Symantec™ Cluster Server Agent for Hitachi TrueCopy/HP-XP Continuous Access Configuration Guide

Windows

6.1

March 2016

Symantec

Symantec Cluster Server Agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access 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

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_apac@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

Chapter 1

Introducing the Symantec 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

The Symantec High Availability 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 TrueCopy/HP-XP arrays.

The agent monitors and manages the state of replicated Hitachi TrueCopy/HP-XP devices that are attached to VCS nodes. 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.

The VCS agent for TrueCopy/HP-XP-CA is enhanced to include additional monitoring and reporting capabilities. You can configure the agent to generate notifications based on the state of the configured HTC devices.

You can use the agent in replicated data clusters and global clusters that run VCS.

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

Supported software

For information on the software versions that the agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Supported hardware

The agent for Hitachi TrueCopy/HP-XP Continuous Access supports all versions of Command Control Interface (CCI).

The agent supports TrueCopy on all microcode levels on all arrays, provided the host, HBA, array combination is in Hitachi's hardware compatibility list.

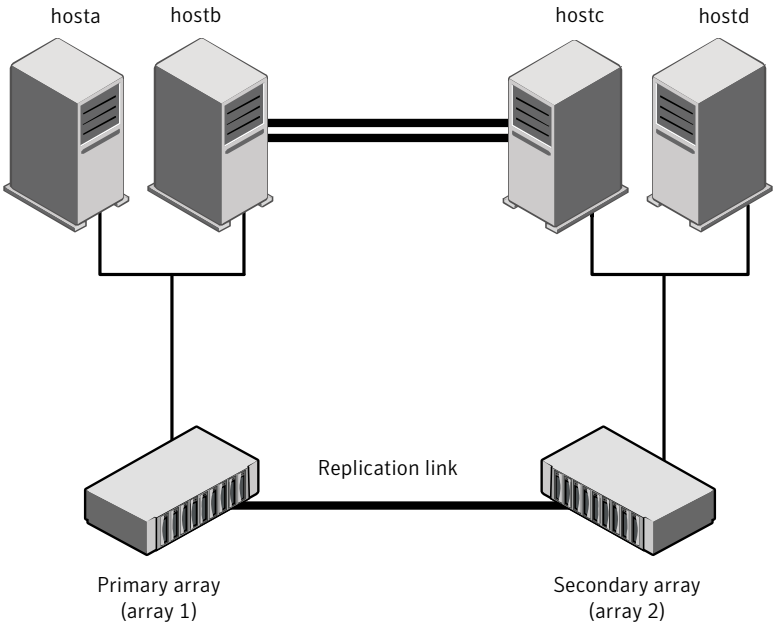
The agent for Hitachi TrueCopy supports HP XP arrays with TrueCopy rebranded as Continuous Access.

The agent does not support other Hewlett-Packard replication solutions under the Continuous Access umbrella such as Continuous Access Storage Appliance (CASA).

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

- Network heartbeating between the two data centers to determine their health; this network heartbeating could be LLT or TCP/IP.
- In a replicated data cluster environment, all hosts are part of the same cluster. You must connect them with the dual and dedicated networks that support LLT. In a global cluster environment, you must attach all hosts in a cluster to the same Hitachi TrueCopy/HP-XP array.

Hitachi TrueCopy/Hewlett-Packard XP Continuous Access agent functions

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

The agent performs the following functions:

online	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/SSUS/SMPL, 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. ■ The OnlineTimeout period of the entry point expires, in which case the resource faults. If the S-VOL devices are in PAIR state, the agent runs the `pairdisplay` command without the `-l` option to retreive the state of the remote site devices. If P-VOL devices are in PAIR state, the agent proceeds with the failover. But if the remote RAID manager is down, then the agent honors the SplitTakeover attribute configuration before performing failover. See "About the Hitachi TrueCopy/Hewlett-Packard XP Continuous Access agent's online function" on page 15.
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. Based on other attribute values, the monitor entry point examines 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. This functionality prevents potential concurrency violation if the group fails over to another node. Note that the agent does not remove the lock file if the agent starts after the following command: `hastop<-all | -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 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.

action\PreSwitch	Ensures that the remote site cluster can come online during a planned failover within a GCO configuration without data loss. The VCS engine on the remote cluster invokes the PreSwitch action on all the resources of the remote Service Group during a planned failover using the `hagrp -switch` command. For this, the PreSwitch attribute must be set to 1. The option `-nopre` indicates that the VCS engine must switch the servicegroup regardless of the value of the PreSwitch service group attribute. If running the PreSwitch action fails, the failover should not occur. This minimizes the application downtime and data loss . For more information on the PreSwitch action and the PreSwitch feature in the VCS engine, refer to the *Symantec Cluster Server Administrator's Guide.*
action\vxdiske	Reports the mapping between the physical disk name and the volume manager disk name for all connected disks.

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

If the state of all local devices is SMPL (Simplex), then the AllowOnlineOnSimplex attribute is honored to allow/disallow resource to come online.

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. If `horctakeover` exits with an error (exit code > 5), for example due to a timeout, then the agent flushes and freezes the group to indicate that user-intervention is required to identify the cause of the error.

For S-VOL devices in any state other than SSWS and SSUS, the agent honors the SplitTakeover attribute and runs the `horctakeover` command to make 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.

If the S-VOL devices are in the SSUS state and if the RoleMonitor attribute is set to 1, the agent runs the pairdisplay command without the -l option, to determine if the S-VOL is in a writable state. The agent behavior when devices are in S-VOL SSUS state is as follows:

- If S-VOL devices are in SSUS writable state, the agent proceeds with online without failover.
- If S-VOL devices are in SSUS read only state, the agent honors the SplitTakeover attribute and accordingly proceeds with failover to make the devices writable.
- In case agent could not connect to remote RAID manager, the agent faults the resource.

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 `horctakeover` command will not be executed, in which case the resource faults.

If S-VOL devices are in PAIR state, the agent issues the `pairdisplay` command without the `-l` option to get the replication link state. If P-VOL devices are in the PAIR state, the agent proceeds with failover. In case remote horcm is down, the SplitTakeover attribute is honored before issuing the `horctakeover` command. The agent validates the value of OnlineTimeout for the HTC type is sufficient to run the `horctakeover` command. If the agent finds this value of OnlineTimeout is insufficient, the agent logs an appropriate error message.

Chapter 2

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

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

Resource type definition for the Hitachi TrueCopy agent

The resource type definition defines the agent in VCS.

```
type HTC (
    static keylist RegList = { SplitTakeover, LinkMonitor, RoleMonitor,
    FreezeSecondaryOnSplit, AllowOnlineOnSimplex }
    static i18nstr ArgList[] = { BaseDir, GroupName, Instance,
    SplitTakeover, LinkMonitor, RoleMonitor, FreezeSecondaryOnSplit,
    AllowOnlineOnSimplex, User, Domain, Password }
    static keylist SupportedActions = { localtakeover, pairresync,
    pairresync-swaps, pairdisplay, PreSwitch, vxdiske }
    str BaseDir = "C:\\HORCM\\etc"
    str GroupName
    int Instance
    int SplitTakeover
    int LinkMonitor
    int RoleMonitor
    int FreezeSecondaryOnSplit
    boolean AllowOnlineOnSimplex = 0
    str User
    str Domain
    str Password
    temp str TargetFrozen
    temp str OldState = ""
)
```

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

Table 2-1 lists the attributes associated with the agent:

Table 2-1 Attributes for the Hitachi TrueCopy agent

Attribute	Description
BaseDir	Path to the RAID Manager Command Line interface. Type-dimension: string-scalar 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: integer

Table 2-1 Attributes for the Hitachi TrueCopy agent *(continued)*

Attribute	Description
SplitTakeover	A flag that determines the following: ■ whether the agent permits a failover to S-VOL devices if the replication link is disconnected (that is, when P-VOL devices are in the PSUE state) ■ whether the agent cannot connect to the remote site RAID manager ■ whether 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 21. Type-dimension: integer-scalar Default: 0
User	The domain user account under which HORCM Manager is started. 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

Table 2-1 Attributes for the Hitachi TrueCopy agent *(continued)*

Attribute	Description
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
RoleMonitor	Determine if the agent must perform detailed monitoring of HTC volumes. If this attribute is set to 0, the agent does not perform detailed monitoring. This attribute is disabled by default. If this attribute is set to 1, the agent monitors the status of the HTC volumes everytime a monitor cycle runs. In addition, the HTC resource comes online only when any of the following conditions are met: ■ When the volume is P-VOL ■ When the volume is S-VOL and the status is SSWS ■ When the volume is S-VOL, the status is SSUS, and the M flag of the corresponding P-VOL is set to W. Type-dimension: integer-scalar Default: 0

Table 2-1 Attributes for the Hitachi TrueCopy agent *(continued)*

Attribute	Description
FreezeSecondaryOnSplit	A flag that determines if the agent must freeze the service group in the remote cluster when the TrueCopy replication link is either split or suspended. The value 1 indicates that the agent must freeze the service group in the remote cluster when the replication link is split or suspended. Type-dimension: integer-scalar Default: 0
AllowOnlineOnSimplex	A flag that determines if the agent must allow a resource to come online when the TrueCopy devices are in SMPL (Simplex) state. This attribute is honored only when the agent attempts to bring a resource online. The value false indicates that the agent must not allow a resource to come online when TrueCopy devices are in SMPL (Simplex) state. Type-dimension: boolean-scalar Default: false
TargetFrozen	For internal use. Do not modify.

About the SplitTakeover attribute for the Hitachi TrueCopy agent

The SplitTakeover attribute determines the following:

- whether the agent permits a failover to S-VOL devices if the replication link is disconnected (that is, when P-VOL devices are in the PSUE state)
- whether the agent cannot connect to the remote site RAID manager
- whether the replication link is manually suspended (i.e. when 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, or if the agent cannot connect to the remote site RAID manager, or if the S-VOL devices are in the SSUS 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.

If the S-VOL devices are in the PAIR state, the agent attempts to contact the RAID manager at the P-VOL side to determine the status of the arrays.

If the P-VOL devices are in the PAIR state, the agent proceeds with failover. But if the P-VOL side is down, the agent attempts to honor the SplitTakeover attribute configuration before proceeding with failover.

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.

SplitTakeover attribute = 1

If there is a replication link failure, or if the primary array fails, or if a pair is suspended, the agent allows failover to the S-VOL devices.

About the FreezeSecondaryOnSplit attribute for the Hitachi TrueCopy agent

In a global cluster environment, if the agent at the P-VOL side detects the PSUE or PSUS state locally and FreezeSecondaryOnSplit is set to 1, then the agent freezes the service group at the S-VOL side to prevent a failover. The agent unfreezes the service group after the link is restored and the devices are resynchronized.

FreezeSecondaryOnSplit attribute = 0

If the value of the FreezeSecondaryOnSplit attribute is 0, the agent unfreezes the remote site service group if it is already frozen. Hence, even if there is a replication link failure, or if the primary array fails, or if a pair is suspended, the agent allows 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.

Specify the value of the ClusterAddress attribute of the remote cluster in the lp_address field against the device group. Symantec recommends that you keep the ClusterService service group online on the same node, where the application service group is online.

The agent honors the default value of the remote RAID manager communication timeout (30sec) and poll (10sec) of the horcm configuration file. If the user modifies the remote RAID manager timeout value and the agent finds it insufficient for online operation, the agent logs an appropriate error message and faults the resource.

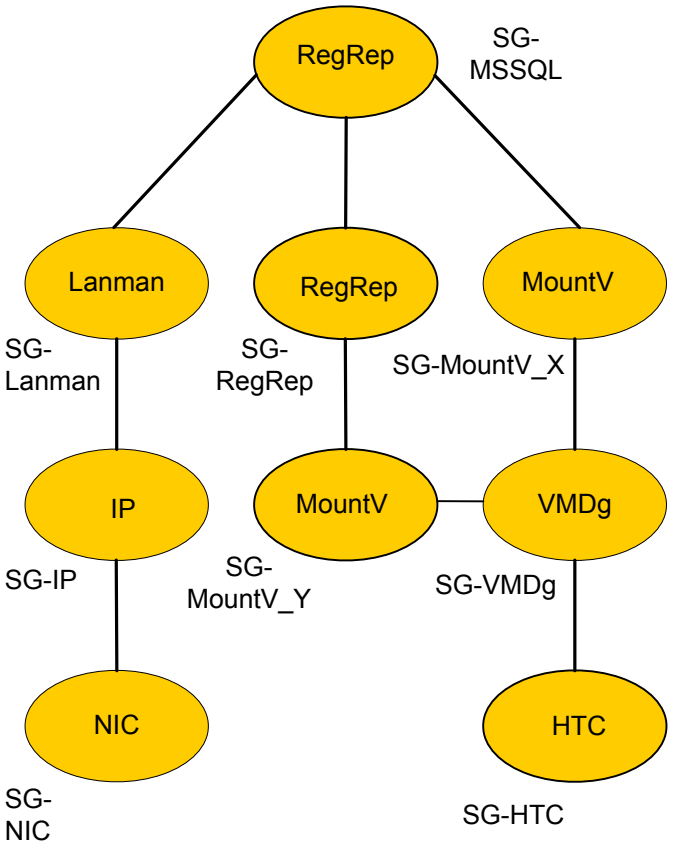
The recommended values of the agent attributes, if the value of remote RAID manager timeout is modified, are as follows:

- The OnlineTimeout value of HTC type should be four times more than the value of remote RAID manager timeout with some additional buffer time (~10sec).
- The MonitorTimeout value of HTC type should be more than twice the value of remote RAID manager timeout with some additional buffer time (~10sec).
- The ActionTimeout value of HTC type should be more than twice the value of remote RAID manager timeout.

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

Figure 2-1 shows a dependency graph of a VCS service group that has a resource of type HTC.

Figure 2-1 VCS service group with resource type HTC



You can configure a resource of type HTC in the main.cf file as:

```
HTC SQLDG (
    GroupName = SQLDG
    Instance = 1
    BaseDir = C:\\HORCM\\etc.
    )
```

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

Before you configure the agent, review the following information:

- 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 cluster" on page 11.
- Make sure that the cluster has an effective heartbeat mechanism in place.
  See "About cluster heartbeats" on page 25.
  See "About preventing split-brain" on page 27.
- Set up system zones in replicated data clusters.
  See "About configuring system zones in replicated data clusters" on page 26.
- Verify that the clustering infrastructure is in place.
  - If you plan to configure the agent in a global cluster, make sure the global service group for the application is configured.
    For more information, see the *Symantec Cluster Server Administrator's Guide*.
  - If you plan to configure the agent in a replicated data cluster, make sure the required replication infrastructure is in place and that the application is configured.
- Ensure that the HORC manager is configured to access the device groups.
  - Verify that the HTC instance is configured appropriately and is in a running state.
  - Verify that the HORC manager CLIs execute successfully. This is essential for the HTC and the HTCSnap agents to be able to fetch HTC-related data and to succesfully perform failover, switchover and other operations.

About cluster heartbeats

In a replicated data cluster, ensure robust heartbeating by using dual, dedicated networks over which the Low Latency Transport (LLT) runs. Additionally, you can configure a low-priority heartbeat across public networks.

In a global cluster, VCS sends ICMP pings over the public network between the two sites for network heartbeating. To minimize the risk of split-brain, VCS sends ICMP pings to highly available IP addresses. VCS global clusters also notify the administrators when the sites cannot communicate.

Hitachi TrueCopy/HP-XP arrays do not support a native heartbeating mechanism between the arrays. The arrays send a support message on detecting replication link failure. You can take appropriate action to recover from the failure and to keep the devices in a synchronized state. The TrueCopy/HP-XP-CA agent supports those actions that can automate the resynchronization of devices after a replication link outage is corrected.

About configuring system zones in replicated data clusters

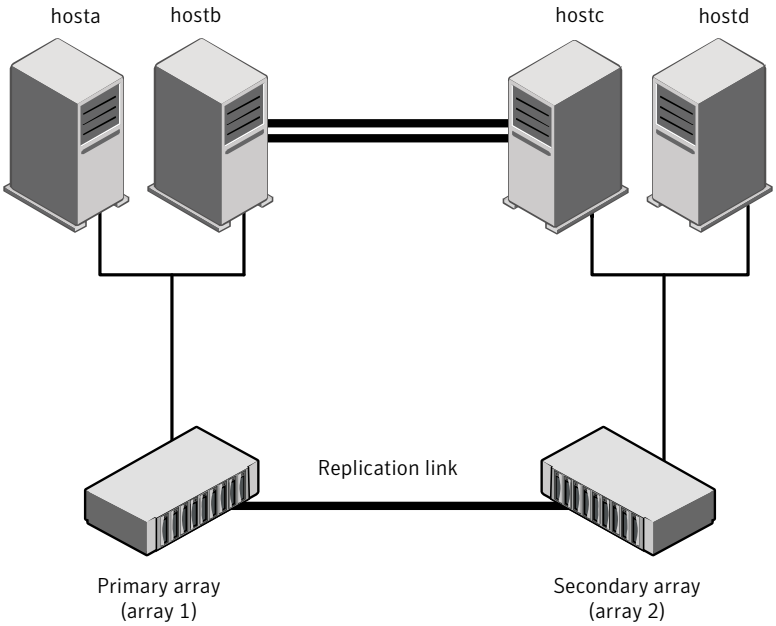
In a replicated data cluster, you can prevent unnecessary TrueCopy/HP-XP-CA failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

Configure the hosts that are attached to an array as part of the same system zone to avoid unnecessary failover.

Figure 2-2 depicts a sample configuration where hosta and hostb are in one system zone, and hostc and hostd are in another system zone.

Use the SystemZones attribute to create these zones.

Figure 2-2 Example system zone configuration



Modify the SystemZones attribute using the following command:

```
hagrp -modify grpname SystemZones hosta 0 hostb 0 hostc 1 hostd 1
```

The variable grpname represents the service group in the cluster.

Global clusters do not require system zones because failover occurs on a remote cluster if all local targets have been exhausted.

About preventing split-brain

Split-brain occurs when all heartbeat links between the primary and secondary hosts are cut. In this situation, each side mistakenly assumes that the other side is down. You can minimize the effects of split-brain by ensuring that the cluster heartbeat links pass through a similar physical infrastructure as the replication links. When you ensure that both pass through the same infrastructure, if one breaks, so does the other.

Sometimes you cannot place the heartbeats alongside the replication links. In this situation, a possibility exists that the cluster heartbeats are disabled, but the replication link is not. A failover transitions the original P-VOL to S-VOL and vice-versa. In this case, the application faults because its underlying volumes become write-disabled, causing the service group to fault. VCS tries to fail it over to another host, causing the same consequence in the reverse direction. This phenomenon continues until the group comes online on the final node. You can avoid this situation by setting up your infrastructure such that loss of heartbeat links also mean the loss of replication links.

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

After configuration, the application service group must follow the dependency diagram.

See “Sample configuration for the TrueCopy/HP-XP-CA agent” on page 23.

Note: You must not change the replication state of devices primary to secondary and viceversa, outside of a VCS 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, and RoleMonitor is disabled.

Configuring the agent manually in a global cluster

Configuring the agent manually in a global cluster involves the following tasks:

To configure the agent in a global cluster

1. Start Cluster Manager (Java Console) and log on to the cluster.
2. If the agent resource type (HTC) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

   systemdrive\Program Files\Veritas\cluster server\conf\Sample_HTC\HTCTypes.cf

3. Click **Import**.
4. Save the configuration.
5. Add a resource of type HTC at the bottom of the service group.

   Link the VMDg and HTC resources so that the VMDg resources depend on HTC.
6. Configure the attributes of the HTC resource.
7. If the service group is not configured as a global service group, configure the service group using the Global Group Configuration Wizard.

   See the *Symantec Cluster Server Administrator's Guide* for more information.
8. Change the ClusterFailOverPolicy attribute from the default, if necessary. Symantec recommends keeping the default, which is Manual, to minimize the chance of failing over on a split-brain.
9. Repeat step 5 through step 8 for each service group in each cluster that uses replicated data.
10. The configuration must be identical on all cluster nodes, both primary and disaster recovery.

Configuring the agent manually in a replicated data cluster

Configuring the agent manually in a replicated data cluster involves the following tasks:

To configure the agent in a replicated data cluster

1. Start Cluster Manager and log on to the cluster.
2. If the agent resource type (HTC) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

   systemdrive\Program Files\Veritas\Cluster Server\conf\config\HTCTypes.cf.

3. Click **Import**.

4 Save the configuration.

5 In each service group that uses replicated data, add a resource of type HTC at the bottom of the service group.

Link the VMDg and HTC resources so that VMDg resources depend on Hitachi Truecopy.

6 Configure the attributes of the HTC resource.

7 Set the SystemZones attribute for the service group to reflect which hosts are attached to the same array.

Chapter 3

Testing VCS disaster recovery support with Hitachi TrueCopy/Hewlett-Packard XP Continuous Access

This chapter includes the following topics:

How VCS recovers from various disasters in an HA/DR setup with Hitachi TrueCopy/Hewlett-Packard XP Continuous Access

This section covers the failure scenarios and how VCS responds to the failures for the following DR cluster configurations:

Global clusters	When a site-wide global service group or system fault occurs, VCS failover behavior depends on the value of the ClusterFailOverPolicy attribute for the faulted global service group. The VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access ensures safe and exclusive access to the configured Hitachi TrueCopy/Hewlett-Packard XP Continuous Access devices. See "Failure scenarios in global clusters" on page 31.
Replicated data clusters	When service group or system faults occur, VCS failover behavior depends on the value of the AutoFailOver attribute for the faulted service group. The VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access ensures safe and exclusive access to the configured Hitachi TrueCopy/Hewlett-Packard XP Continuous Access devices. See "Failure scenarios in replicated data clusters" on page 36.

See the *Symantec Cluster Server Administrator's Guide* for more information on the DR configurations and the global service group attributes.

Failure scenarios in global clusters

Table 3-1 lists the failure scenarios in a global cluster configuration and describes the behavior of VCS and the agent in response to the failure.

See the *Symantec Cluster Server Administrator's Guide* for more information on the DR configurations and the global service group attributes.

Table 3-1 Failure scenarios in a global cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access

Failure	Description and VCS response

Application failure	Application cannot start successfully on any hosts at the primary site.
	VCS response at the secondary site:
	■ Causes global service group at the primary site to fault and displays an alert to indicate the fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto or Connected—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual—No action. You must bring the global group online at the secondary site.
	Agent response:
	■ The agent does the following:
	  ■ Write enables the devices at the secondary site, except when the link is manually suspended with the read-only option.
	  ■ 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 node failure or an application failure" on page 45.
	See "Replication link / Application failure scenarios" on page 41.

Host failure	All hosts at the primary site fail.
	VCS response at the secondary site:
	■ Displays an alert to indicate the primary cluster fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual or Connected—No action. You must bring the global group online at the secondary site.
	Agent response:
	■ The agent does the following:
	  ■ Write enables the devices at the secondary site, except when the link is manually suspended with the read-only option.
	  ■ 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 node failure or an application failure" on page 45.

Table 3-1 Failure scenarios in a global cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response

Site failure	All hosts and the storage at the primary site fail.
	
	VCS response at the secondary site:
	
	■ Displays an alert to indicate the cluster fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual or Connected—No action. You must bring the global 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—Agent does not perform failover to the secondary site.
	
	See "Performing failback after a site failure" on page 46.

Table 3-1 Failure scenarios in a global cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response
Replication link failure	Replication link between the arrays at the two sites fails. The volume state on the primary site becomes PSUE. VCS response: No action. Agent response: When the replication link is disconnected, the agent does the following based on the value of LinkMonitor attribute of the HTC resource: ■ 0—No action. ■ 1—The agent periodically attempts to resynchronize the S-VOL side using the `pairresync` command. ■ 2—The agent periodically attempts to resynchronize the S-VOL side and also sends notifications about the disconnected link. Notifications are sent in the form of either SNMP traps or emails. For information about the VCS NotifierMngr agent, see the *Symantec Cluster Server Bundled Agents Reference Guide*. If the value of the LinkMonitor attribute is not set to 1 or 2, 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. See "Replication link / Application failure scenarios" on page 41.

Table 3-1 Failure scenarios in a global cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response

Network failure	The network connectivity and the replication link between the sites fail.
	VCS response at the secondary site:
	■ VCS at each site concludes that the remote cluster has faulted.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Manual or Connected—No action. You must confirm the cause of the network failure from the cluster administrator at the remote site and fix the issue.
	  ■ Auto—VCS brings the global group online at the secondary site which may lead to a site-wide split brain. This causes data divergence between the devices on the primary and the secondary arrays.
	  When the network (wac and replication) connectivity restores, you must manually resync the data.
	  Note: Symantec recommends that the value of the ClusterFailOverPolicy attribute is set to Manual for all global groups to prevent unintended failovers due to transient network failures.
	To resynchronize the data after the network link is restored:
	■ Take the global service group offline at both the sites.
	■ Manually resync the data.
	  Use the `pairresync-swap` command to resynchronize from the secondary.
	■ Bring the global service group online on the secondary site.
	Agent response: Similar to the site failure.

Storage failure	The array at the primary site fails.
	VCS response at the secondary site:
	■ Causes the global service group at the primary site to fault and displays an alert to indicate the fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto or Connected—VCS automatically brings the faulted global service group online at the secondary site.
	  ■ Manual—No action. You must bring the global 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.

Failure scenarios in replicated data clusters

Table 3-2 lists the failure scenarios in a replicated data cluster configuration, and describes the behavior of VCS and the agent in response to the failure.

Table 3-2 Failure scenarios in a replicated data cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access

Failure	Description and VCS response

Application failure	Application cannot start successfully on any hosts at the primary site.
	VCS response:
	■ Causes the service group at the primary site to fault.
	■ Does the following based on the AutoFailOver attribute for the faulted service group:
	  ■ 1—VCS automatically brings the faulted service group online at the secondary site.
	  ■ 2—You must bring the service group online at the secondary site.
	Agent response:
	■ The agent does the following:
	  ■ Write enables the devices at the secondary site, except when the link is manually suspended with the read-only option.
	  ■ 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 node failure or an application failure" on page 45.
	See "Replication link / Application failure scenarios" on page 41.

Table 3-2 Failure scenarios in a replicated data cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response

Host failure	All hosts at the primary site fail.
	VCS response:
	■ Causes the service group at the primary site to fault.
	■ Does the following based on the AutoFailOver attribute for the faulted service group:
	  ■ 1—VCS automatically brings the faulted service group online at the secondary site.
	  ■ 2—You must bring the service group online at the secondary site.
	Agent response:
	■ The agent does the following:
	  ■ Write enables the devices at the secondary site, except when the link is manually suspended with the read-only option.
	  ■ 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 node failure or an application failure" on page 45.

Table 3-2 Failure scenarios in a replicated data cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response

Site failure	All hosts and the storage at the primary site fail.
	
	VCS response:
	
	■ Causes the service group at the primary site to fault.
	■ Does the following based on the AutoFailOver attribute for the faulted service group:
	  ■ 1—VCS automatically brings the faulted service group online at the secondary site.
	  ■ 2—You must bring the 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 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— Agent does not perform failover to the secondary site.
	
	See "Performing failback after a site failure" on page 46.

Table 3-2 Failure scenarios in a replicated data cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response
Replication link failure	Replication link between the arrays at the two sites fails. VCS response: No action. Agent response: When the replication link is disconnected, the agent does the following based on the LinkMonitor attribute of the HTC resource: ■ 0—No action. ■ 1—The agent periodically attempts to resynchronize the S-VOL side using the `pairresync` command. ■ 2—The agent periodically attempts to resynchronize the S-VOL side and also sends notifications about the disconnected link. Notifications are sent in the form of either SNMP traps or emails. For information about the VCS NotifierMngr agent, see the *Symantec Cluster Server Bundled Agents Reference Guide*. If the value of the LinkMonitor attribute is not set to 1 or 2, you must manually resynchronize the HTC devices after the link is restored. To manually resynchronize the HTC devices after the link is restored: 1 Before you resync the S-VOL device, you must split off the Shadow Image device from the S-VOL device at the secondary site. 2 You must initiate resync of S-VOL device using the agent's pairresync action. 3 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. See "Replication link / Application failure scenarios" on page 41.

Table 3-2 Failure scenarios in a replicated data cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response
Network failure	The LLT and the replication links between the sites fail. VCS response: ■ VCS at each site concludes that the nodes at the other site have faulted. ■ Does the following based on the AutoFailOver attribute for the faulted service group: ■ 2—No action. You must confirm the cause of the network failure from the cluster administrator at the remote site and fix the issue. ■ 1—VCS brings the service group online at the secondary site which leads to a cluster-wide split brain. This causes data divergence between the devices on the arrays at the two sites. When the network (LLT and replication) connectivity is restored, VCS takes all the service groups offline on one of the sites and restarts itself. This action eliminates concurrency violation where in the same group is online at both the sites. After taking the service group offline, you must manually resync the data. **Note:** Symantec recommends that the value of the AutoFailOver attribute is set to 2 for all service groups to prevent unintended failovers due to transient network failures. To resynchronize the data after the network link is restored: **1** Take the service groups offline at both the sites. **2** Manually resync the data. Depending on the site whose data you want to retain use the `pairresync` or the `pairresync-swap` commands. **3** Bring the service group online on one of the sites. Agent response: Similar to the site failure.

Table 3-2 Failure scenarios in a replicated data cluster configuration with VCS agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access *(continued)*

Failure	Description and VCS response

Storage failure	The array at the primary site fails.
	VCS response:
	■ Causes the service group at the primary site to fault and displays an alert to indicate the fault.
	■ Does the following based on the AutoFailOver attribute for the faulted service group:
	  ■ 1—VCS automatically brings the faulted service group online at the secondary site.
	  ■ 2—You must bring the 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 does not perform failover to the secondary site.

Replication link / Application failure scenarios

Table 3-3 shows the link failure scenarios and recommended actions:

Table 3-3 Replication link / Application failure scenarios

Event	Fence level	Recommended action
Link fails and is restored, but application does not fail over.	never, async	Run the `pairresync` action to resynchronize the S-Vols.
Link fails and application fails to the S-VOL side.	never, async, or data	Run the `pairresync-swaps` action to promote the S-VOLs to P-VOLs, and resynchronize the original P-VOLs.
Action faults due to I/O errors.	data	Run the `localtakeover` action to write enable the local devices. Clear faults and restart service group.

Testing the global service group migration

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

To test the global service group migration in global cluster setup

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

Perform the following steps:

- Switch the global service group from the primary site to any node in the secondary site.

```
hagrp -switch global_group -any -clus cluster_name
```

VCS brings the global service group online on a node 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 service group from the secondary site to the primary site.

Perform the following steps:

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

```
hagrp -switch global_group -any -clus cluster_name
```

VCS brings the global 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.

To test service group migration in replicated data cluster setup

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

Perform the following steps:

- Switch the service group from the primary site to any node in the secondary site.

```
hagrp -switch service_group -to sys_name
```

VCS brings the service group online on a node 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 service group from the secondary site to the primary site.

Perform the following steps:

- Switch the service group from the secondary site to any node in the primary site.

  ```
  hagrp -switch service_group -to sys_name
  ```

  VCS brings the service group online on a node 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 host failure

Review the details on host failure and how VCS 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 31.

See "Failure scenarios in replicated data clusters" on page 36.

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

To test disaster recovery for host failure in global cluster setup

1 Halt the hosts at the primary site.

  The value of the ClusterFailOverPolicy attribute for the faulted global group determines the VCS failover behavior.

  - Auto—VCS brings the faulted global service group online at the secondary site.
  - Manual or Connected—You must bring the global service group online at the secondary site.
    On a node in the secondary site, run the following command:

    ```
    hagrp -online -force global_group -any
    ```

2 Verify that the global service group is online at the secondary site.

  ```
  hagrp -state global_group
  ```

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

To test disaster recovery for host failure in replicated data cluster setup

1 Halt the hosts at the primary site.

The value of the AutoFailOver attribute for the faulted service group determines the VCS failover behavior.

- 1—VCS brings the faulted service group online at the secondary site.
- 2—You must bring the service group online at the secondary site.
  On a node in the secondary site, run the following command:

  ```
  hagrp -online service_group -to sys_name
  ```

2 Verify that the service group is online at the secondary site.

```
hagrp -state global_group
```

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

Testing disaster recovery after site failure

Review the details on site failure and how VCS 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 31.

See "Failure scenarios in replicated data clusters" on page 36.

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 nodes 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.

The value of the ClusterFailOverPolicy attribute for the faulted global group determines the failover behavior of VCS.

- Auto—VCS brings the faulted global group online at the secondary site.
- Manual or Connected—You must bring the global group online at the secondary site.
  On a node in the secondary site, run the following command:

```
hagrp -online -force global_group -any
```

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

3 Verify that the global service group is online at the secondary site.

```
hagrp -state global_group
```

To test disaster recovery for site failure in replicated data cluster setup

1 Halt all hosts 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.

The value of the AutoFailOver attribute for the faulted global service group determines the VCS failover behavior.

- 1—VCS brings the faulted global service group online at the secondary site.
- 2—You must bring the global service group online at the secondary site. On a node in the secondary site, run the following command:

```
hagrp -online service_group -sys sys_name
```

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

3 Verify that the global service group is online at the secondary site.

```
hagrp -state global_group
```

Performing failback after a node failure or an application failure

Review the details on node failure and application failure and how VCS 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 31.

See "Failure scenarios in replicated data clusters" on page 36.

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

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

1 Switch the global service group from the secondary site to any node in the primary site.

```
hagrp -switch global_group -any -clus cluster_name
```

VCS brings the global 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.

To perform failback after a host failure or an application failure in replicated data cluster

1 Switch the global service group from the secondary site to any node in the primary site.

```
hagrp -switch service_group -to sys_name
```

VCS brings the global service group online on a node 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 brings the global 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 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 31.

See "Failure scenarios in replicated data clusters" on page 36.

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 service group to the primary site.

To perform failback after a site failure in global cluster

1 Take the global service group offline at the secondary site. On a node at the secondary site, run the following command:

```
hagrp -offline global_group -any
```

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

After the resync is complete, the devices in the secondary are P-VOL and the devices in the primary are S-VOL. The device state is PAIR at both the sites.

3 Bring the global service group online at the primary site. On a node in the primary site, run the following command:

```
hagrp -online global_group -any
```

This again swaps the role of P-VOL and S-VOL.

To perform failback after a site failure in replicated data cluster

1 Take the global service group offline at the secondary site. On a node in the secondary site, run the following command:

```
hagrp -offline service_group -sys sys_name
```

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

After the resync is complete, the devices in the secondary are P-VOL and the devices in the primary are S-VOL .The device state is PAIR at both the sites.

3 Bring the global service group online at the primary site. On a node in the primary site, run the following command:

```
hagrp -online service_group -sys sys_name
```

This again swaps the roles of P-VOL and S-VOL.

Chapter 4

Setting up fire drill

This chapter includes the following topics:

About fire drills

A fire drill procedure verifies the fault-readiness of a disaster recovery configuration. This procedure is done without stopping the application at the primary site and disrupting user access.

A fire drill is performed at the secondary site using a special service group for fire drills. The fire drill service group is identical to the application service group, but uses a fire drill resource in place of the replication agent resource. The fire drill service group uses a copy of the data that is used by the application service group.

In clusters employing Hitachi TrueCopy/Hewlett-Packard XP Continuous Access, the HTCSnap resource manages the replication relationship during a fire drill.

Bringing the fire drill service group online demonstrates the ability of the application service group to come online at the remote site when a failover occurs.

The HTCSnap agent supports fire drills for storage devices that are managed using Veritas Volume Manager, which is a component of Symantec Storage Foundation.

The agent supports fire drills in a Storage Foundation for Oracle RAC environment.

About the HTCSnap agent

The HTCSnap agent is the fire drill agent for Hitachi TrueCopy/Hewlett-Packard XP Continuous Access. The agent maintains the replication relationship between the source and target arrays when running a fire drill. Configure the HTCSnap resource in the fire drill service group, in place of the HTC resource.

HTCSnap agent functions

The HTCSnap agent performs the following functions:

online

Gold Configuration

- Suspends replication between the source and the target arrays.
- Takes a local snapshot of the target LUN.
- Resumes the replication between the arrays.
- Takes the fire drill service group online by mounting the replication target LUN.
- Creates a lock file to indicate that the resource is online.

Silver Configuration

- Suspends replication between the source and the target arrays.
- Takes a local snapshot of the target LUN.
- Takes the fire drill service group online by mounting the target LUN.
- Creates a lock file to indicate that the resource is online.

Bronze Configuration

- Splits replication between the source and the target arrays.
- Takes the fire drill service group online using the target array.
- Creates a lock file to indicate that the resource is online.

offline

Gold Configuration

- Destroys the snapshot by synchronizing data between the target array and the device on which snapshot was taken.
- Removes the lock file created by the online function.

Silver Configuration

- Resumes replication between the source and the target arrays.
- Synchronizes data between the target array and the device on which the snapshot was taken. Destroys the snapshot of the target array after the data is synchronized.

Bronze Configuration

- Resumes the replication between the source and the target arrays.
- Removes the lock file created by the Online operation.

monitor	Verifies the existence of the lock file to make sure the resource is online.
clean	Restores the state of the LUNs to their original state after a failed online function.

Resource type definition for the HTCSnap agent

Following is the resource type definition for the HTCSnap agent:

```
type HTCSnap (
    static keylist RegList = { MountSnapshot, UseSnapshot }
    static keylist SupportedActions = { clearvm }
    static str ArgList[] = { TargetResName, MountSnapshot,
    UseSnapshot, RequireSnapshot, ShadowInstance,
    DiskGroupSnapList, User, Domain, Password }
    static int OpenTimeout = 180
    str TargetResName
    int ShadowInstance
    int MountSnapshot
    int UseSnapshot
    int RequireSnapshot
    str DiskGroupSnapList
    str User
    str Domain
    str Password
    temp str Responsibility
    temp str FDFile
)
```

Attribute definitions for the HTCSnap agent

To customize the behavior of the HTCSnap agent, configure the following attributes:

ShadowInstance	The instance number of the ShadowInstance P-VOL group. The P-VOL group must include one of the following: ■ The same LUNs as in the TrueCopy S-VOL group (if taking snapshots of replicated data). ■ The same LUNs as in the VxVM disk group (if taking snapshots of non-replicated data). Type-dimension: integer-scalar

TargetResName	Name of the resource managing the LUNs that you want to take snapshot of. Set this attribute to the name of the HTC resource if you want to take a snapshot of replicated data. Set this attribute to the name of the DiskGroup resource if the data is not replicated. For example, in a typical database setup, you might replicate data files and redo logs, but you may choose to avoid replicating temporary tablespaces. The temporary tablespace must still exist at the DR site and may be part of its own disk group. Type-dimension: string-scalar
MountSnapshot	Specifies whether the resource uses the snapshot to bring the service group online. Set this attribute to 1. Type-Dimension: integer-scalar **Note:** Set this attribute to 1 only if UseSnapshot is set to 1.
UseSnapshot	Specifies whether the HTCSnap resource takes a local snapshot of the target array. Set this attribute to 1. Type-Dimension: integer-scalar See "About the Snapshot attributes" on page 52.
RequireSnapshot	Specifies whether the HTCSnap resource must take a snapshot before coming online. Set this attribute to 1 if you want the resource to come online only after it succeeds in taking a snapshot. Type-Dimension: integer-scalar **Note:** Set this attribute to 1 only if UseSnapshot is set to 1.
DiskGroupSnapList	This is an optional attribute that lists the original disk group names and the fire drill disk group names. Type-dimension: string-scalar

Responsibility	Do not modify. For internal use only. Used by the agent to keep track of resynchonizing snapshots. Type-Dimension: temporary string
FDFile	Do not modify. For internal use only. Used by the agent to store the absolute pathname to the file with the latest fire drill report on the local system. Type-Dimension: temporary string

About the Snapshot attributes

The UseSnapshot, MountSnapshot, and RequireSnapshot attributes define the fire drill configuration.

Table 4-1 lists the snapshot attribute values for fire drill configurations:

Table 4-1 Snapshot attribute values for fire drill configurations

Attribute	Gold	Silver	Bronze
MountSnapshot	1	0	0
UseSnapshot	1	1	0

Setting the RequireSnapshot attribute to 0 enables a Gold or Silver configuration to run in the Bronze mode if the snapshot operation fails.

Sample configuration for a fire drill service group

The sample configuration of a fire drill service group is identical to an application service group with a hardware replication resource. However, in a fire drill service group, the HTCSnap resource replaces the HTC resource.

You can configure a resource of type HTCSnap in the main.cf file as follows.

```
HTCSnap sqldg_fd {
    TargetResName = "HTC"
    ShadowInstance = 5
    UseSnapshot = 1
    RequireSnapshot = 0
    MountSnapshot = 1
    }
```

Additional considerations for running a fire drill

Follow these guidelines for fire drills in a Windows environment:

- The primary and secondary sites must be fully configured with TrueCopy/HP-XP-CA replication and the global cluster option. The configuration must follow the applicable instructions in the Symantec Storage Foundation HA for Windows documentation for configuring disaster recovery with TrueCopy/HP-XP-CA.
- The secondary system where you plan to run the fire drill must have access to the replicated volumes.
- Ensure that Hitachi RAID Manager / Command Control Interface (CCI) is installed.
- You must configure ShadowImage pairs (for Hitachi) before running the Fire Drill wizard.
- During a fire drill, Volume Manager commands like `vxassist rescan` can cause performance issues due to the number of Volume Manager objects like diskgroups, disks, and volumes. To avoid this, you must increase the timeout value of the agent for larger configurations.
  For more information, refer to *Symantec Cluster Server Release Notes.*

Before you configure the fire drill service group

Before you configure the fire drill service group, follow the steps below:

- Make sure the application service group is configured with a HTC resource.
- Make sure the infrastructure to take snapshots is properly configured. This process involves creating the Shadow Image pairs.
- If you plan to use Gold or Silver configuration, make sure ShadowImage for TrueCopy is installed and configured at the target array.
- For the Gold configuration, you must use Veritas Volume Manager to import and deport the storage.
- You can use the Silver configuration only with ShadowImage pairs that are created with the `-m noread` flag to the `paircreate` command. A fire drill uses the `-E` flag to split the pairs, which requires a 100% resynchronization. The Silver mode that preserves the snapshots as `noread` after a split.
- The name of the ShadowImage device group must be the same as the replicated device group for both replicated and non-replicated LUNs that are to be snapshot. The instance number may be different.

- Make sure the HORC instance managing the S-VOLs runs continuously; the agent does not start this instance.
- For non-replicated devices:
  - You must use Veritas Volume Manager.
    On HP-UX, you must use Veritas Volume Manager 5.0 MP1.
  - For Gold configuration to run without the Bronze mode, set the RequireSnapshot attribute to 1.

Configuring the fire drill service group

This section describes how to use the Fire Drill wizard to create the fire drill service group.

About the Fire Drill wizard

Symantec Storage Foundation High Availability for Windows (SFW HA) provides a Fire Drill Wizard to help you set up and run a fire drill on a disaster recovery environment. You launch the Fire Drill Wizard from the Solutions Configuration Center.

The Fire Drill Wizard tests the fault readiness of a disaster recovery configuration by mimicking a failover from the primary site to the secondary site. The wizard does this without stopping the application at the primary site and disrupting user access.

The Fire Drill Wizard supports conducting a fire drill for a disaster recovery site that uses Volume Replicator (VVR) or that uses Hitachi TrueCopy/Hewlett-Packard XP Continuous Access hardware replication.

Verifying a successful fire drill

Run the fire drill routine periodically to verify the application service group can fail over to the remote node.

To verify a successful fire drill

1. Bring the fire drill service group online on a node at the secondary site that does not have the application running.

   If the fire drill service group comes online, it action validates your disaster recovery configuration. The production service group can fail over to the secondary site in the event of an actual failure (disaster) at the primary site.

2. If the fire drill service group does not come online, review the VCS engine log for more information.

3. Take the fire drill offline after its functioning has been validated.

   Failing to take the fire drill offline could cause failures in your environment. For example, if the application service group fails over to the node hosting the fire drill service group, there would be resource conflicts, resulting in both service groups faulting.

Index

I

L

M

P

R

S

T

U