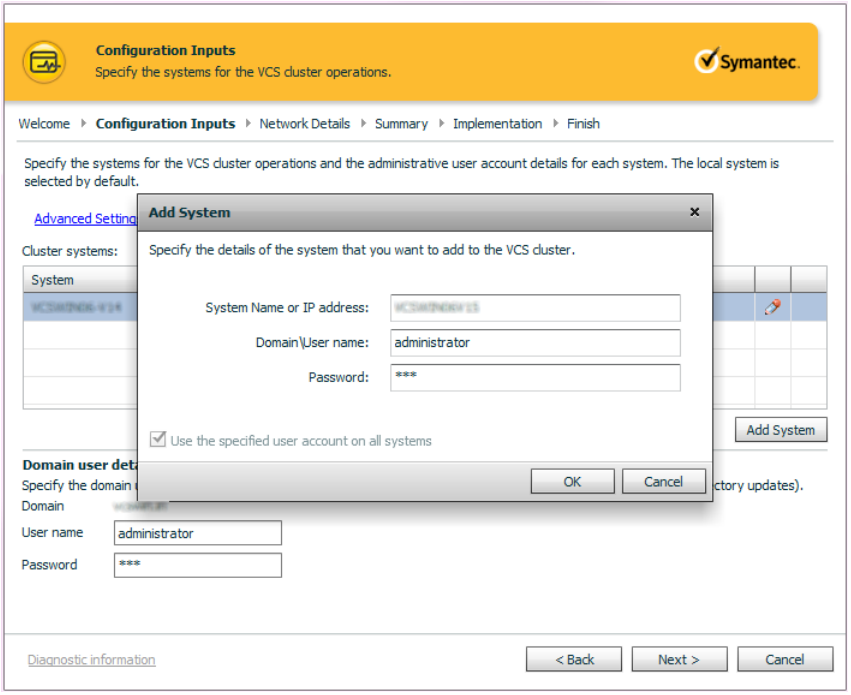
Note: The specified user account must have administrative privileges on the system.

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.

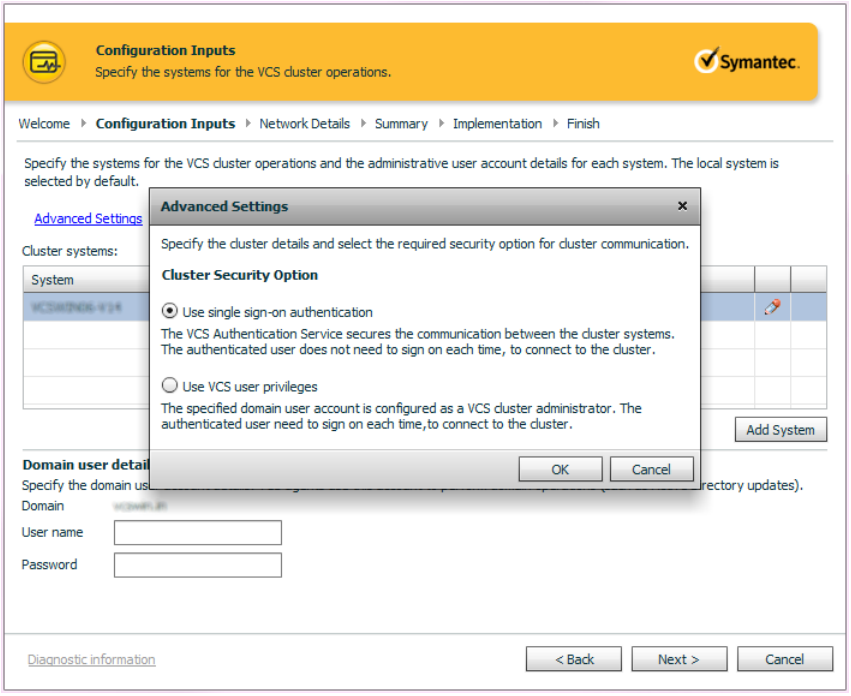
The wizard validates the system details and then adds the system to VCS cluster system list.


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
ctory updates).
Domain
User name
administrator
Password
***
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
Diagnostic information
< Back
Next >
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:

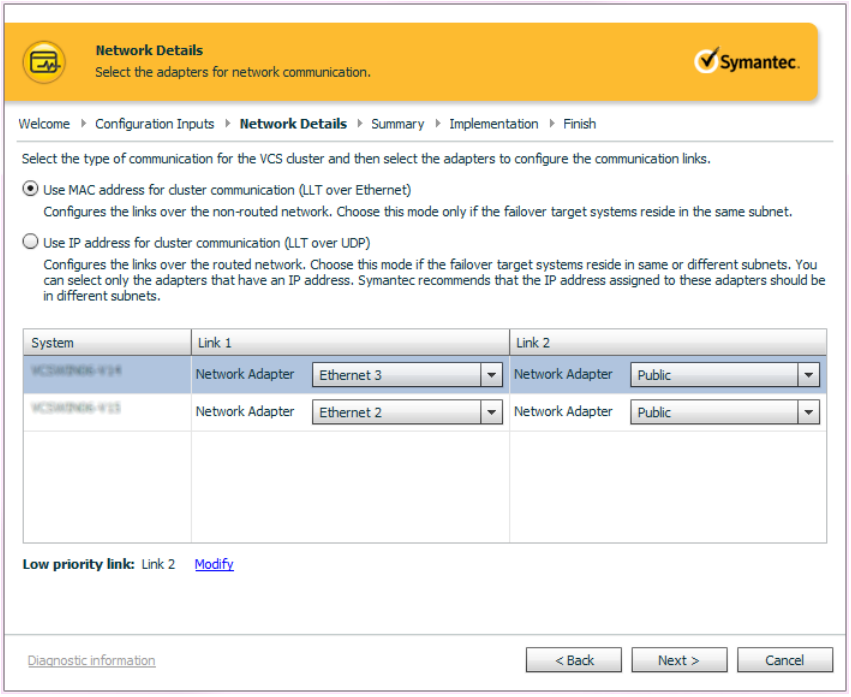
- **Use MAC address for cluster communication (LLT over Ethernet)** : The LLT over Ethernet communication configures the links over the non-routed network. Choose this mode only if the failover target systems reside in the same subnet.
- **Use IP address for cluster communication (LLT over UDP)**: The LLT over UDP communication configures the links over the routed network. You can 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.

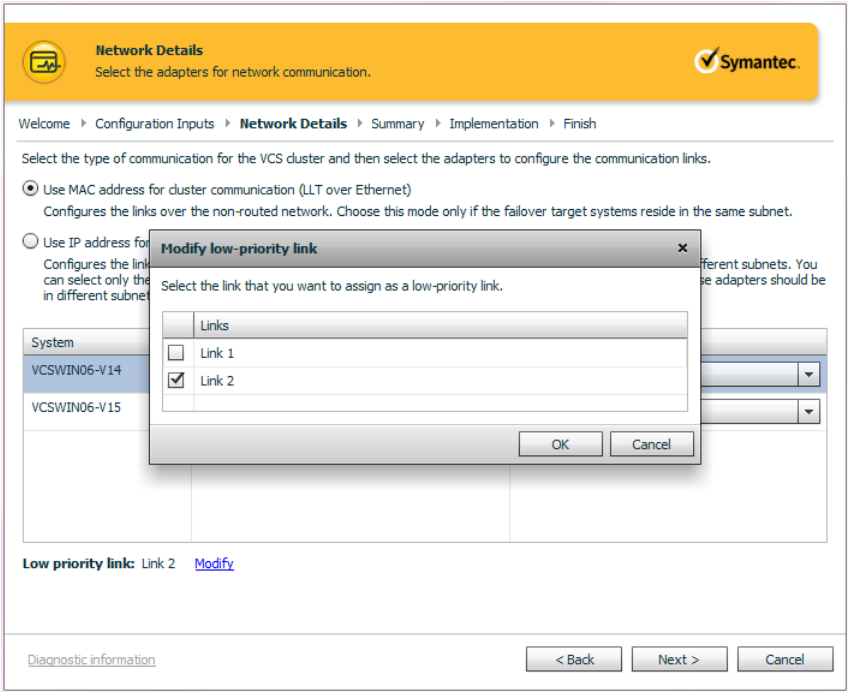
Symantec recommends the following:

- 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.



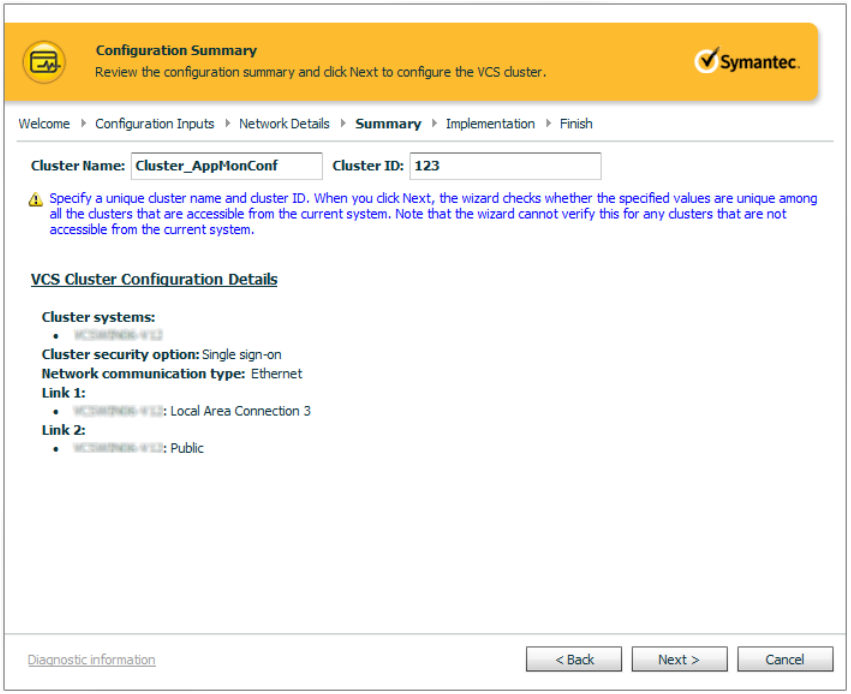
By default, the VCS cluster communication link that uses the public adapter is configured as low-priority link. To change the priority, click **Modify**. In the Modify low-priority link dialog box, select the link and click **OK**.



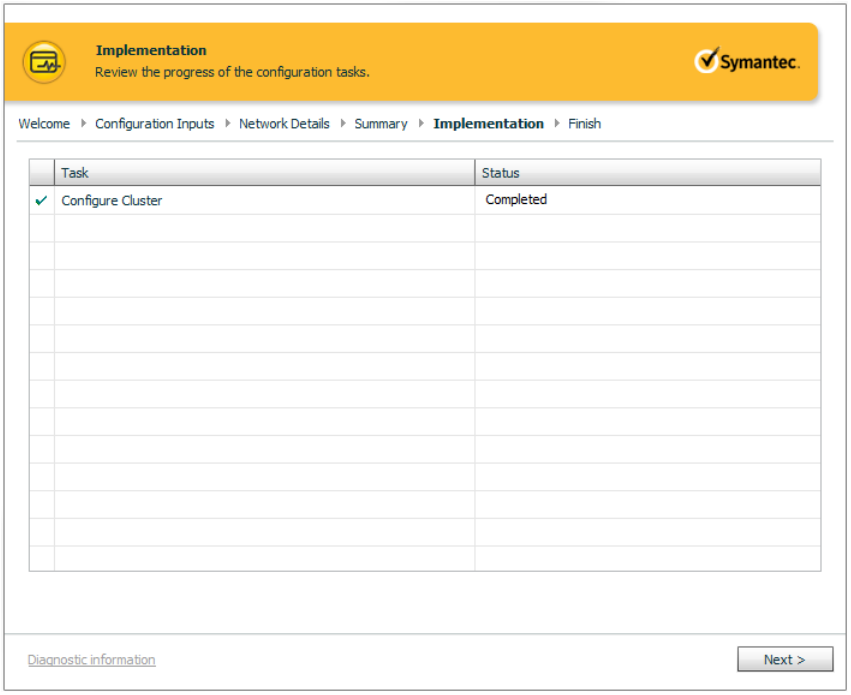
For information about adding or changing the selected network links after the configuration workflow is complete, see the *Symantec Cluster Server Administrator's Guide*.

8 On the Configuration Summary panel, specify a cluster name and a cluster ID of your choice. Click **Validate** to check whether the values are unique in the existing network. On the Confirmation dialog box, click **Proceed**. 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.

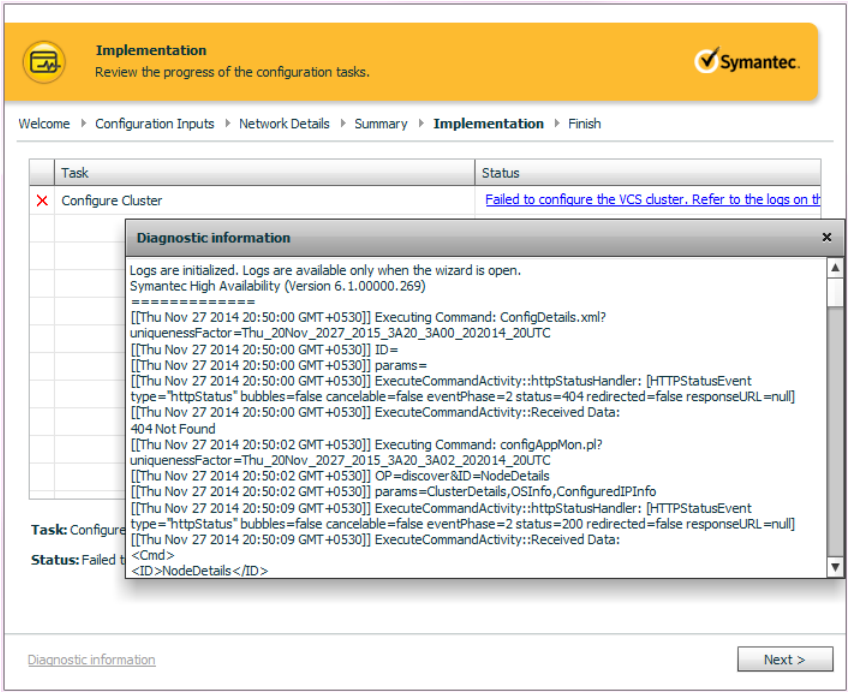
After the validation is successful, review the VCS cluster configuration details and then click **Next** to initiate the configuration.



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**.

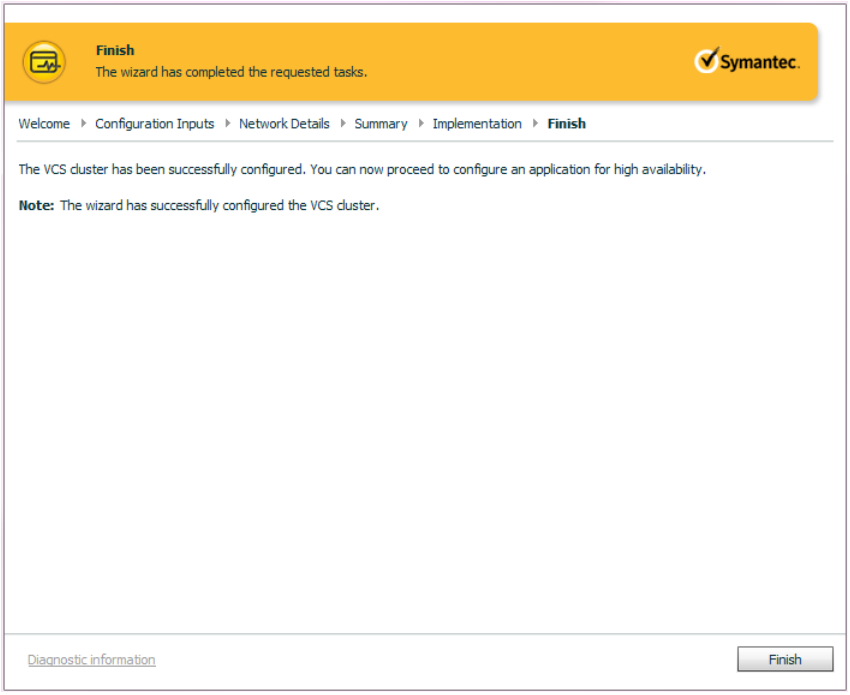


If the configuration tasks fail, click **Diagnostic information** to check the details of the failure.


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.



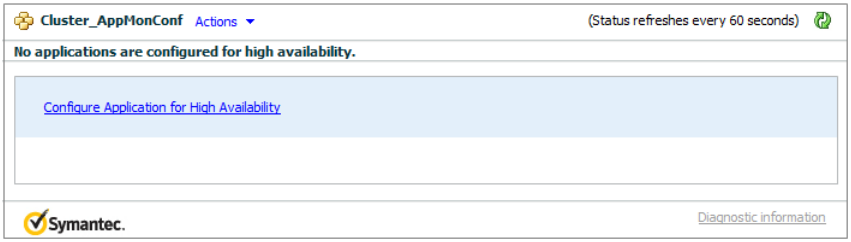
The Symantec High Availability view now displays the link to configure an application for high availability.

Configuring the application

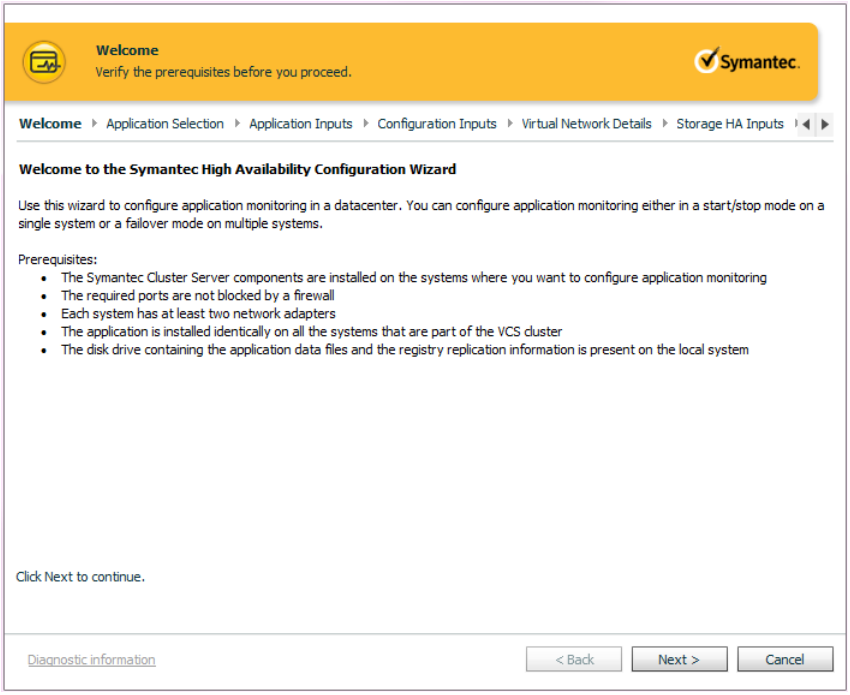
Perform the following steps to configure the WebSphere MQ queue manager for high availability on a virtual machine.

To configure the application

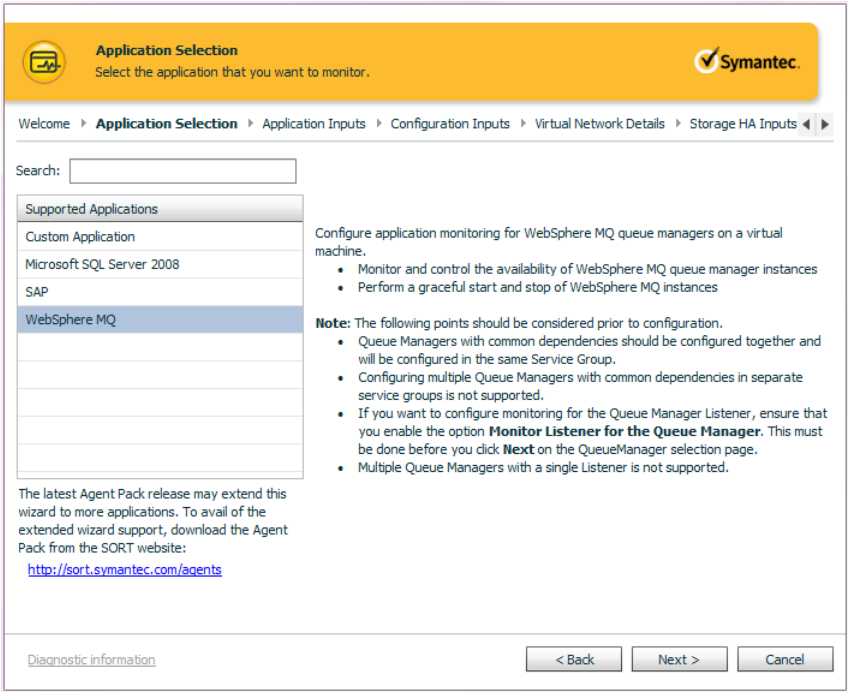
1. Launch the vSphere Client and connect to the vCenter Server that manages the virtual machine. On the Inventory view of the vCenter Server, in the left pane, select the virtual machine where you want to configure application monitoring. Then, in the right pane, select the Symantec High Availability 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 **WebSphere MQ** 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

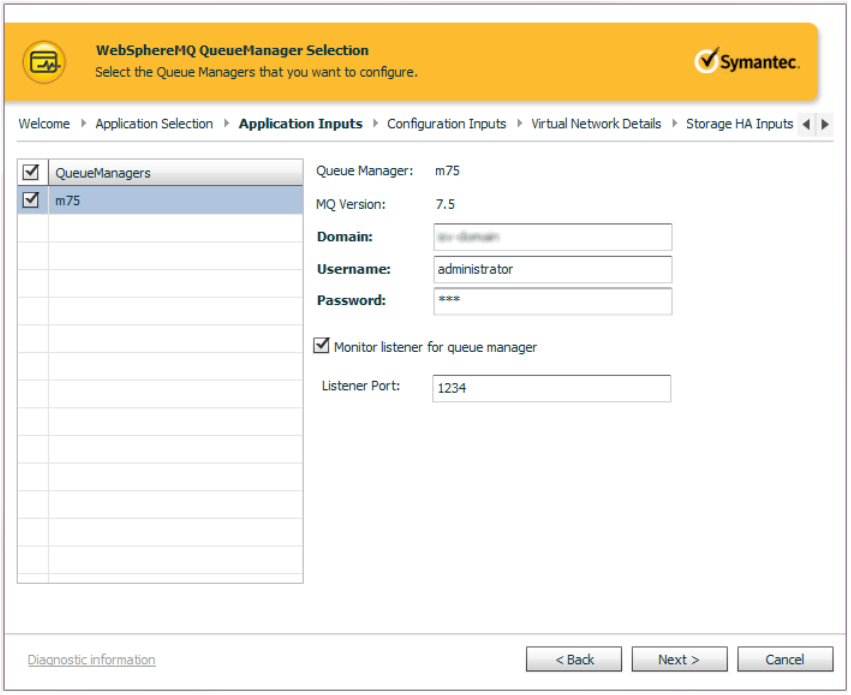
5 On the WebSphereMQ QueueManager Selection panel, from the QueueManagers list, select the queue manager instances that you want to monitor.

Note: The wizard does not display queue manager instances that are already configured.

Specify the domain name, user name, and password of the user for the queue manager.

If you want to monitor the related queue manager listener, check the **Monitor listener for queue manager** check box and enter the listener port number in the **Listener Port** field. A separate resource for the listener is created using the generic application agent.

Note: The Symantec High Availability Configuration wizard supports only one listener associated with each queue manager.

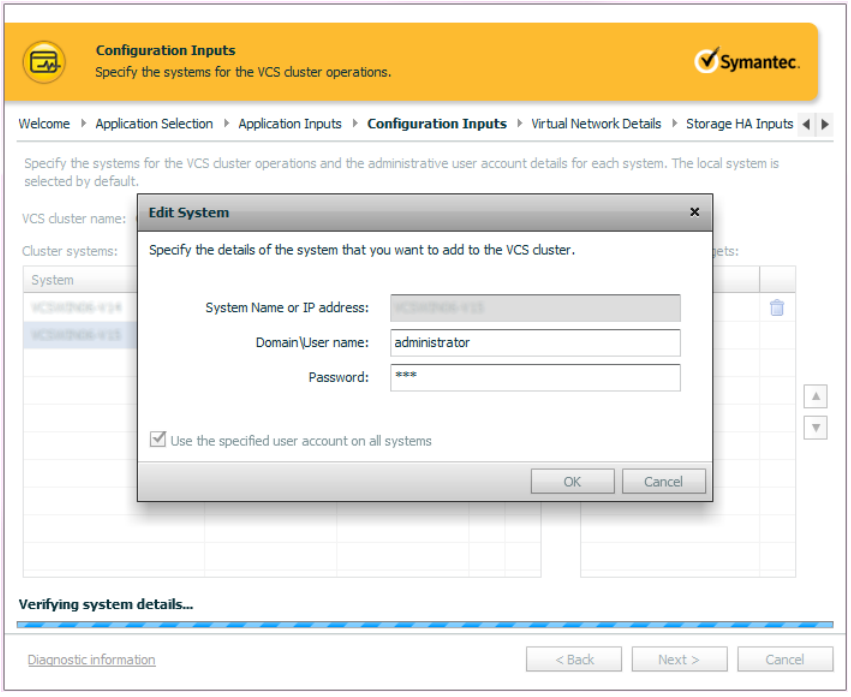


Click **Next**.

6 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.



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

Note: This panel appears only if you have specified a listener port on the WebSphereMQ QueueManager Selection panel.

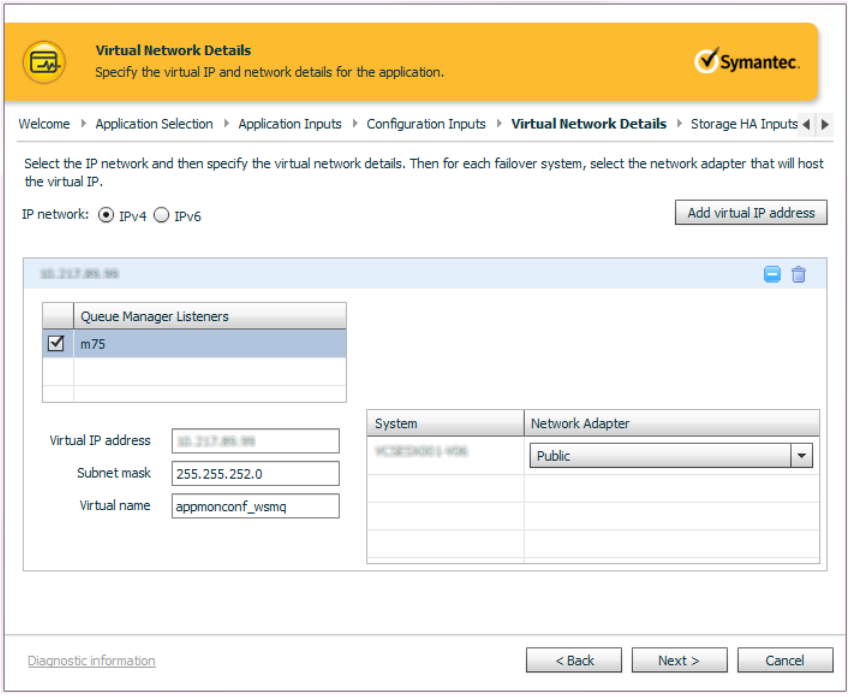
To specify the virtual IP and network details, select the IP protocol and then specify the following details for each failover system:

Note: You must select the same IP protocol as that 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	Select the network adapter that will host the virtual IP.

If you want to add another virtual IP address, click **Add virtual IP address**. A virtual IP input panel appears, in which you can enter the details as described earlier in this step.

Note: You can only provide either a set of IPv4 addresses or a set of IPv6 addresses, not both.

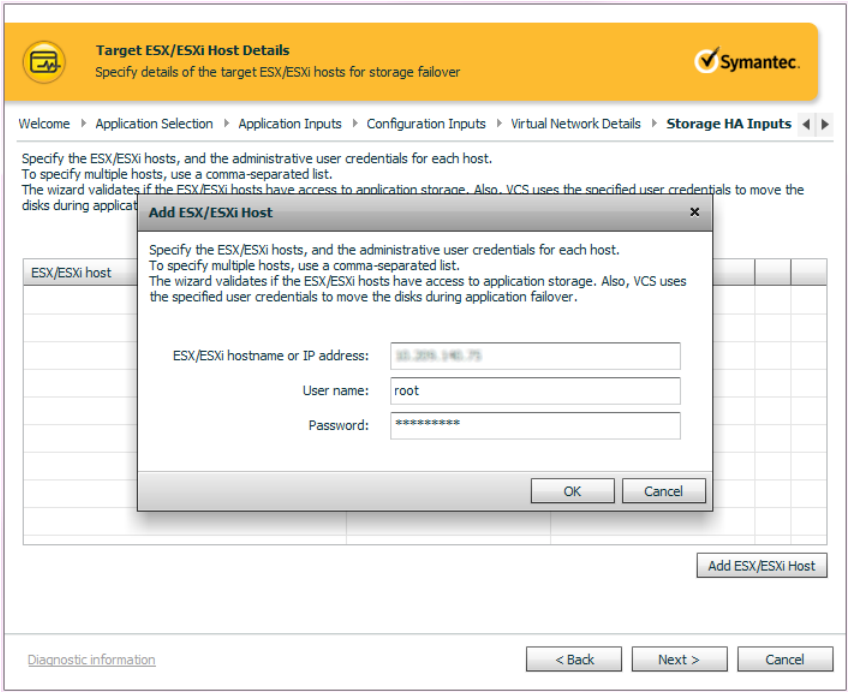

Virtual Network Details
Specify the virtual IP and network details for the application.
Symantec.
Welcome
Application Selection
Application Inputs
Configuration Inputs
Virtual Network Details
Storage HA Inputs
Select the IP network and then specify the virtual network details. Then for each failover system, select the network adapter that will host the virtual IP.
IP network:
IPv4
IPv6
Add virtual IP address
Queue Manager Listeners
m75
Virtual IP address
Subnet mask
255.255.252.0
Virtual name
appmonconf_wsmq
System
Network Adapter
Public
Diagnostic information
< Back
Next >
Cancel

8 On the Target ESX/ESXi Host Details panel, specify the hosts and the administrative user account details for each host, and then click **Next**.

Note: This panel appears only if you have selected multiple application failover targets on the Configuration Inputs panel.

To specify the 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.



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

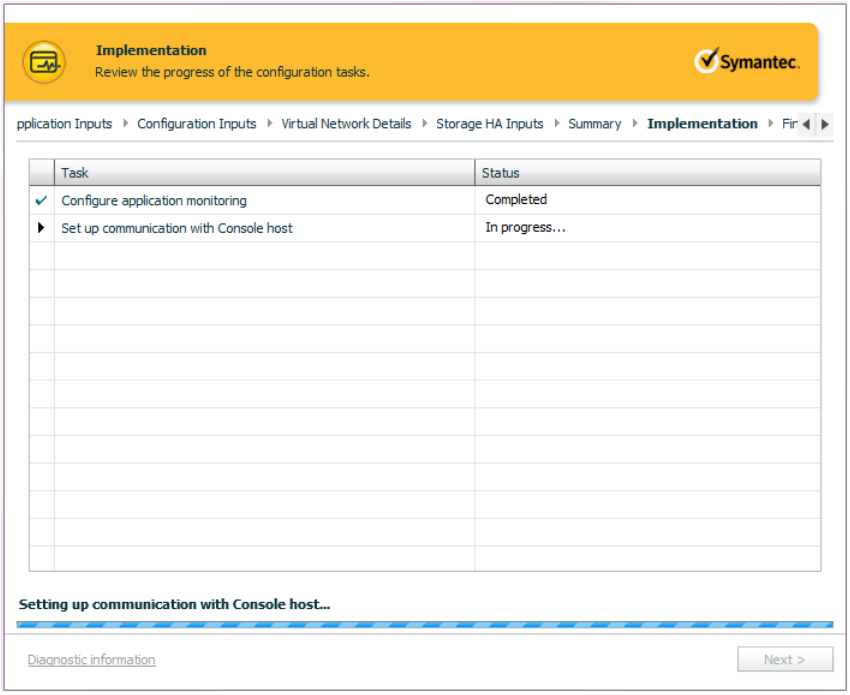
9 On the Configuration Summary panel, review the application configuration details.

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.

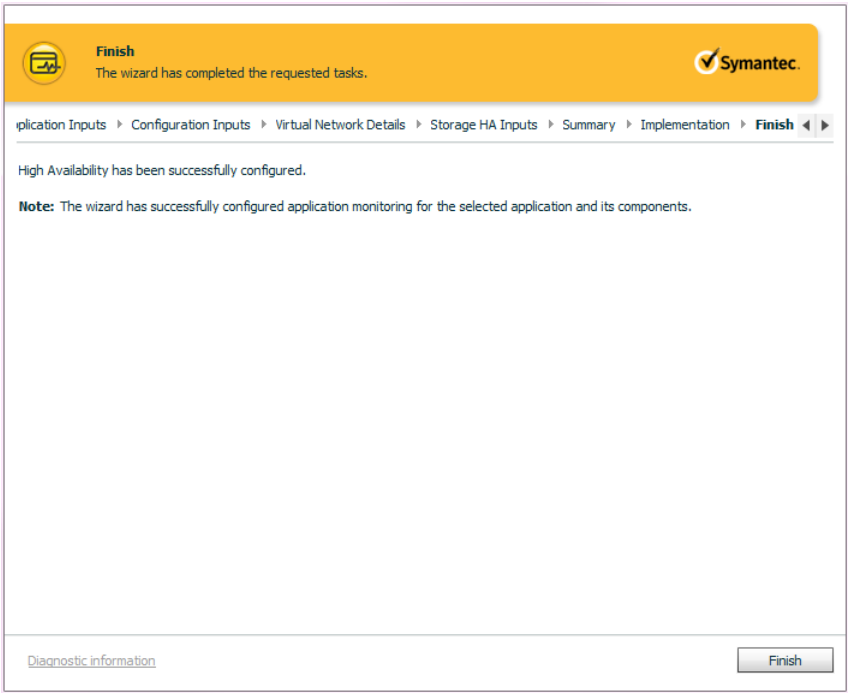
10 On the Implementation panel, the wizard performs the application configuration tasks.

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.

11 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.

Understanding service group configurations

One or more WebSphere MQ Queue Manager instances can be discovered on a virtual machine. These WebSphere MQ Queue Manager instances may or may not share the same mount points, disks, disk groups, volume, or virtual IP address. The WebSphere MQ Queue Manager listeners that do not share any of these forms a separate service group.

Resource dependency

Following are the resource dependencies:

- When the listeners are monitored using the Independent of Queue Manager option, the listener resources associated with a WebSphere MQ Queue Manager instance depends on the WebSphere MQ resource.
- Listener resources also depend on the configured IP resources.
- The WebSphere MQ resource depends on mount point resources which are discovered for that particular WebSphere MQ instance. The wizard checks if the DataPath and LogPath for the Queue Manager are on the shared storage.
- Mount point resources depend on VxVM volume. VxVM volume depends on DiskGroup resources.
- DiskGroup resources depend on the shared disks which are configured as VMware Disks resources.

Service group dependency

The Symantec High Availability Configuration wizard does not create service group dependency for WebSphere MQ.

Infrastructure service groups

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

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

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

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

The following are the VCSInfraSG notes:

- Before you configure the application for monitoring, ensure that SSO is configured between the Symantec High Availability Console and the guest. If SSO is not configured, VCSInfraSG fails to come online.

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

Understanding configuration scenarios

You can configure WebSphere MQ Queue Manager instances in different ways using the Symantec High Availability Configuration wizard.

- Configuring a single instance/multiple instances in VCS
- Configuring multiple WebSphere MQ Queue Manager instances in VCS using multiple runs of the wizard
- Configuring multiple applications

Configuring a single instance/multiple instances in VCS

Use the Symantec High Availability Configuration wizard to configure one or more WebSphere MQ Queue Manager instances in a single run. In the Application Inputs panel, select the WebSphere MQ Queue Manager instances from the Queue Manager list. For each instance, you must specify the following mandatory parameters:

- Domain
- User
- Password
- Listener related to the specific Queue Manager

Configuring multiple WebSphere MQ Queue Manager instances in VCS using multiple runs of the wizard

If you are configuring the first WebSphere MQ Queue Manager instance on a machine where more than one Queue Manager instance is present, configure it by following the steps in the Configuring a single instance/multiple instances in VCS section.

The Symantec High Availability Configuration wizard will not allow you to configure the next WebSphere MQ Queue Manager instance if any of the mandatory dependent resources such as mount point, disk group, and disk are already configured in VCS.

- If existing resources are part of the WebSphere MQ service group, unconfigure the existing service group and then reconfigure the new instance along with the old instances/listeners which were part of the pre-existing service group.

  Note: All the queue managers that share the mount point for the Queue Manager DataPath or LogPath must be configured in a single run of the wizard.

- If existing resources are part of an application service group other than WebSphere MQ, the wizard does not support configuring multiple applications. You can configure these applications through CLI or Veritas Operations Manager.

Configuring multiple applications

If you run the Symantec High Availability Configuration wizard multiple times, you can configure multiple applications of different types.

If you are configuring the first application on a machine where more than one application is running, you can configure it by following the steps in the Configuring a single instance/multiple instances in VCS section.

The Symantec High Availability Configuration wizard will not allow you to configure the next application if any of the mandatory dependent resources such as mount point, disk group, and disk are already configured in VCS.

Symantec High Availability Configuration wizard limitations

Following are the Symantec High Availability Configuration wizard limitations:

- The wizard supports WebSphere MQ 7.0 or later.
- The wizard does not monitor the Command Server Process for WebSphere MQ queue manager. To manually configure the Command Server Process for monitoring, use the command line interface.
- The wizard supports discovery of only VxVM type of storage.
- The wizard does not discover the disks used by the application if the controllers attached to the virtual machine are of different type. To correctly discover and identify the association of mount points to the virtual disks, all the controllers attached to the virtual machine must be of same type.
- The wizard does not discover disks that are attached to the virtual machine in shared mode.

Troubleshooting

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.

Workaround: 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 following error after you click **Next** on the Application Selection panel:

```
hadiscover is not recognized as an internal or external command
```

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

Workaround: Close 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 component 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.

Workaround: If you want to stop the VCS cluster (and not the applications running on cluster nodes), instead of the `hastop -all` command, use the `hastop -all -force` command. This command stops the cluster without affecting the virtual disks attached to the VCS cluster nodes.

Log files

The log files are stored in the virtual machine on which you configured application monitoring.

The healthview_A.log file contains the steps performed by the back-end to configure the application. To check the file, you must access: `C:\Program Files\Veritas\cluster server\log\healthview_A.log`

The WebSphereMQ_A.log file contains the actions performed by the agent. To check the file, you must access: `C:\Program Files\Veritas\cluster server\log\WebSphereMQ_A.log`

The engine_A.log file contains the actions performed by the VCS cluster. To check the file, you must access: `C:\Program Files\Veritas\cluster server\log\engine_A.log`

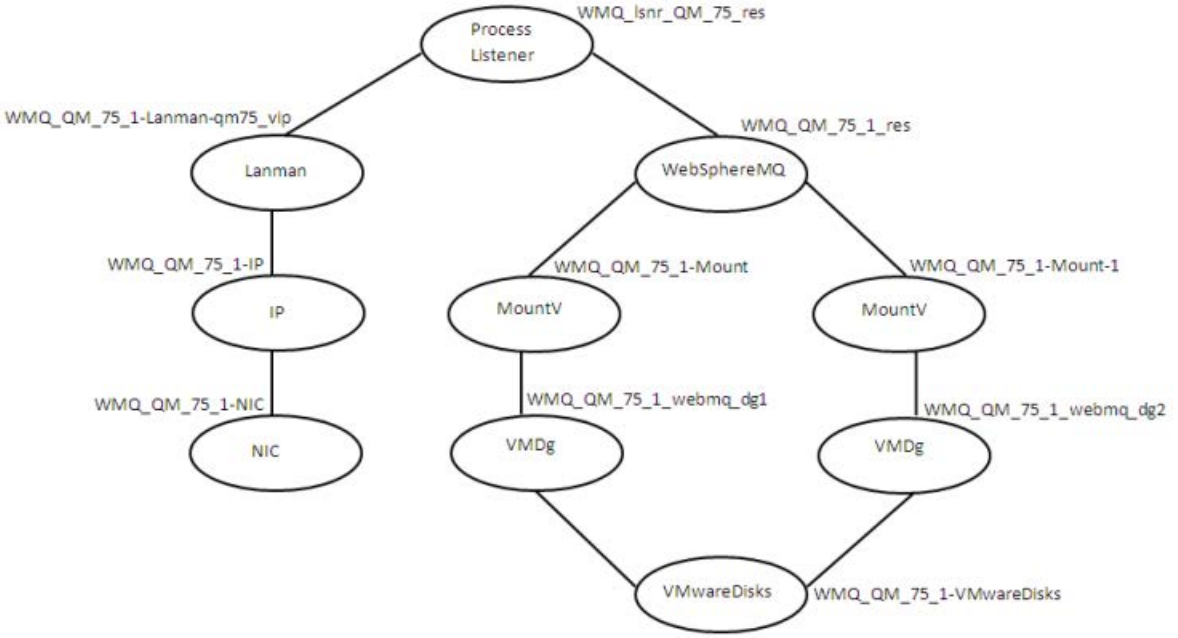
Sample configurations

The sample configurations includes description for typical service groups that are configured using the Symantec High Availability Configuration wizard.

Sample VCS configuration file for single WebSphere MQ Queue Manager instance (VxVM)

Figure 4-2 shows a typical service group configured to monitor the state of a WebSphere MQ Queue Manager instance. In this example, the WebSphere MQ Queue Manager instance uses VxVM volume as storage.

Figure 4-2 Dependency graph for single WebSphere MQ Queue Manager instance (VxVM)



Review the sample configuration with a resource of type WebSphere MQ Queue Manager that is configured as follows in main.cf file.

```
include "types.cf"

cluster clus_vm4_vm5 (
 SecureClus = 1
 )

system SysA (
 )

system SysB (
 )

group VCSInfraSG (
 SystemList = { SysA = 0, SysB = 1 }
 UserAssoc = { Type = "vcs internal",
   Name = "VCS Infrastructure service group" }
```

```
 Parallel = 1
 AutoStartList = { SysA, SysB }
 OnlineRetryLimit = 5
 )

 Process VCSNotifySinkRes (
  StartProgram = "C:\\Program Files\\Veritas\\Cluster Server\\bin\\
  notify_sink.exe"
  StartupDirectory = "C:\\Program Files\\Veritas\\Cluster Server\\bin"
  )



 // resource dependency tree
 //
 // group VCSInfraSG
 // {
 // Process VCSNotifySinkRes
 // }


group WMQ_QM_75_1 (
 SystemList = { SysA = 0 }
 UserAssoc = { Type = WebSphereMQ, Name = WMQ_QM_75_1 }
 AutoStartList = { SysA }
 )

 IP WMQ_QM_75_1-IP (
  Address = "10.20.50.6"
  SubNetMask = "255.255.252.0"
  MACAddress @SysA = "00:50:56:8A:5D:CD"
  )

 Lanman WMQ_QM_75_1-Lanman-qm75_vip (
  VirtualName = qm75_vip
  IPResName = WMQ_QM_75_1-IP
  )

 MountV WMQ_QM_75_1-Mount (
  MountPath = "w:"
  VolumeName = webmq_vol1
  VMDGResName = WMQ_QM_75_1_webmq_dg1_VMNSDg
  )
```

```
MountV WMQ_QM_75_1-Mount-1 (
 MountPath = "x:"
 VolumeName = webmq_vol2
 VMDGResName = WMQ_QM_75_1_webmq_dg2_VMNSDg
 )

NIC WMQ_QM_75_1-NIC (
 MACAddress @SysA = "00:50:56:8A:5D:CD"
 )

Process WMQ_lsnr_QM_75_res (
 StartProgram = "C:\\Program Files (x86)\\WebMQ_7.5\\
 WebSphere MQ_3\\bin\\runmqlsr.exe
 -r -m QM_75 -t TCP -p 5555 -i 10.20.50.6"
 StopProgram = "C:\\Program Files (x86)\\WebMQ_7.5\\
 WebSphere MQ_3\\bin\\endmqlsr.exe
 -m QM_75"
 UserName = webmqadm
 )

VMNSDg WMQ_QM_75_1_webmq_dg1_VMNSDg (
 DiskGroupName = webmq_dg1
 DGGuid = 0cb34d1c-89e4-40a5-9450-93fe65c7c714
 )

VMNSDg WMQ_QM_75_1_webmq_dg2_VMNSDg (
 DiskGroupName = webmq_dg2
 DGGuid = e36f74e4-028f-4f84-a60c-3b85b672c8fd
 )

VMwareDisks WMQ_QM_75_1-VMwareDisks (
 ESXDetails = { "10.209.64.79" = "root=aocMpmPoeGbgCgd" }
 DiskPaths = {
   "6000C293-3fc9-68ac-691e-3f5129477bb9:[WebSphereMQ_LUN1]
    PUNB200M2LABS14vm4/
    PUNB200M2LABS14vm4_1.vmdk" = "0:1",
   "6000C299-104d-b606-0047-20975a11990b:[WebSphereMQ_LUN2]
    PUNB200M2LABS14vm4/
    PUNB200M2LABS14vm4_2.vmdk" = "0:2",
   "6000C29a-4674-fd09-c9cf-403dfb4b690e:[ds001] PUNB200M2LABS14vm4/
    PUNB200M2LABS14vm4_3.vmdk" = "0:3" }
 IsVMHAEnabled = 0
```

```
 )

WebSphereMQ WMQ_QM_75_1_res (
 QueueManager = QM_75
 Domain = isv-domain
 User = webmqadm
 Password = encrypted_password
 MQVer = "7.5"
 Home = "C:\\Program Files (x86)\\WebMQ_7.5\\WebSphere MQ_3"
 )

WMQ_QM_75_1_res requires WMQ_QM_75_1-Mount
WMQ_QM_75_1_res requires WMQ_QM_75_1-Mount-1
WMQ_lsnr_QM_75_res requires WMQ_QM_75_1_res
WMQ_lsnr_QM_75_res requires WMQ_QM_75_1-Lanman-qm75_vip
WMQ_QM_75_1-IP requires WMQ_QM_75_1-NIC
WMQ_QM_75_1-Lanman-qm75_vip requires WMQ_QM_75_1-IP
WMQ_QM_75_1-Mount requires WMQ_QM_75_1_webmq_dg1_VMNSDg
WMQ_QM_75_1-Mount-1 requires WMQ_QM_75_1_webmq_dg2_VMNSDg
WMQ_QM_75_1_webmq_dg1_VMNSDg requires WMQ_QM_75_1-VMwareDisks
WMQ_QM_75_1_webmq_dg2_VMNSDg requires WMQ_QM_75_1-VMwareDisks


// resource dependency tree
//
// group WMQ_QM_75_1
// {
// Process WMQ_lsnr_QM_75_res
//     {
//     WebSphereMQ WMQ_QM_75_1_res
//         {
//         MountV WMQ_QM_75_1-Mount
//             {
//             VMNSDg WMQ_QM_75_1_webmq_dg1_VMNSDg
//                 {
//                 VMwareDisks WMQ_QM_75_1-VMwareDisks
//                 }
//             }
//         MountV WMQ_QM_75_1-Mount-1
//             {
//             VMNSDg WMQ_QM_75_1_webmq_dg2_VMNSDg
//                 {
//                 VMwareDisks WMQ_QM_75_1-VMwareDisks
```

```
//                  }
//              }
//          }
//      Lanman WMQ_QM_75_1-Lanman-qm75_vip
//          {
//          IP WMQ_QM_75_1-IP
//              {
//              NIC WMQ_QM_75_1-NIC
//              }
//          }
//      }
// }
```

Chapter 5

Configuring the service groups for WebSphere MQ Queue Manager

This chapter includes the following topics:

- About configuring a service group for the agent for WebSphere MQ
- Configuring a WebSphere MQ resource
- Configuring a WebSphere MQ Listener

About configuring a service group for the agent for WebSphere MQ

To provide high availability for WebSphere MQ components, you must configure WebSphere MQ in a clustered environment and use the Symantec High Availability agent for WebSphere MQ to manage the Queue Manager components.

Configuring a WebSphere MQ resource

In a clustered environment, you can configure a WebSphere MQ resource using two methods:

Active-Passive configuration

The Active-Passive configuration is an easier method of configuration. This method limits the configuration to one service group running a WebSphere MQ Queue Manager on a particular node at one time.

Active-Active configuration

The Active-Active configuration allows multiple service groups running WebSphere MQ Queue Managers on a particular node simultaneously. This configuration incurs additional complexity in configuration and maintenance.

Active-Passive configuration

In an active-passive configuration, all WebSphere MQ Queue Managers running on a single node are configured under a single service group. In case of a failure of any queue manager component, the whole service group fails over to the other node in a cluster.

Perform the following steps on the node that hosts the service group:

To configure a WebSphere MQ Queue Manager using active-passive configuration

1. Ensure that a file system is located on a shared disk.

   This file system must be in the same service group in which the WebSphere MQ Queue Manager is to be created.

   Mount location should be same on all clustered nodes.

2. Use the WebSphere MQ tools to create the WebSphere MQ Queue Manager.

   Refer to the WebSphere MQ documentation for details.

3. Define this WebSphere MQ Queue Manager as a resource in the service group.

   See "Sample configuration for WebSphere MQ" on page 72.

You can now create additional Queue Managers on the same node on which the service group is currently online.

Ensure that you always define the additional Queue Manager as a cluster server resource in the same service group where other Queue Managers are defined.

Active-Active configuration

In an active-active configuration, you can configure each WebSphere MQ Queue Manager in a separate service group, and each Queue Manager can fail over independent of each other. This configuration is complex to implement and maintain. However, this configuration provides the flexibility that some applications may require. This method also supports many-to-one and many-to-many cluster configurations.

Perform the following steps on the node that hosts the service group to which the WebSphere MQ Queue Manager belongs.

To configure a WebSphere MQ Queue Manager using active-active configuration

1. Use the WebSphere MQ tools to create the WebSphere MQ Queue Managers that you require. Refer to the WebSphere MQ documentation for details.
2. Create a file system for each WebSphere MQ Queue Manager on the shared disk. Add each file system to a separate service group.

   See "Sample configuration for WebSphere MQ" on page 72.
3. Move the log directory (for example, C:\Program Files\IBM\WebSphere MQ\log*QueueManagerName*) to a directory on each file system on the shared disk. Ensure that you copy the sub-directories also.
   - Take a backup of the contents of the log directory for the queue manager at some other location.
   - Make sure that the log directory is empty.
   - Create mount points for shared storage.
   - Restore the content of the log directory from the backup location, on to a directory on shared storage.
4. Move the qmgr directory (for example, C:\Program Files\IBM\WebSphere MQ\Qmgrs*QueueManagerName*) to a directory on each file system on the shared disk. Ensure that you copy the sub-directories also.
   - Take a backup of the contents of the qmgr directory for the Queue Manager at some other location.
   - Make sure that the qmgr directory is empty.
   - Create mount points for shared storage.
   - Restore the content of the qmgr directory from the backup location, on to a directory on shared storage.
5. Define the Queue Managers as resources in separate service groups.

   See "Sample configuration for WebSphere MQ" on page 72.

Note: WebSphere MQ can run on many nodes in the cluster. These nodes are defined in the SystemList attribute. Replicate the registry information for newly created queue manager from the node in which the queue manager is created to all other clustered nodes. The replicated registry key is: HKLM\Software\IBM\MQseries\CurrentVersion\Configuration\QueueManager*QueueManager NAME*\

Configuring a WebSphere MQ Listener

A WebSphere MQ Queue Manager uses a Listener to listen for requests on a specific IP address. Symantec recommends that you configure a Listener resource in the cluster using a bundled process agent. A example listener resource configuration is shown as follows.

You can replace these values with the virtual IP address and Queue Manager name defined within the cluster.

```
Process mq_listener (
Critical = 1
StartProgram = "\"C:\\Program Files\\IBM\\WebSphere
MQ\\bin\\runmqlsr.exe\" -r -m QM_75 -t TCP"
StopProgram = "\"C:\\Program Files\\IBM\\WebSphere
MQ\\bin\\endmqlsr.exe\" -m QM_75"
UserName = administrator
Password = encrypted_password
Domain = isv-domain
)
```

For details about the WebSphere MQ listener, refer to the IBM WebSphere MQ documentation.

Chapter 6

Troubleshooting the agent for WebSphere MQ

This chapter includes the following topics:

- Using correct software and operating system versions
- Meeting prerequisites
- Configuring WebSphere MQ Queue Manager resources
- Starting the WebSphere MQ Queue Manager outside a cluster
- Monitoring WebSphere MQ Queue Manager processes
- Reviewing error log files

Using correct software and operating system versions

Ensure that no issues arise due to incorrect software and operating system versions. For the correct versions of operating system and software to be installed on the resource systems, refer to SORT site: https://sort.symantec.com/agents

Meeting prerequisites

Before installing the Symantec High Availability agent for WebSphere MQ, double check that you meet the prerequisite requirements. For a list of prerequisites:

See "Before you install the agent for WebSphere MQ" on page 13.

Configuring WebSphere MQ Queue Manager resources

Before using an WebSphere MQ Queue Manager resource, ensure that you configure the agent attributes correctly. For more information,

See "Agent attributes for WebSphere MQ" on page 18.

Starting the WebSphere MQ Queue Manager outside a cluster

If you face problems while working with a resource, you must disable the resource within the cluster framework. A disabled resource is not under the control of the cluster framework, and so you can test the WebSphere MQ Queue Manager independent of the cluster framework. Refer to the cluster documentation for information about disabling a resource. You can then restart the WebSphere MQ Queue Manager outside the cluster framework.

Note: Use the same parameters that the resource attributes define within the cluster framework while restarting the resource outside the framework.

A sample procedure to start a WebSphere MQ Queue Manager outside the cluster framework, is illustrated as follows:

To restart the WebSphere MQ Queue Manager outside the framework

1. Log in as an MQUser.
2. Start the WebSphere MQ Queue Manager.

   ```
   strmqm Queue Manager Name
   ```

   If the WebSphere MQ Queue Manager works properly outside the cluster framework, you can then attempt to implement the Queue Manager within the cluster framework.

Monitoring WebSphere MQ Queue Manager processes

The agent for WebSphere MQ monitors the following processes:

- amqzxma0.exe
- amqzmuc0.exe
- amqzmur0.exe
- amqrrmfa.exe

- amqzdmaa.exe
- runmqchi.exe
- amqpcsea.exe

Reviewing error log files

If you face problems while using the WebSphere MQ Queue Manager or the agent for WebSphere MQ, use the error log files described in this section to investigate the problems. Contact Symantec help for more information.

Reviewing VCS log files

In case of problems while using the agent for WebSphere MQ, you can also access the VCS engine log file for more information about a particular resource.

The VCS engine log file is c:\program files\veritas\cluster server\log\engine_A.txt.

Using WebSphere MQ log files

If the WebSphere MQ Queue Manager has problems, you can access the server log files to further diagnose the problem. The WebSphere MQ Queue Manager log files are located in the Queue Manager Home\qmgrs*Queue Manager Name*\errors directory.

Using trace level logging

The ResLogLevel attribute controls the level of logging that is written in a cluster log file for each WebSphere MQ Queue Manager resource. You can set this attribute to TRACE, which enables very detailed and verbose logging. If you set ResLogLevel to TRACE, a very high volume of messages is produced. Symantec recommends that you must localize the ResLogLevel attribute for particular resource.

To localize ResLogLevel attribute for a resource

1. Identify the resource for which you want to enable detailed logging.
2. Localize the ResLogLevel attribute for the identified resource:

   ```
   # hares -local Resource_Name ResLogLevel
   ```

3. Set the ResLogLevel attribute to TRACE for the identified resource:

   ```
   # hares -modify Resource_Name ResLogLevel TRACE -sys SysA
   ```

4 Note the time before you begin to operate the identified resource.

5 Test the identified resource. The function reproduces the problem that you are attempting to diagnose.

6 Note the time when the problem is reproduced.

7 Set the ResLogLevel attribute back to INFO for the identified resource:

```
# hares -modify Resource_Name ResLogLevel INFO -sys SysA
```

8 Review the contents of the VCS engine output log file. Use the time noted in Step 4 and Step 6 to diagnose the problem.

Contact Symantec support for more help.

Appendix A

Sample Configurations

This appendix includes the following topics:

- About the sample configuration for the agent for WebSphere MQ
- Sample agent type definition
- Sample configuration for WebSphere MQ
- Sample service group configuration for WebSphere MQ

About the sample configuration for the agent for WebSphere MQ

The sample configuration depicts the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the agent for WebSphere MQ. For more information about these resource types, see the *Symantec Cluster Server Bundled Agents Reference Guide*.

Sample agent type definition

A sample agent type definition is shown as follows:

```
type WebSphereMQ (
 static str ArgList[] = { ResLogLevel, State, IState,
QueueManager, CommandServer, Domain, User, Password, MQVer, Home,
SecondLevelMonitor, MonitorProgram }
 str ResLogLevel = INFO
 str QueueManager
 boolean CommandServer = 0
 str Domain
 str User
```

```
 str Password
 str MQVer = "6.0"
 str Home
 int SecondLevelMonitor
 str MonitorProgram
)
```

Sample configuration for WebSphere MQ

A sample main.cf file is shown as follows:

```
include "types.cf"
include "WebSphereMQTypes.cf"
cluster SFWHA50 (
UserNames = { admin = gpqIpkPmqLqqOyqKpn, a = jQQk }
Administrators = { admin, a }
)
system systemA (
)
system systemB (
)
group mqgrp (
SystemList = { systemA = 0, systemB = 1 }
)
MountV mq_qmgr_mnt (
MountPath = "C:\\Program Files\\IBM\\WebSphere
MQ\\Qmgrs\\QM_57"
VolumeName = mq_qmgr_vol
VMDGResName = mq_qmgr_dg
ForceUnmount = ALL
)
MountV mq_log_mnt (
MountPath = "C:\\Program Files\\IBM\\WebSphere
MQ\\log\\QM_57"
VolumeName = mq_log_vol
VMDGResName = mq_log_dg
ForceUnmount = ALL
)
Process mq_listener (
StartProgram = "\"C:\\Program Files\\IBM\\WebSphere
MQ\\bin\\runmqlsr.exe\" -r -m QM_57 -t TCP"
StopProgram = "\"C:\\Program Files\\IBM\\WebSphere
MQ\\bin\\endmqlsr.exe\" -m QM_57"
```

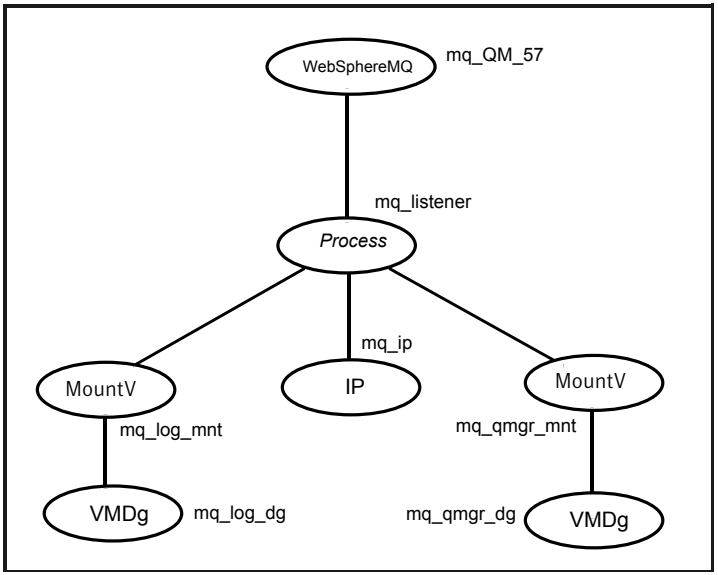
```
UserName = administrator
Password = encrypted_password
Domain = isv-domain
)
VMDg mq_qmgr_dg (
DiskGroupName = mq_qmgr_dg
DGGuid = c844de2f-efbc-431f-b6dd-9a5abc6ece55
)
VMDg mq_log_dg (
DiskGroupName = mq_log_dg
DGGuid = "0dd2cb27-b7e3-4f72-a6a5-2b0e80b90b31"
)
WebSphereMQ mq_queuemgr_QM_57 (
QueueManager = QM_57
CommandServer = 1
Domain = isv-domain
User = administrator
Password = encrypted_password
Home = "C:\\Program Files\\IBM\\WebSphere MQ"
SecondLevelMonitor = 1
)
mq_qmgr_mnt requires mq_qmgr_dg
mq_log_mnt requires mq_log_dg
mq_queuemgr_QM_57 requires mq_listener
mq_listener requires mq_qmgr_mnt
mq_listener requires mq_log_mnt
// resource dependency tree
//
// group mqgrp
// {
//  WebSphereMQ mq_queuemgr_QM_57
//  {
//   Process mq_listener
//   {
//    MountV mq_qmgr_mnt
//    {
//     VMDg mq_qmgr_dg
//    }
//    MountV mq_log_mnt
//    {
//     VMDg mq_log_dg
//    }
//   }
```

```
//   }
// }
```

Sample service group configuration for WebSphere MQ

Figure A-1 depicts a typical service group configuration for WebSphere MQ Queue Manager.

Figure A-1 Service group configuration



Index

A

agent
- installing in VCS environment 13
- removing in VCS environment;uninstalling in VCS environment 15
- sample configuration 72
- upgrading 16

agent attributes
- CommandServer 19
- Domain 19
- Home 19
- MQVer 20
- Password 19
- QueueManager 20
- ResLogLevel 21
- User 20

agent function 11
- clean 12
- monitor 11
- offline 11
- online 11

C

configuring
- active-active configuration 64
- active-passive configuration 64
- WebSphere MQ Listener 66
- WebSphere MQ resource 63

M

Monitor
- WebSphere MQ Queue Manager processes 68

V

virtual environment
- before configuring monitoring 27
- configuring WebSphere MQ queue manager for high availability 29
- launching the wizard 28