Veritas™ Cluster Server One Agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris, ESX,
Windows Server 2003/2008

5.0 Service Pack 1

March 2010

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: 5.0SP1.0

Document version: 5.0SP1.0.0

Legal Notice

Symantec, the Symantec Logo, Veritas, Veritas Storage Foundation 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. 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 automatic software upgrades protection
- 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 web site 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

Documentation feedback

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:

sfha_docs@symantec.com

Support agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Technical Support 3

Chapter 1 Introducing the Veritas Cluster Server One Agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 9

About the agent for Hitachi TrueCopy / HP-XP Continuous Access 10
What's new in this release 10
Supported software for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 11
Supported hardware for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 11
Typical Hitachi TrueCopy / Hewlett-Packard XP Continuous Access setup in a VCS One cluster 11
Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent functions 12
  About the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent's online function 14

Chapter 2 Installing and removing the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 15

Installing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on UNIX 15
  Installing the agent packages using the installer 16
  Installing the agent package using the CLI 17
  Adding the agent resource type definitions to the Policy Master Server on UNIX 18
  Adding the agent resource type definitions to the Policy Master Server on Windows 20
Removing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on UNIX 21
  Removing the agent packages using the installer 21
  Removing the agent package using CLI 22

Removing the agent type definition from the Policy Master system on UNIX 23
Removing the agent type definition from the Policy Master sytem on Windows 23
Installing, modifying and removing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on Windows 24
Before installing the agent 24
Installing the agent 24
Modifying or removing the agent installation 28
Uninstalling the agent pack 30

Chapter 3 Configuring the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 33

Configuration concepts for the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent 33
Resource type definition for the Hitachi TrueCopy agent 33
Attribute definitions for the TrueCopy/HP-XP-CA agent 34
Sample configuration for the TrueCopy/HP-XP-CA agent 37
Before you configure the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 37
Configuring the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 38

Chapter 4 Managing and testing clustering support for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access 39

Failure scenarios in global clusters 39
Testing the global composite service group migration 43
Testing disaster recovery after site failure 44
Testing disaster recovery after client system failure 45
Performing failback after a client system failure or an application failure 46
Performing failback after a site failure 46

Index 49

1

Introducing the Veritas Cluster Server One Agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

This chapter includes the following topics:

- About the agent for Hitachi TrueCopy / HP-XP Continuous Access
- What's new in this release
- Supported software for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access
- Supported hardware for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access
- Typical Hitachi TrueCopy / Hewlett-Packard XP Continuous Access setup in a VCS One cluster
- Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent functions

About the agent for Hitachi TrueCopy / HP-XP Continuous Access

The VCS One agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access provides support for application failover and recovery. The agent provides this support in environments that use TrueCopy/HP-XP-CA to replicate data between Hitachi / HP-XP arrays.

The agent monitors and manages the state of replicated Hitachi / HP-XP devices that are attached to VCS One client systems. The agent ensures that the system that has the TrueCopy/HP-XP-CA resource online also has safe and exclusive access to the configured devices.

You can use the agent in global clusters that run VCS One.

The agent supports TrueCopy/HP-XP-CA in all fence levels that are supported on a particular array.

The agent supports different fence levels for different arrays:

Table 1-1 Supported fence levels

Arrays	Supported fence levels
Hitachi Lightning	data, never, and async
Hitachi Thunder	data and never

The Hitachi TrueCopy / HP-XP Continuous Access agent also supports Hitachi Universal Replicator for asynchronous replication on two sites.

Note: The Veritas Cluster Server One agent Hitachi TrueCopy / HP-XP Continuous Access does not start the Raid Manager. You must start the RAID manager outside Veritas Cluster Server One control for the agent to function correctly.

Note: The terms Hitachi TrueCopy, TrueCopy/HP-XP-CA, and Hitachi TrueCopy/HP XP Continuous Access are all used interchangeably.

What's new in this release

The VCSOne agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access includes the following new or enhanced features:

- The agent for TrueCopy/HP-XP-CA is supported on ESX 3.5/4.0/4i.

- The agent for TrueCopy/HP-XP-CAprovides support for Windows Server 2003 and 2008.

Supported software for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

The agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access supports the following software versions:

Veritas Cluster Server One	■ VCS One 5.0 SP1on AIX ■ VCS One 5.0 SP1 on HP-UX 11i v2, 11iv3 ■ VCS One 5.0 SP1 on Red Hat Enterprise Linux ■ VCS One 5.0 SP1on SUSE Linux Enterprise Server ■ VCS One 5.0 SP1 on Solaris SPARC ■ VCS One 5.0 SP1 on Solaris x64 (OPTERON) ■ VCS One 5.0 SP1 on ESX 3.5/4.0/4i ■ VCS One 5.0 SP1 on Windows Server 2003, 2008. See the product's Release Notes for more details on the supported architectures and the operating system versions.
Command Control Interface (CCI)	All versions

Supported hardware for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

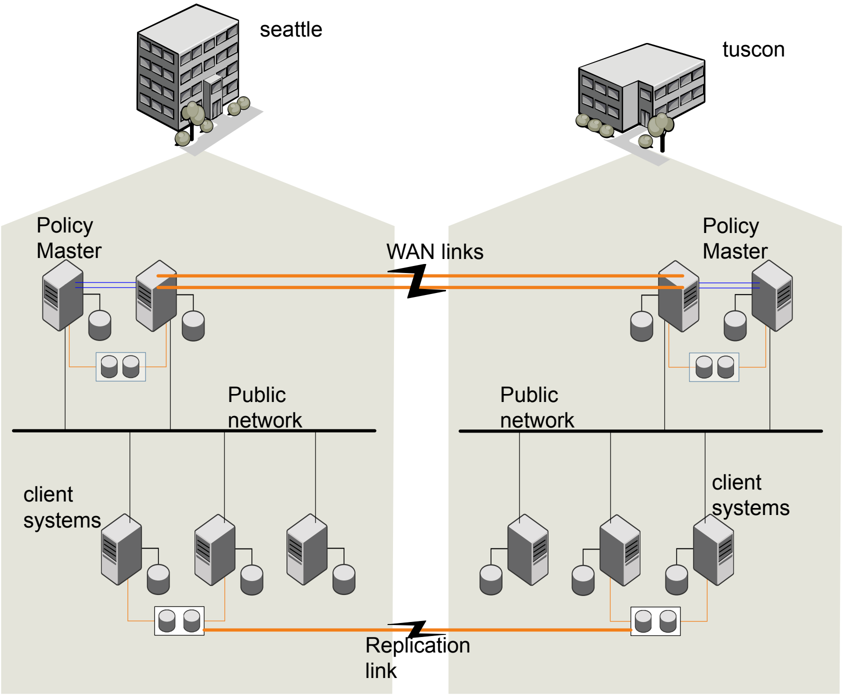
The agent for Hitachi TrueCopy provides support for the following:

- The agent supports TrueCopy on all microcode levels on all arrays, provided the host, HBA, array combination is in Hitachi's hardware compatibility list.
- The agent for Hitachi TrueCopy does not support other Hewlett-Packard replication solutions under the Continuous Access umbrella such as Continuous Access Storage Appliance (CASA). The agent only supports Continuous Access XP.

Typical Hitachi TrueCopy / Hewlett-Packard XP Continuous Access setup in a VCS One cluster

Figure 1-1 displays a typical cluster setup in a TrueCopy/HP-XP-CA environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a TrueCopy/HP-XP-CA environment typically consists of the following hardware infrastructure:

- The primary array (array1) has one or more P-VOL hosts. A Fibre Channel or SCSI directly attaches these hosts to the Hitachi / HP-XP array that contains the TrueCopy/HP-XP-CA P-VOL devices.
- The secondary array (array2) has one or more S-VOL hosts. A Fibre Channel or SCSI directly attaches these hosts to a Hitachi / HP-XP array that contains the TrueCopy/HP-XP-CA S-VOL devices. The S-VOL devices are paired with the P-VOL devices in the P-VOL array. The S-VOL hosts and arrays must be at a significant distance to survive a disaster that may occur at the P-VOL side.

Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent functions

The VCS One enterprise agent for Hitachi TrueCopy monitors and manages the state of replicated devices that are attached to VCS One client systems.

The agent performs the following functions:

online	If the state of all local devices is read-write enabled, the agent creates a lock file on the local host to indicate that the resource is online. This action makes the devices writable for the application. If one or more devices are not in a writable state, the agent runs the `horctakeover` command to enable read-write access to the devices. See "About the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent's online function" on page 14.
offline	The agent removes the lock file that was created for the resource by the online entry point. The agent does not run any TrueCopy commands because taking the resource offline is not indicative of an intention to give up the devices.
monitor	Verifies the existence of the lock file to determine the resource status. If the lock file exists, the agent reports the status of the resource as online. If the lock file does not exist, the agent reports the status of the resource as offline. The monitor entry point does not examine the state of the devices or the state of the replication link between the arrays.
open	Removes the lock file from the host on which this entry point is called, only when the dependent resources or service groups or Vframes dependent on this HTC resource are offline. This functionality prevents potential concurrency violation if the group fails over to another node. `hastop -client -local -force`
clean	Determines whether if it is safe to fault the resource if the online entry point fails or times out. The main consideration is whether a management operation was in progress when the online thread timed out and was killed. If a management operation was in progress, it could potentially leave the devices in an unusable state.
info	Reports the current role and status of the devices in the device group. This entry point can be used to verify the device state and to monitor dirty track trends.

action	The agent supports the following actions using the `hares -action` command from the command line: ■ pairdisplay—Displays information about all devices. ■ pairresync—Resynchronizes the S-VOL devices from the VCS One command line after connectivity failures are detected and corrected. ■ pairresync-swaps—Promotes the S-VOLs to P-VOLs and resynchronizes the original P-VOLs. ■ localtakeover—Makes the local devices write-enabled.

About the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent's online function

If the state of all local devices is read-write enabled, the agent makes the devices writable by creating a lock file on the local host.

If one or more devices are not in a writable state, the agent runs the `horctakeover` command to enable read-write access to the devices.

For S-VOL devices in any state other than SSWS, the agent runs the `horctakeover` command and makes the devices writable. The time required for failover depends on the following conditions:

- The health of the original primary.
- The RAID Manager timeouts as defined in the horcm configuration file for the device group.

The agent considers P-VOL devices writable and takes no action other than going online, regardless of their status.

If the S-VOL devices are in the COPY state, the agent runs the `horctakeover` command after one of the following:

- The synchronization from the primary completes.
- When the OnlineTimeout period of the entry point expires, the command `horctakeover` will not be executed, in which case the resource faults.

2

Installing and removing the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

This chapter includes the following topics:

- Installing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on UNIX
- Removing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on UNIX
- Installing, modifying and removing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on Windows

Installing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on UNIX

You must install the agent for TrueCopy/HP-XP-CA on all the client systems of the VCS One cluster that will host the TrueCopy/HP-XP-CA service group. You can install the agent for TrueCopy/HP-XP-CA using the installagpack program or using the command line interface (CLI).

The installation of the agent packs involves the following phases:

Installing the agent packages	See "Installing the agent packages using the installer" on page 16.

Adding the agent resource type definitions	See "Adding the agent resource type definitions to the Policy Master Server on UNIX" on page 18. See "Adding the agent resource type definitions to the Policy Master Server on Windows" on page 20.

Note: The installagpack program supports only the -addtypes, -rmtypes, -responsefile, and -rsh options. Symantec recommends that you do not use any of the other options from the `installagpack` command help output.

Installing the agent packages using the installer

You can install the agent packages on one or more client systems of a specific platform type.

Note: To install the VCS One client for managing VMware ESX Servers, use the software disc for Red Hat Enterprise Linux 4 (RHEL 4) x86 (32-bit) or RHEL 5 x86_64

Perform the following steps to install the agent packages using the installer

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.
2. Depending on the platform type, navigate to the directory containing the agent installer:

AIX	`cd1/aix/vcsone/`*`vcsone_version`*
HP-UX	`cd1/hpux/hpux`*`os_version`*`/vcsone/`*`vcsone_version`* Where *os_version* is the HP-UX version.
Linux	`cd1/linux/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`cd1/solaris/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where, *dist_arch* is 'sol_sparc' or 'sol_x64'.

3. Enter the following command to start the agent pack installation:

   ```
   # ./installagpack [-rsh]
   ```

   You can use the `-rsh` option if rsh and rcp are used for communication between systems instead of the default ssh and scp. This option requires that systems be preconfigured such that the `rsh` commands between systems execute without prompting for passwords or confirmations.
4. Enter the name of the client systems where you want to install the agents.
5. Choose whether to install all the agents or any specific agent. Follow the installer prompt to specify your option.
6. Review the output as the installation program installs the agent packages.

   You can view installation logs in the /var/VRTS/install/logs directory.

Installing the agent package using the CLI

You can install the desired agent package using the CLI, on one or more client systems of a specific platform type.

Perform the following steps to install the agent packages using CLI

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.
2. Depending on the platform type, navigate to the directory containing the agent installer:

AIX	# **cd1/aix/vcsone/vcsone_version/pkgs**
HP-UX	# **cd1/hpux/hpux*os_version*/vcsone/vcsone_version/depot**
Linux	# **cd1/linux/*dist_arc*h/vcsone/vcsone_version/rpms** Where, *dist* is the Linux distribution and *arch* is the architecture
Solaris	# **cd1/solaris/*dist_arch*/vcsone/vcsone_version/pkgs** Where *dist_arch* is 'sol_sparc' or 'sol_x64'

3. Type the following command on each client system to install the agent. Answer the prompt accordingly:

AIX	# **installp -ac -d . VRTSvcstc.rte**
HP-UX	# **swinstall -s \`pwd\` VRTSvcstc**
Linux	# **rpm -ivh VRTSvcstc_rpm_filename**
Solaris	# **pkgadd -d . VRTSvcstc**

Adding the agent resource type definitions to the Policy Master Server on UNIX

You must add the agent resource type definitions to the Policy Master database configuration. You can perform this task from any client system in the VCS One cluster.

Note: You must add the agent resource type definitions only one time per platform type.

To add the agent resource types to the policy master database configuration

1. Set up RSH or SSH communications between the client system and the policy master system.

   For information on configuring SSH for remote communication, refer to the *Veritas Cluster Server One Installation Guide*.

2. Make sure that the PM daemon is running.

   ```
   # /opt/VRTSvcsone/bin/haclus -display
   ```

   The output should show ClusterState is RUNNING.

3. If you have just installed the agents on VCS One client systems and still have the VCS One Agent Pack software disc mounted, skip to step 6.

4. Mount the VCS One Agent Pack software disc.

5. Depending on the platform type, navigate to the directory containing the agent installer:

AIX	`cd1/aix/vcsone/`*`vcsone_version`*
HP-UX	`cd1/hpux/hpux`*`os_version`*`/vcsone/`*`vcsone_version`* Where *os_version* is the HP-UX version.
Linux	`cd1/linux/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`cd1/solaris/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist_arch* is the sol_sparc or sol_x64.

6. Enter the command to start the agent pack installer for adding resource types to the Policy Master configuration database. Use the `-addtypes` option:

   ```
   # ./installagpack -addtypes
   ```

7. When the installer prompts, enter the virtual IP address of the Policy Master.

8. Review the output as the installer verifies communication with the Policy Master system.

9. Choose whether to add the type definitions for all the agents or for specific agents. Follow the installer prompts to add the type definitions.
10. Review the output as the installer adds the agent types to the PM database configuration and copies the appropriates types.xml files to the PM system.

    You can view installation logs in the /var/VRTS/install/logs directory.

Adding the agent resource type definitions to the Policy Master Server on Windows

After you have installed the agent package, you must add the agent resource type definitions to the Policy Master database configuration. You must perform this task from the Policy Master Server.

Note: You must add the agent resource type definitions only one time per platform type.

To add the agent resource types to the Policy Master Server on Windows, perform the following steps from the Policy Master Server command prompt

1. Create a temporary directory on the Policy Master Server, to add the type definitions.

```
C:\> mkdir addtypes_tmp
```

2. Change your working directory to the temporary directory created in step 1.

```
C:\> chdir addtypes_tmp
```

3. Insert the VCS One software disc and copy the agent's type xml file in to the temporary directory.
4. Convert this type xml file into type cmd file.

```
C:\addtypes_tmp> haconf -xmltocmd type_xml_filename.xml
```

5. Rename the *type_xml_filename*.xml.cmd file to *type_xml_filename*.bat
6. Run the batch file.

```
C:\addtypes_tmp> type_xml_filename.bat >log.txt 2>&1
```

7. Review the log.txt file for any errors.
8. Verify whether the type has been successfully added to the Policy Master Server.

```
C:\addtypes_tmp> hatype -list -platform platform_name
```

Removing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on UNIX

Removing the agent package involves removing the agent files from each client system where it was installed.

You can remove the packages using the agent pack installer or the command line.

See "Removing the agent packages using the installer" on page 21.

See "Removing the agent package using CLI" on page 22.

After removing the agent packages you can remove the agent type definition from the Policy Master system.

See "Removing the agent type definition from the Policy Master system on UNIX" on page 23.

See "Removing the agent type definition from the Policy Master sytem on Windows" on page 23.

Removing the agent packages using the installer

You can remove all the agent packages or the desired agent package using the uninstallagpack program.

Note: The uninstallagpack program supports only the -responsefile and -rsh options. Symantec recommends that you do not use any of the other options from the `uninstallagpack` command help output.

To remove the agent packages from the client systems

1. Freeze the service groups that hosts the application, on the system from which you want to remove the agent package.

   ```
   # hagrp -freeze <groupname>
   ```

2. Stop the agent on all client systems before you remove the agent package from the system.

   ```
   # haagent -stop -notransition <AgentName> -sys <system_name>
   ```

3. Ensure that the agent operations are stopped on all the cluster systems.

   ```
   # haagent -display <AgentName>
   ```

4. Mount the VCS One Agent Pack software disc on the client system where you plan to run the uninstallagpack program.

5 Depending on the platform type, navigate to the directory containing the agent uninstaller:

AIX	**cd1/aix/vcsone/*vcsone_version***
HP-UX	**cd1/hpux/hpux*os_version*/vcsone/*vcsone_version*** Where *os_version* is the HP-UX version.
Linux	**cd1/linux/*dist_arch*/vcsone/*vcsone_version*** Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	**cd1/solaris/*dist_arch*/vcsone/*vcsone_version*** Where *dist_arch* is the sol_sparc or sol_x64.

6 Start the uninstallagpack program.

```
# ./uninstallagpack [-rsh]
```

7 Enter the name of the client systems on which you want to uninstall the agent pack. The names must be separated by spaces.

8 Choose whether to remove all the agent packages or a specific agent package. Follow the installer prompt to remove the agent package.

9 Review the output as the program verifies the agent pack that you installed and removes the agent packages.

You can view logs in the /var/VRTS/install/logs directory.

Removing the agent package using CLI

You can remove a desired agent package using the CLI.

Note: You must remove this agent package from each client system in the cluster.

To remove the agent for TrueCopy/HP-XP-CA from a client system

◆ Type the following command on each client system to remove the agent. Answer prompts accordingly:

AIX	`# installp -u VRTSvcstc`
HP-UX	`# swremove VRTSvcstc`
Linux	`# rpm -e VRTSvcstc`
Solaris	`# pkgrm VRTSvcstc`

Removing the agent type definition from the Policy Master system on UNIX

After you remove the agent packages, you can remove the agent type definitions for agents you removed, from the Policy Master system.

To remove the agent type definition from the Policy Master system on UNIX

1. Navigate to the following directory on the client system.

   ```
   # cd /opt/VRTS/install
   ```

2. Run the following command to remove the agent type definition from the Policy Master system:

   ```
   # ./installagpack -rmtypes
   ```

3. When the installer prompts, enter the virtual IP address of the Policy Master.
4. Choose whether to remove the type definitions for all the agents or for specific agents. Follow the installer prompts to remove the type definitions.

   You can view logs in the /var/VRTS/install/logs directory.

Removing the agent type definition from the Policy Master sytem on Windows

After you remove the agent packages, you can remove the agent type definitions for agents you removed, from the Policy Master system.

To remove the agent type definition from the Policy Master system on Windows

◆ Run the following command from the Policy Master Server command prompt.

C:\> hatype -delete *agentname*_i.e._*typename* -platform *platformname*

Installing, modifying and removing the Veritas Cluster Server One agent for TrueCopy/HP-XP-CA on Windows

This section describes how to install, modify or remove the the VCS One agent for TrueCopy/HP-XP-CA, from the selected client systems.

Before installing the agent

Ensure that you have performed the following tasks before you proceed to install the VCS One agent for TrueCopy/HP-XP-CA.

- Verify that you have installed and configured VCS One client on all cluster systems.
  Refer to the *Veritas Cluster Server One Installation and Configuration Guide* for instructions.
- Verify that you have Local Administrator privileges on the system where you want to install the agent.

Installing the agent

Use the VCS One Agent Pack Installer, to install the agent.

You can launch the installer from the Policy Master Server and install the agent on the desired client systems or launch the installer from the client system and install the agent on a local as well as remote client systems.

Along with the agent installation, you can also update the agent resource types on the Policy Master Server.

Note: Updating the agent resource type is an one time activity. If you plan to update the resource type using the installer, you must run the installer from a client system.

To install the agent

1. Insert the agent pack software disc and run the `setup.exe` file.
2. On the CD Browser Welcome panel, under the Product Installation menu, click **VCS One Agent Pack**.

3. On the Agent Pack Installer Welcome panel, review the pre-requisites and click **Next**.
4. On the License Agreement panel, review the End User License Agreement and select **I accept the terms of License Agreement** and then click **Next**.
5. On the Option Selection panel, select the agents you want to install and click **Next**.
6. On the System Selection panel, add the systems on which you want to install the VCS One Agent Pack. You can perform this in one of the following ways:
   - In the System Name text box, manually type the system name and click **Add**.
   - Alternatively, browse to select the systems.
     On the Select Systems panel, the systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click **OK**.

   Once you add or select a system, the wizard performs the verification checks and notes the verification details. To review the details, click the corresponding information icon.

   By default the wizard uses %ProgramFiles%\Veritas as the installation directory. However, if you have customized your installation directory during the VCS One client installation, the agent pack uses the customized directory as the installation directory.
7. On the System Selection panel, click **Next**.

   Note that the installer fails to proceed with the installation, unless all the selected systems have passed the verification checks and are ready for installation. In case the verification checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the installation click **Re-verify** to re-initiate the verification checks for this system.
8. On the Pre-install Summary panel, review the summary and click **Next**.
9. On the Installation panel, review the progress of installation and click **Next** when the installation is complete.
10. On the Post-install Summary panel, review the installation result and click **Next**.

    If the installation has failed on any of the system, refer to the log file for details.

11 On the Finish panel, click **Finish**, if you plan to only install the agent. You can now configure the agent on the systems where the installation was successful.

However, if you also plan to update the agent resource types on the Policy Master Server on Windows, click **Next**.

Note: If you are updating the resource types on the Policy Master Server on UNIX,

See “Adding the resource types to the Policy Master Server on UNIX” on page 27.

12 For updating the agent resource type, specify the following details on the Policy Master details panel, and then click **Next**.

Policy Master: IP Address: Port:	Type the virtual IP address of the Policy Master (PM). Do not specify the physical IP address of the PM server. Type the port number used by the PM. The default port is 14151.
Use Logged-on user credentials	This check box is selected by default. Continue with the selection if you want the wizard to use the logged on user account context to perform the client configuration tasks. The credentials values are populated in the respective fields below and the fields are disabled by default. If you do not want to use the logged on user account context, clear this check box and enter the relevant credentials in the fields below.
User Name	Type a user name **Note:** This user account must be configured on the Policy Master and must have read access to the VCS One OU and the privileges to add and modify service groups. The user account must also have the privileges to attach service groups to the desired OUValue. If you choose to use the logged-on user, ensure that the logged-on user account has these privileges.
Password	Type the password for the specified user.
Domain Type	Select the appropriate domain type from the drop-down list. For a Windows PM, select unixpwd or nt.
Domain Name	Type the qualified domain name of the Policy Master (PM) server. For example, if your PM is in the domain mydomain.com, type mydomain.

13 On the Policy Master Type Update panel, review the progress and click **Finish** after the process is complete.

Adding the resource types to the Policy Master Server on UNIX

After you install the agent, you must add the agent resource type to the Policy Master Server.

To add the agent resource type to the Policy Master on UNIX, perform the following steps from the Policy Master Server

1. Create a temporary folder on the Policy Master Server.

   ```
   # mkdir addtypes_tmp
   ```

2. Change your working directory to the temporary directory created in step 3 above.

   ```
   # chdir addtypes_tmp
   ```

3. Mount the VCS One software disc and navigate to the following directory:

   DVD\Installer\PMTypeUpdate

4. Copy the resource type XMLs for the required agent type into the temporary directory.

5. Convert the type XML file to type cmd file.

   ```
   /opt/VRTSvcsone/bin/haconf -xmltocmd resource-type-XML
   target-directory
   ```

6. Run the newly generated .cmd file to add the resource type to the Policy Master database.

Modifying or removing the agent installation

To remove the agents installed or to install additional VCS One agents, for high availability of other applications, you must run the VCS One Agent Pack Installer in the modify mode.

Note that you can run the VCS One Agent Pack Installer in the modify mode, only on the local client system.

To modify the agent installation

1. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**. In case you are working on Windows Server 2008, go to Programs and Features. (**Start** > **Settings** > **Control Panel** > **Programs and Features**)

2. Scroll to VCS One Agent Pack and select it.

3. Click **Change**.

4. On the Mode Selection panel, select **Add or Remove**, to perform either of the following tasks:

   - Install another VCS One agent available in the agentpack.
   - Remove the installed VCS One agent.

5. On the Option Selection panel, the agents that are already installed are selected by default. Depending on the task you want to perform,
   - Clear the selection for the agents you want to remove
   - Select the agents you want to add
6. On the System Selection panel, click **Next**.
7. On the Pre-Install panel, review the pre-update report and click **Next**.
8. On the Installation panel, review the progress and click **Next** after the process is complete.
9. On the Post-Install panel, review the Post-update report and click **Next**.
10. On the Finish panel, click **Finish** if you have removed any agent. However, if you have added any agent, click **Next**, to update the agent resource type on the Policy Master Server.

11 On the Policy Master details panel, specify the following details and then click **Next**.

Policy Master: IP Address: Port:	Type the virtual IP address of the Policy Master (PM). Do not specify the physical IP address of the PM server. Type the port number used by the PM. The default port is 14151.
Use Logged-on user credentials	This check box is selected by default. Continue with the selection if you want the wizard to use the logged on user account context to perform the client configuration tasks. The credentials values are populated in the respective fields below and the fields are disabled by default. If you do not want to use the logged on user account context, clear this check box and enter the relevant credentials in the fields below.
User Name	Type a user name **Note:** This user account must be configured on the Policy Master and must have read access to the VCS One OU and the privileges to add and modify service groups. The user account must also have the privileges to attach service groups to the desired OUValue. If you choose to use the logged-on user, ensure that the logged-on user account has these privileges.
Password	Type the password for the specified user.
Domain Type	Select the appropriate domain type from the drop-down list. For a Windows PM, select unixpwd or nt.
Domain Name	Type the qualified domain name of the Policy Master (PM) server. For example, if your PM is in the domain mydomain.com, type mydomain.

12 On the Policy Master Type Update panel, review the progress and click **Finish** after the process is complete.

Uninstalling the agent pack

You can uninstall the VCS One Agent Pack, using the VCS One Agent Pack Installer.

You can uninstall the agents from the local as well as multiple remote client systems.

To uninstall the agent

1. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.

   In case you are working on Windows Server 2008, go to Programs and Features. (**Start** > **Settings** > **Control Panel** > **Programs and Features**)

2. Scroll to VCS One Agent Pack and select it.

3. Click **Remove**.

   In case of Windows Server 2008, click **Uninstall**.

4. On the VCS One Agent Pack Installer welcome page, review the list of prerequisites and click **Next**.

5. On the System Selection panel, add the systems from which you want to uninstall the VCS One client. You can perform this in one of the following ways:

   - In the System Name text box, manually type the system name and click **Add**.
   - Alternatively, browse to select the systems.
     The systems that belong to the domain in which you have logged in are listed in the Available Systems list. Select one or more systems and click the right arrow to move them to the Selected Systems list. Click **OK**.
     Once you add or select a system, the wizard performs the verification checks and notes the verification details. To review the details, click the corresponding information icon.

     Note: By default the local system is selected for un-installation. In case you are performing a remote un-installation and do not want to uninstall the AgentPack from the local system, click the corresponding <remove> icon to remove the system from the list.

6. Click **Next**.

   Note that the wizard fails to proceed with the un-installation, unless all the selected systems have passed the validation checks and are ready for un-installation. In case the validation checks have failed on any of the system, review the details and rectify the issue. Before you choose to proceed with the un-installation click **Re-verify** to re-initiate the verification checks for this system.

7. On the Pre-uninstall Summary panel, review the summary and click **Next**.

8. On the VCS One Agent Pack Un-installation panel, review the uninstallation progress and click **Next** when the uninstallation is complete.

9. On the Post-uninstall Summary panel, review the uninstallation results and click **Next**.

   If the un-installation has failed on any of the system, review its summary report and check the log file for details.

10. On the Finish panel, click **Finish**.

Chapter 3

Configuring the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

This chapter includes the following topics:

- Configuration concepts for the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent
- Before you configure the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access
- Configuring the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

Configuration concepts for the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent

Review the resource type definition and attribute definitions for the agent.

Resource type definition for the Hitachi TrueCopy agent

The resource type definition represents the VCS One configuration of the agent and specifies how the agent is defined in the configuration file main.xml. For more information, refer to the sample HTCTypes.platform.xml files in the `/etc/VRTSagents/ha/conf/HTC` directory on the primary client system.

Attribute	**Default value**
BaseDir	/HORCM/usr/bin
GroupName	<No default value>
Instance	<No default value>
SplitTakeover	0
LinkMonitor	0

Attribute definitions for the TrueCopy/HP-XP-CA agent

Following are the attributes associated with the agent:

BaseDir	Path to the RAID Manager Command Line interface. Type-dimension: string-scalar Default: /HORCM/usr/bin. Default: `C:\\HORCM\\etc`.
GroupName	Name of the device group that the agent manages. Type-dimension: string-scalar
Instance	The Instance number of the device that the agent manages. Multiple device groups may have the same instance number. Do not define the attribute if the instance number is zero. Type-dimension: string-scalar
SplitTakeover	A flag that determines whether the agent permits a failover to S-VOL devices if the replication link is disconnected (i.e. when P-VOL devices are in the PSUE state) or the replication link is manually suspended (i.e. when P-VOL devices are in the PSUS state). See “About the SplitTakeover attribute for the Hitachi TrueCopy agent” on page 35. Type-dimension: integer-scalar Default: 0
User	The domain user account under which HORCM Manager is started, if it is not running. Type-dimension: string-scalar

Domain	The domain for the account specified in the User field This user must have sufficient privileges to perform the HORCM commands. Type-dimension: string-scalar
Password	The password for the user account specified in the User field. This password must be encrypted using the encryption tool provided by VCS i.e. `vcsencrypt -agent`. Type-dimension: string-scalar
LinkMonitor	A flag that defines whether the agent periodically attempts to resynchronize the S-VOL side if the replication link is disconnected. The agent uses the `pairresync` command to resynchronize arrays. The value 1 indicates that when the replication link is disconnected, the agent periodically attempts to resynchronize the S-VOL side using the `pairresync` command. If the value of the LinkMonitor attribute is set to 2, the agent generates SNMP traps or alerts when the status of the attached P-VOL and S-VOL changes. If the status of the configured HTC device changes to PSUE, PSUS, SSUS, or SSWS, the agent generates an SNMP trap indicating that the resource health has gone down. For all other types of status changes of the configured HTC devices, the agent generates an SNMP trap indicating that the resource health has improved. An error or information type message is logged by the agent in the VCS HIgh Availability engine log- "The state of <P-VOL/S-VOL> devices in device group <device group name> has changed from <previous state> to <current state>. Setting LinkMonitor does not affect the SplitTakeover behavior. However, you can minimize the time during which the P-VOL is in the PSUE state by setting the LinkMonitor attribute. Type-dimension: integer-scalar Default: 0
TargetFrozen	For internal use. Do not modify.

About the SplitTakeover attribute for the Hitachi TrueCopy agent

The SplitTakeover attribute determines whether the agent permits a failover to S-VOL devices if the replication link is disconnected, (that is, if P-VOL devices are in the PSUE state) or if the replication is manually suspended, (that is, if P-VOL devices are in the PSUS state).

SplitTakeover attribute = 0

The default value of the SplitTakeover attribute is 0.

The default value indicates that the agent does not permit a failover to S-VOL devices if the P-VOL devices are in the PSUE state. If a failover occurs when the replication link is disconnected, data loss may occur because the S-VOL devices may not be in sync.

In this scenario, the agent attempts to contact the RAID manager at the P-VOL side to determine the status of the arrays. If the P-VOL side is down, the agent attempts to go online.

With the SplitTakeover attribute set to 0, the agent attempts to contact the RAID manager at the P-VOL side to determine the status of the arrays. If the P-VOL side is not PSUE or not reachable, the agent proceeds with failover.

With the SplitTakeover attribute set to 0 and the status of the HTC device changed to PSUS (Pair Suspended Manually), the service groups at the remote site are frozen.

If a device group is made up of multiple devices, then, in case of a link failure, the state of each device changes on an individual basis. This change is not reflected on the device group level. Only those devices to which an application made a write after a link failure change their state to PSUE. Other devices in the same device group retain their state to PAIR.

Note: Setting LinkMonitor does not affect the SplitTakeover behavior. However you can minimize the time during which the P-VOL is in the PSUE by setting the LinkMonitor attribute.

SplitTakeover attribute = 1

If the value of SplitTakeover is 1, the agent tries to make the SVOL devices writable, irrespective of the state of PVOL devices. Hence, even if there is a replication link failure, or the primary array fails, the agent attempts to failover to the S-VOL devices.

About the HTC configuration parameters

The TrueCopy/HP-XP-CA agent uses RAID manager to interact with Hitachi devices. All information about the remote site is exchanged mainly over the network.

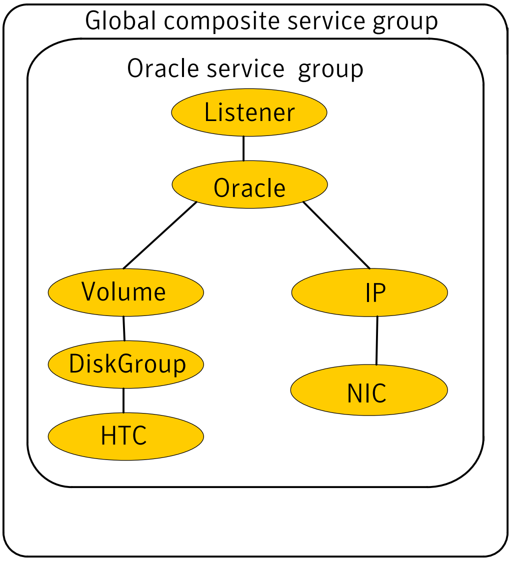
To obtain information on the remote cluster of the pair, mention the details of the remote site in the instance configuration file.

Update the HORCM_INST section of the configuration file.

Sample configuration for the TrueCopy/HP-XP-CA agent

Figure 3-1shows a dependency graph of a VCS One global composite service group that has a resource of type HTC.

Figure 3-1 VCS One global composite service group with resource type HTC



Before you configure the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

Before you configure the agent, review the following information:

- Review the configuration concepts, which describe the agent's type definition and attributes.
  See "Configuration concepts for the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent" on page 33.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical Hitachi TrueCopy / Hewlett-Packard XP Continuous Access setup in a VCS One cluster" on page 11.
- Verify that the clustering infrastructure is in place.
  - If you plan to configure the agent in a global cluster, make sure the global composite service group for the application is configured.

For more information, see the *Veritas Cluster Server One User's Guide*.

Configuring the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

You can adapt most clustered applications to a disaster recovery environment by:

- Converting their devices to TrueCopy/HP-XP-CA devices
- Synchronizing the devices
- Adding the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent to the service group

Note: You must not change the replication state of a cluster from primary to secondary and viceversa, outside of a VCS One setup. The agent for Hitachi TrueCopy / HP-XP Continuous Access fails to detect a change in the replication state if the role reversal is done externally.

4

Managing and testing clustering support for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

This chapter includes the following topics:

- Failure scenarios in global clusters
- Testing the global composite service group migration
- Testing disaster recovery after site failure
- Testing disaster recovery after client system failure
- Performing failback after a client system failure or an application failure
- Performing failback after a site failure

Failure scenarios in global clusters

Table 4-1 lists the failure scenarios in a global cluster configuration and describes the behavior of VCS One and the agent in response to the failure.

See the *Veritas Cluster Server One User's Guide* for more information on the DR configurations and the global composite service group attributes.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access

Failure	Description and VCS One response
Application failure	Application cannot start successfully on any client system at the primary site. VCS One response at the secondary site: ■ Causes global composite service group at the primary site to fault and triggers a BPA event. ■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site. Agent response: ■ Write enables the devices at the secondary site. ■ The agent does the following: ■ Swaps the P-VOL/S-VOL role of each device in the device group. ■ Restarts replication from P-VOL devices on the secondary site to the S-VOL devices at the primary site. See "Performing failback after a client system failure or an application failure" on page 46.
Client system failure	All client systems at the primary site fail. VCS One response at the secondary site: ■ Triggers a BPA event. ■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site. Agent response: ■ Write enables the devices at the secondary site. ■ The agent does the following: ■ Swaps the P-VOL/S-VOL role of each device in the device group. ■ Restarts replication from P-VOL devices on the secondary site to the S-VOL devices at the primary site.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS One response
Site failure	All PMs, client systems, and their storage at the primary site fail. VCS One response at the secondary site: ■ Triggers a BPA event. ■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site. Agent response: The agent does the following on the secondary site in case of a manual failover based on the value of the SplitTakeover attribute of the HTC resource: ■ 1—The agent issues the `horctakeover` command to make the HTC devices write-enabled. The HTC devices go into the SSWS (Suspend for Swapping with S-VOL side only) state. If the original primary site is restored, you must execute the pairresync-swaps action on the secondary site to establish reverse replication. ■ 0 - No action is taken. See "Performing failback after a site failure" on page 46.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS One response
Replication link failure	Replication link between the arrays at the two sites fails. The volume state on the primary site becomes PSUE. VCS One response: No action. Agent response: The agent does the following based on the LinkMonitor attribute of the HTC resource: ■ 1—When the replication link is disconnected, the agent periodically attempts to resynchronize the S-VOL side using the `pairresync` command. ■ 0—No action. If the value of the LinkMonitor attribute is not set to 1, you must manually resynchronize the HTC devices after the link is restored. To manually resynchronize the HTC devices after the link is restored: ■ Before you resync the S-VOL device, you must split off the Shadow Image device from the S-VOL device at the secondary site. ■ You must initiate resync of S-VOL device using the agent's pairresync action. ■ After P-VOL and S-VOL devices are in sync, reestablish the mirror relationship between the Shadow Copy and the S-VOL devices. If you initiate a failover to the secondary site when resync is in progress, the online function of the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent waits for the resync to complete and then initiates a takeover of the S-VOL devices. **Note:** If you did not configure Shadow Copy devices and if disaster occurs when resync is in progress, then the data at the secondary site becomes inconsistent. Symantec recommends configuring Shadow Copy devices at both the sites.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS One response
Network failure	The network connectivity and the replication link between the sites fail. VCS One response: ■ VCS One at each site concludes that the remote cluster has faulted. ■ The global cluster failover in VCS One is manual. No action. ■ You must confirm the cause of network failure from the cluster administrator at each site and fix the issue. To resynchronize the data after the network link is restored: ■ Take the global composite service group offline at both the sites. ■ Manually resync the data. Use the `pairresync swap` command to resynchronize from the secondary. ■ Bring the global composite service group online on the secondary site. Agent response: Similar to the site failure
Storage failure	The array at the primary site fails. VCS One response at the secondary site: ■ Causes the global composite service group at the primary site to fault and triggers a BPA event. ■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site. Agent response: The agent does the following based on the SplitTakeover attribute of the HTC resource: ■ 1—The agent issues the `horctakeover` command to make the HTC devices write-enabled. The S-VOL devices go into the SSWS state. ■ 0—The agent faults the HTC resource.

Testing the global composite service group migration

After you configure the VCS One agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access, verify that the global composite service group can migrate to hosts across the sites. Depending on your DR configuration, perform one of the following procedures.

To test the global composite service group migration in global cluster setup

1. Fail over the global composite service group from the primary site to the secondary site.

   Perform the following steps:

- Switch the global composite service group from the primary site to the secondary site.

  ```
  hacsg -switch <global_csg> -clus <secondary_clusname>
  ```

  VCS One brings the global composite service group online at the secondary site.

- Verify that the HTC devices at the secondary site are write-enabled, and the device state is PAIR.

2 Fail back the global composite service group from the secondary site to the primary site.

  Perform the following steps:

  - Switch the global composite service group from the secondary site to the primary site.

    ```
    hacsg -switch <global_csg> -clus <primary_clusname>
    ```

    VCS One brings the global composite service group online at the primary site.

  - Verify that the HTC devices at the secondary site are write-enabled, and the device state is PAIR.

Testing disaster recovery after site failure

Review the details on site failure and how VCS One and the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access behave in response to the failure.

See “Failure scenarios in global clusters” on page 39.

Depending on the DR configuration, perform one of the following procedures to test the disaster recovery in the event of site failure.

To test disaster recovery for site failure in global cluster setup

1. Halt all client systems and the arrays at the primary site.

   If you cannot halt the array at the primary site, then disable the replication link between the two arrays.

   You must bring the global composite service group online at the secondary site. Run the following command:

   ```
   hacsg -online -force global_csg
   ```

2. Verify that the HTC devices at the secondary site are write-enabled, and the device state is SSWS.
3. Verify that the global composite service group is online at the secondary site.

   ```
   hacsg -state global_csg
   ```

Testing disaster recovery after client system failure

Review the details on client system failure and how VCS One and the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access behave in response to the failure.

See "Failure scenarios in global clusters" on page 39.

Depending on the DR configuration, perform one of the following procedures to test how VCS One recovers after all client systems at the primary site fail.

To test disaster recovery for client system failure in global cluster setup

1. Halt the client system at the primary site.

   You must bring the global composite service group online at the secondary site. Run the following command:

   ```
   hacsg -online -force global_csg
   ```

2. Verify that the HTC devices at the secondary site are write-enabled, and the device state is PAIR.
3. Verify that the global composite service group is online at the secondary site.

   ```
   hacsg -state global_csg
   ```

Performing failback after a client system failure or an application failure

Review the details on client system failure and application failure and how VCS One and the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access behave in response to these failures.

See "Failure scenarios in global clusters" on page 39.

After the client systems at the primary site are restarted, you can perform a failback of the global composite service group to the primary site. Depending on your DR configuration, perform one of the following procedures.

To perform failback after a client system failure or an application failure in global cluster

1. Switch the global composite service group from the secondary site to the primary site.

   ```
   hacsg -switch <global_csg> -clus <remote_clusname>
   ```

   VCS One brings the global composite service group online at the primary site.

2. Verify that the HTC devices at the primary site are write-enabled and the device state is PAIR.

Performing failback after a site failure

After a site failure at the primary site, the hosts and the storage at the primary site are down. VCS One brings the global composite service group online at the secondary site and the Hitachi TrueCopy / Hewlett-Packard XP Continuous Access agent write enables the S-VOL devices.

The device state is SSWS.

Review the details on site failure and how VCS One and the agent for Hitachi TrueCopy / Hewlett-Packard XP Continuous Access behave in response to the failure.

See "Failure scenarios in global clusters" on page 39.

When the hosts and the storage at the primary site are restarted and the replication link is restored, you can perform a failback of the global composite service group to the primary site.

To perform failback after a site failure in global cluster

1. Take the global composite service group offline at the secondary site. At the secondary site, run the following command:

   ```
   hacsg -offline global_csg
   ```

2. Since the application has made writes on the secondary due to a failover, resync the primary from the secondary site and reverse the PVOL/SVOL roles with pairresync-swaps action on the secondary site .

   After the resync is complete, the devices in the secondary are PVOL and the devices in the primary are SVOL .The device state is PAIR at both the sites.

3. Bring the global composite service group online at the primary site. Run the following command:

   ```
   hacsg -online global_csg
   ```

   This again swaps the role of PVOL and SVOL.

A

add
    resource type
        Policy Master on UNIX 18
        Policy Master Server on Windows 20
    resource types
        Policy Master on UNIX 27
agent functions 12
    action 12
    clean 12
    info 12
    monitor 12
    offline 12
    online 12
    open 12
attribute definitions
    Hitachi TrueCopy agent 34
attributes
    BaseDir 34
    Domain 34
    GroupName 34
    Instance 34
    LinkMonitor 34
    Password 34
    SplitTakeover 34
    TargetFrozen 34
    User 34
    VCSResLock 34

B

BaseDir attribute 34
before installing the agent
    Windows client 24

C

configuring
    before 33
    samples 37

D

Domain attribute 34

F

failure scenarios
    global clusters 39
        application failure 39
        client system failure 39
        network failure 39
        replication link failure 39
        site failure 39
        storage failure 39

G

global clusters
    failure scenarios 39
GroupName attribute 34

H

Hitachi TrueCopy agent
    about 10
    attribute definitions 34

I

install
    agent package
        UNIX client 15
        using CLI 17
        using installer 16
        Windows client 24
Instance attribute 34

L

LinkMonitor attribute 34

M

modify
    agent installation 28

P

Password attribute 34

R

remove
  agent installation 28
  agent package
    UNIX client 21
    using CLI 22
    using installer 21
  resource type
    Policy Master on UNIX 23

S

sample configuration 37
SplitTakeover attribute 34

T

TargetFrozen attribute 34
typical setup 11

U

Uninstall
  agent pack
    Windows client 30
User attribute 34

V

VCSResLock attribute 34