Veritas™ Cluster Server Agent for Hitachi TrueCopy Installation and Configuration Guide

Windows Server 2003, Windows Server 2008

5.1

April 2009

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: 5.1.0

Document version: 5.1.0.1

Legal Notice

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

http://www.symantec.com/business/support/assistance_care.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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

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

Asia-Pacific and Japan	contractsadmin@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:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security 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.
Educational Services	Educational 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

Select your country or language from the site index.

Introducing the Veritas agent for Hitachi TrueCopy

This chapter includes the following topics:

About the agent for Hitachi TrueCopy

The Veritas agent for Hitachi TrueCopy provides support for application failover and recovery. The agent provides this support in environments that use TrueCopy to replicate data between Hitachi arrays.

The agent monitors and manages the state of replicated Hitachi TrueCopy devices that are attached to VCS nodes. The agent ensures that the system that has the TrueCopy resource online also has safe and exclusive access to the configured devices.

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

The agent supports TrueCopy 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
Lightning	data, never, and async
Thunder	data and never

The Hitachi TrueCopy agent also supports Hitachi Universal Replicator for asynchronous replication on two sites.

Supported software and hardware

The Hitachi TrueCopy agent supports Storage Foundation and High Availability Solutions 5.1 for Windows and Veritas Cluster Server 5.1 for Windows.

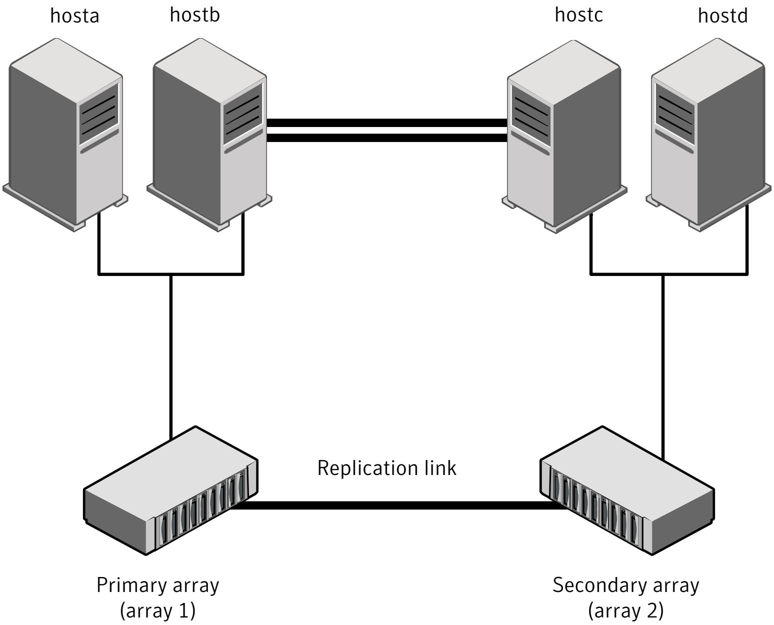
The agent for Hitachi TrueCopy provides support for the following:

- All versions of 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.
- Hewlett-Packard XP arrays with TrueCopy rebranded as Continuous Access
  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 setup in a VCS cluster

Figure 1-1 displays a typical cluster setup in a TrueCopy environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a TrueCopy 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 array that contains the TrueCopy 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 array that contains the TrueCopy 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 array.

Hitachi TrueCopy 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 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 agent's online function” on page 13.

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. 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	Resynchronizes the devices from the VCS command line after connectivity failures are detected and corrected. The agent supports the following actions: ■ pairdisplay—Displays information about all devices. ■ pairresync—Resynchronizes the S-VOLs. ■ 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 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 or SSUS, 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.

Installing and removing the agent for Hitachi TrueCopy

This chapter includes the following topics:

- Before you install the agent for TrueCopy
- Installing the agent for TrueCopy
- Removing the agent for TrueCopy

Before you install the agent for TrueCopy

Set up your cluster. For information about installing and configuring VCS, see the *Veritas Cluster Server Installation Guide*.

Set up replication and the required hardware infrastructure.

See "Typical Hitachi TrueCopy setup in a VCS cluster" on page 10.

Installing the agent for TrueCopy

If you did not install the TrueCopy when you installed Veritas Storage Foundation and High Availability for Windows, follow these instructions to install the agent.

You must install the Hitachi TrueCopy agent on each node in the cluster. In global cluster environments, install the agent on each node in each cluster. These instructions assume that you have already installed Storage Foundation and High Availability for Windows (SFW HA).

To install the agent forTrueCopy

1 Open the Windows Control Panel and click **Add or Remove Programs.**

2 Click the SFW HA Server Components entry and click **Change.**

3. On the installer screen, click **Add or Remove** and click **Next.**
4. In the Option Selection dialog box, select the agent and click **Next.**
5. The installer validates the system for installation.

   If a system is rejected, the Comments column displays the cause of rejection. Highlight the system to view detailed information about the failure in the Details box. Resolve the error, highlight the node in the selected systems list, and click **Validate Again.**

   After all the systems are accepted, click **Next.**
6. An informational message appears if you selected the DMP option. Review the information and click **OK** to continue.
7. Review the summary of your selections and click **Next.**
8. Click **Update** to start the installation.
9. The installer displays the status of installation. After the installation is complete, review the installation report and click **Next.**
10. Click **Finish.**

Removing the agent for TrueCopy

This section describes steps for uninstalling the agent. Do not attempt to remove the agent if service groups accessing the shared storage are online.

To remove the agent TrueCopy

1. Open the Windows Control Panel and click **Add or Remove Programs.**
2. Click the VSFW HA Server Components entry and click **Remove.**
3. Review the Welcome page and click **Next.**
4. In the Option Selection dialog box, select the TrueCopy agent and click **Next.**
5. The installer validates the system for uninstallation.

   If a system is rejected, the Comments column displays the cause of rejection. Highlight the system to view detailed information about the failure in the Details box. Resolve the error, highlight the node in the selected systems list, and click **Validate Again.**

   After all the systems are accepted, click **Next.**
6. Review the summary of your selections and click **Uninstall.**
7. The installer displays the status of uninstallation.

8 After the uninstallation is complete, review the report and click **Next.**

9 Click **Finish.**

Note: For Win IA64 and Win x64 architectures, you must manually delete the agent directory if it is not removed after the uninstallation.

Chapter 3

Configuring the agent for Hitachi TrueCopy

This chapter includes the following topics:

Configuration concepts for the Hitachi TrueCopy agent

Review the configuration concepts and failure scenarios for the agent.

Resource type definition for the Hitachi TrueCopy agent

The resource type definition defines the agent in VCS.

```
type HTC (
    static str ArgList[] = { BaseDir, GroupName, Instance}
        static int Numthreads = 1
        static keylist SupportedActions = {localtakeover, pairresync,
        pairresync-swaps, pairdisplay}
        NameRule = resource.Groupname
        str BaseDir = "C:\\HORCM\\etc"
        str GroupName
        int Instance
        int SplitTakeover = 1
int LinkMonitor = 0
)
```

Attribute definitions for the Hitachi TrueCopy agent

The descriptions of the agent attributes are as follows:

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: string-scalar

SplitTakeover

A flag that 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.

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, 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.

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

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.

The default value for this 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 a global cluster environment, if the agent at the P-VOL side detects the PSUE state locally, it 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.

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.

About the HTC configuration parameters

The TrueCopy agent uses RAID manager for Windows NT 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.

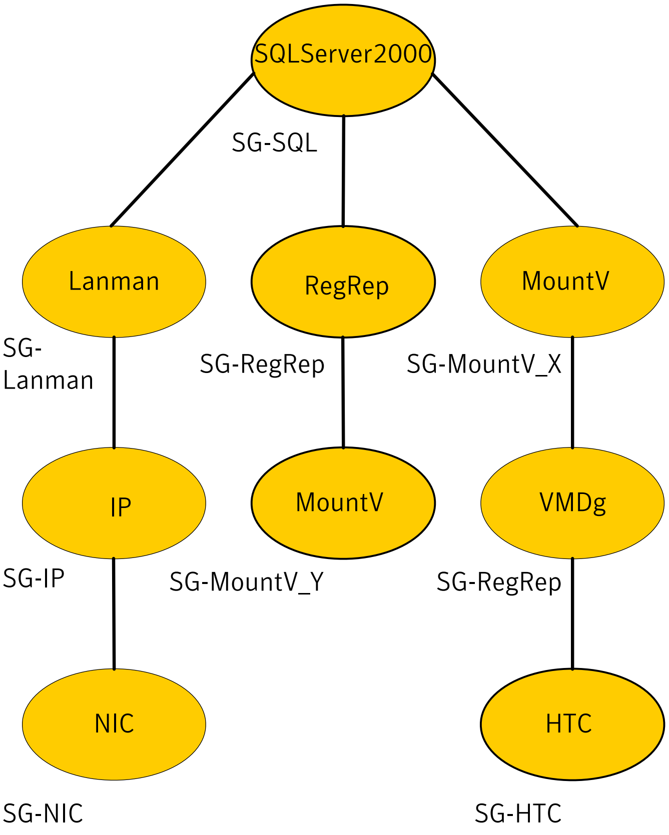
Update the HOTCM_INST section of the configuration file.

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.

Sample configuration for the Hitachi TrueCopy agent

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

Figure 3-1 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 TrueCopy

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 agent" on page 19.

- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical Hitachi TrueCopy setup in a VCS cluster" on page 10.
- Make sure that the cluster has an effective heartbeat mechanism in place.
  See "About cluster heartbeats" on page 24.
  See "About preventing split-brain" on page 25.
- Set up system zones in replicated data clusters.
  See "About configuring system zones in replicated data clusters" on page 24.
- 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 *Veritas 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.
    For more information, see the *Veritas Cluster Server Administrator's Guide*.

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 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 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

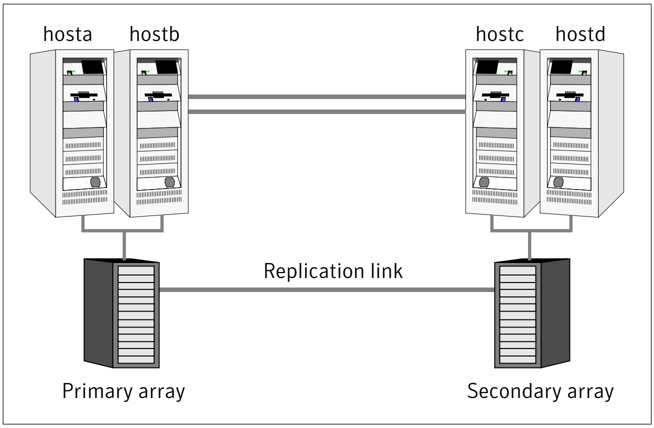
In a replicated data cluster, you can prevent unnecessary TrueCopy failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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

Figure 3-2 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 3-2 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 TrueCopy

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

- Converting their devices to TrueCopy devices
- Synchronizing the devices
- Adding the Hitachi TrueCopy agent to the service group

See *Veritas Cluster Server Administrator's Guide* for more information.

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

See "Sample configuration for the Hitachi TrueCopy agent" on page 22.

Performing a manual Volume Manager rescan

If you configure Volume Manager diskgroups on the disks that are replicated, the diskgroups do not come online the first time after failover on the secondary node. You must perform a manual Volume Manager rescan on all the secondary nodes after setting up replication and other dependent resources, in order to bring the diskgroups online. This rescans all Volume Manager objects and must be performed only once after which the failover works uninterrupted.

To perform a manual Volume Manager rescan

1. Bring all the resources in the service group offline on the primary node.
2. Bring the TrueCopy resource online on all the secondary nodes.
3. Run VM rescan on all the secondary nodes.
4. Bring all the resources (e.g. DiskGroup, Mount, and Application) online on the secondary nodes.
5. Fail over the service group to the primary node.

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

   Program Files\Veritas\Cluster Server\conf\config\TrueCopyTypes.cf
3. Click **Import**.
4. Save the configuration.
5. Add a resource of type TrueCopy 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 TrueCopy resource.
7. If the service group is not configured as a global group, configure the service group using the Global Group Configuration Wizard.

   See the *Veritas Cluster Server Administartor's Guide* for more information.
8. Change the ClusterFailOverPolicy 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.

Note: The Disaster Recovery wizard configures the required settings for the TrueCopy resource in the VCS application service group. Optional settings are left in the default state. The wizard creates a complete disaster recovery setup using the TrueCopy replication and validates the replication setup. For information on using the Disaster Recovery wizard, see the Solutions guides chapters on 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 (TrueCopy) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

   ```
   Program Files\Veritas\Cluster Server\conf\config\TrueCopyTypes.cf.
   ```

3. Click **Import**.
4. Save the configuration.
5. In each service group that uses replicated data, add a resource of type TrueCopy at the top of the service group.

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

6. Configure the attributes of the TrueCopy resource. Note that some attributes must be localized to reflect values for the hosts that are attached to different arrays.
7. Set the SystemZones attribute for the service group to reflect which hosts are attached to the same array.

4

Managing and testing clustering support for Hitachi TrueCopy

This chapter includes the following topics:

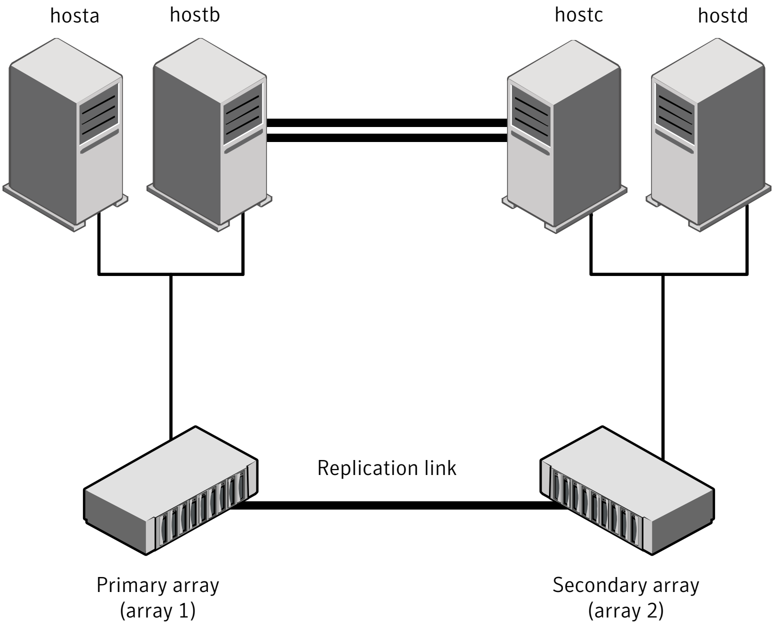
Typical test setup for the Hitachi TrueCopy agent

A typical test environment includes the following characteristics:

- Two hosts (hosta and hostb) are attached to the P-VOL Hitachi TrueCopyarray.
- Two hosts (hostc and hostd) are attached to the S-VOL Hitachi TrueCopy array.
- The application runs on hosta and devices in the local array are P-VOLs in the PAIR state.
- A replicated data cluster has two dedicated heartbeat links.
  A global cluster has one network heartbeat.

Figure 4-1 depicts a typical test environment.

Figure 4-1 Typical test setup



Testing service group migration

Verify the service group can migrate to different hosts in the cluster and across clusters.

To perform the service group migration test

1 In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group.

Migrate the service group to a host that is attached to the same array.

2 Click **Switch To**, and click the system that is attached to the same array (hostb) from the menu.

The service group comes online on hostb and local volumes remain in the P-VOL/PAIR state.

3 In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group.

Migrate the service group to a host that is attached to a different array.

4 Click **Switch To**, and click the system that is attached to another array (hostc) from the menu.

The service group comes online on hostc and volumes there transition to the P-VOL/PAIR state, changing the original P-VOLs to S-VOLs.

5 In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group.

Migrate the service group back to its original host.

6 Click **Switch To**, and click the system on which the group was initially online (hosta).

The group comes online on hosta. The devices return to the original state in step 1.

Testing host failure

In this scenario, the host where the application runs is lost. Eventually all the hosts in the system zone or cluster are lost.

To perform the host failure test

1 Halt or shut down the host where the application runs (hosta).

The service group fails over to hostb and devices are in the P-VOL/PAIR state.

2 Halt or shut down hostb.

In a replicated data cluster, the group fails over to hostc or hostd depending on the FailOverPolicy attribute in the cluster.

In a global cluster, a cluster down alert appears and gives you the opportunity to fail over the service group manually.

The devices on the target array remain S-VOLs. They remain S-VOLs because they cannot communicate with the original primary’s RAID manager, but they transition to the writable SSWS status. The failover can take some time as the RAID manager connection times out.

3 Reboot the two hosts that were shut down. A swap resynchronization is required to demote the original P-VOLs:

```
hares -actionHTCRes pairresync-swaps -sys system
```

4 Switch the service group to its original host when VCS starts.

Do the following:

- In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group.

- Click **Switch To**, and click the system on which the service group was initially online (hosta).

  The service group comes online on hosta and devices swap roles again.

Performing a disaster test

Test how robust your cluster is in case of a disaster.

To perform a disaster test

1. Shut down all hosts on the source side and shut down the source array.

   If you cannot shut down the primary array, disconnect the replication link between the two arrays and simultaneously shut down the hosts. This action mimics a disaster scenario to the secondary side.

2. In a replicated data cluster, the service group fails over to hostc or hostd in the following conditions:

   - All devices were originally in the PAIR state.
   - No synchronization was in progress at the time of disaster.

3. In a global cluster, the administrator is notified of the failure. The administrator can then initiate the failover.

Performing the failback test

You can set up your cluster for a failback test.

The failback test verifies the application can fail back to its original host after a failover to a remote site.

To perform a failback test

1. Reconnect the replication link and reboot the original P-VOL hosts.
2. Take the service group offline.
3. Write-disable both sides.
4. Manually resynchronize the device.
5. After the resynchronization is complete, migrate the application back to the original primary side.
6. C:\>hagrp -online aglagrp -sys hosta

   The devices swap roles again and the environment state will be the same as when the test began.

Failure scenarios for Hitachi TrueCopy

Review the failure scenarios and agent behavior in response to failure.

Site disaster

In a total site failure, all hosts and the array are completely disabled, either temporarily or permanently.

In a replicated data cluster, site failure is detected the same way as a total host failure, that is, the loss of all LLT heartbeats.

In a global cluster environment, VCS detects the failure by the loss of the ICMP heartbeat between the clusters.

If a failover occurs, the online entry point of the TrueCopy agent runs the `horctakeover` command. The RAID manager waits for the timeout in trying to contact its peer RAID manager daemon before taking over the disks. This wait can cause delay in the failover. This timeout is defined in the device group's instance's configuration file. Make sure the value of the OnlineTimeout entry point of the HTC type is greater than the RAID manager timeout.

The online entry point detects whether any synchronization was in progress when the source array was lost. Since the target devices are inconsistent until the synchronization completes, the agent does not write-enable the devices, but it times out and faults. You must restore consistent data from a snapshot or tape backup.

All host or all application failure

Even if both arrays are operational, the service group fails over in the following conditions:

- All hosts on the P-VOL side side are disabled.
- The application cannot start successfully on any P-VOL host.

In replicated data cluster environments, the failover can be automatic, whereas in global cluster environments failover requires user confirmation by default.

In both replicated data cluster and global cluster environments, multiple service groups can fail over in parallel.

TrueCopy does not provide any serialization restrictions on simultaneous device group failover. However, the `horctakeover` command makes an attempt to contact the RAID manager on the original P-VOL when performing a failover. In such a case, if the RAID manager is inaccessible, failover is delayed until the surviving

RAID manager's connect timeout expires. This timeout is defined in the configuration file for the particular instance.

Replication link failure

Hitachi arrays send an alert in the following situations:

- When the array detects a replication link failure
- When any P-VOLs, on which data has been written, transition from the PAIR state to the PSUE state

In fence levels never and async, a replication link failure does not compromise the application's ability to write to its local devices. The arrays start tracking changed regions on disk in preparation for resynchronization when the link is restored.

The devices do not automatically resynchronize when the link is restored, nor do they change state when the restoration is detected. An administrator can resynchronize the devices, either from the command line or by running a configured action using the agent's action entry point.

Table 4-1 shows the situations that require administrative action after you repair a link failure.

These actions depend on the fence level and any events that occurred during the failure.

Table 4-1 Replication link 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.
Application faults due to I/O errors.	data	Run the `localtakeover` action to write-enable the local devices. Clear faults and restart service group.

Split-brain in a TrueCopy environment

When split-brain occurs in a replicated database cluster, VCS assumes a total disaster because the P-VOL side hosts and array are unreachable. VCS attempts to start the application on the secondary site. Once the heartbeats are restored, VCS stops the applications on one side and restarts the VCS engine (HAD). This action eliminates concurrency violation of the same group being online at two places simultaneously.

Administrators must resynchronize the volumes manually using the `pairresync` commands.

In a global cluster, you can confirm the failure before failing over the service groups. You can check with the site administrator to identify the cause of the failure. If a fail over mistakenly occurs, the situation is similar to the replicated data cluster case. However, when the heartbeat is restored, VCS does not stop HAD at either site. VCS forces you to choose which group to take offline. You must resynchronize the data manually.