Cluster Server Agent for HPE 3PAR Remote Copy Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

8.0.2

VERITAS™

Veritas InfoScale™ Availability Agents

Last updated: 2023-06-30

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party (“Third Party Programs”). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third-party legal notices document accompanying this Veritas product or available at:

https://www.veritas.com/about/legal/license-agreements

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

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

infoscaledocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 Introducing the agent for HPE 3PAR Remote Copy 6

About the agent for HPE 3PAR Remote Copy 6
Supported software 7
Typical HPE 3PAR Remote Copy setup in a VCS cluster 7
HPE 3PAR Remote Copy agent functions 8
About the agent's online function 11

Chapter 2 Installing and removing the agent for HPE 3PAR Remote Copy 13

Before you install the agent for HPE 3PAR Remote Copy 13
Installing the agent for HPE 3PAR Remote Copy 13
Installing the agent IPS package on Oracle Solaris 11 systems 14
Installing agent packages on Solaris brand non-global zones 15
Upgrading the agent for HPE 3PAR Remote Copy 16
Removing the agent for HPE 3PAR Remote Copy 17

Chapter 3 Configuring the agent 18

Configuration concepts for the 3PAR Remote Copy agent 18
Resource type definition for the 3PAR Remote Copy agent 18
Attribute definitions for the 3PAR Remote Copy agent 19
Sample configuration for the 3PAR Remote Copy agent 22
Before you configure the agent for HPE 3PAR Remote Copy 22
About cluster heartbeats 22
To set up a passwordless SSH 23

Chapter 4 Managing and testing clustering support for HPE 3PAR Remote Copy 24

Typical test setup for the HPE 3PAR Remote Copy agent 25
How VCS recovers from various disasters in an HA/DR setup with HPE 3PAR Remote Copy 26

Failure scenarios in global clusters and replicated data clusters 26
Testing global service group migration between global clusters 30
Testing service group migration between replicated data clusters 32
Testing all hosts failure in a global cluster 33
Testing all hosts failure in a replicated data cluster 34

Chapter 1

Introducing the agent for HPE 3PAR Remote Copy

This chapter includes the following topics:

- About the agent for HPE 3PAR Remote Copy
- Supported software
- Typical HPE 3PAR Remote Copy setup in a VCS cluster
- HPE 3PAR Remote Copy agent functions

About the agent for HPE 3PAR Remote Copy

The Cluster Server agent for HPE 3PAR Remote Copy provides support for application failover and recovery. The agent provides this support in environments that use 3PAR Remote Copy functionality to copy a Remote Copy group from one InServ Storage Server to another.

The agent provides this support for applications that are protected by the HPE 3PAR Remote Copy replication feature in VCS global clusters and replicated data clusters.

The agent also supports HPE 3PAR Primera Storage arrays on Linux.

The agent supports the synchronous and periodic modes of replication with the mirror_config policy.

Note: When the mode of replication is periodic, you must configure the synchronization period for the volume group before using the agent. There is no default synchronization period.

Supported software

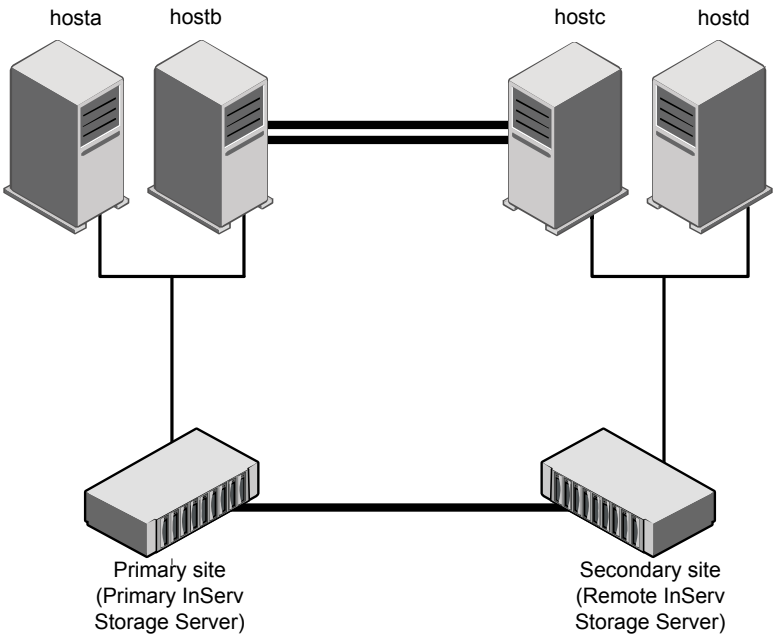
For information on the software versions that the Infoscale (Infoscale Availability) agent for 3PAR Remote Copy supports, see the Veritas Services and Operations Readiness Tools (SORT) site:

https://sort.veritas.com/agents

Typical HPE 3PAR Remote Copy setup in a VCS cluster

Figure 1-1 displays a typical cluster setup in a 3PAR Remote Copy environment.

Figure 1-1 Typical clustering setup for the agent



VCS clusters that use 3PAR Remote Copy for copying Remote Copy groups from one InServ Storage Server to another, use the following hardware infrastructure:

- The Primary InServ Storage Server, also known as the primary server, has the primary volume group. A volume group has one or more Remote Copy volumes that are logically related and for which there is a cross-volume ordering of writes. The primary volume group contains the set of volumes to be copied.

- The Remote InServ Storage Server, also known as the secondary or backup server, has the secondary volume group. The secondary volume group contains the volumes that are copied from the primary server.
- The Remote InServ Storage Server must be at a significant distance to survive a disaster that may occur at the primary site.

HPE 3PAR Remote Copy agent functions

The Cluster Server agent for 3PAR Remote Copy monitors and manages the state of copied volumes that are attached to VCS nodes.

The agent performs the following functions:

online	Makes the Remote Copy group writable for the application. If one or more volumes are in the read only (RO) state, the agent runs a `setrcopygroup` command to enable read-write access to the volumes. See "About the agent's online function" on page 11. If the state of all local devices is read-write enabled (RW), the agent creates a lock file on the local host. The lock file indicates that the resource is online.
offline	Removes the lock file on the local host. The agent does not run any Remote Copy commands because taking the resource offline is not indicative of the intention to give up the volumes.
monitor	Verifies that the lock file exists. If the lock file exists, the monitor function reports the status of the resource as online. If the lock file does not exist, the monitor function reports the status of the resource as offline.

open	Removes the lock file on the host where the function is called. This operation prevents potential concurrency violation if the service group fails over to another node. Note that the agent does not remove the lock file if the agent was started after running the following command: `hastop <-all | -local> -force`
clean	Determines if it is safe to fault the resource if the online function fails or times out.
info	Populates the value of the data transfer role and the state of the Remote Group in the ResourceInfo attribute. For example, the state could be Started or Stopped.
action/recover	This action function is meant to run when the failed primary comes back online and is used for groups on which the failover operation has already been run. This action function changes the matching primary volume groups on the backup system to secondary volume groups and then starts and synchronizes the specified group. This action function executes the `setrcopygroups –recover` *`groupname`* command.
action/restore	This action function is used on groups on which the recover operation has already been run. This action function returns specified groups to their natural direction and starts them. This action function executes the `setrcopygroups restore` *`groupname`* command.

action/revert	This action function is meant to run when failed primary comes back online and is used for groups on which the failover operation has already been run. Unlike the action/recover function, this action function discards the data written on the failover group and synchronizes the group to the point at which failover took place. This action function executes the `setrcopygroup reverse -current` *`groupname`* command. **Note:** The action/revert operation results in the loss of any data that is written to the primary volumes from the time that their groups were stopped.
action/startrcopygroup	Starts remote copy for the specified group. The agent invokes the `startrcopygroup` command to 3PAR InServe storage server.
action/PreSwitch	This action function ensures that the remote site cluster can come online during a planned failover within a GCO configuration. The VCS engine on the remote cluster invokes the PreSwitch action on all the resources of the remote site 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 *Cluster Server Administrator's Guide*.

action/syncrcopy	Synchronizes the specified remote copy group. The agent invokes the `syncrcopy` command to the 3PAR InServe storage server.
action/getremoteinfo	Prints the group role, status, replication mode, and synchronization status of the Remote Copy group from the host where it is executed.
action/GetCurrentRPO	Fetches the current point in time RPO. Invoke this action function on the DR system where the ComputeDRSLA attribute is set to 1. The RPO is computed in seconds. **Note:** The agent does not store the computed RPO; make a note of the RPO for future reference.
attr_changed	Monitors the changes in the attribute GroupName. If the group name is changed, the instructions are logged in for the changes to be effective. Also monitors the ComputeDRSLA attribute. Depending on the new value of the ComputeDRSLA attribute, this function either initiates or terminates the process of computing the RPO.

Note: The agent uses the following internal action functions to compute the RPO: StartRPOComputation, StopRPOComputation, StartWriter, ReportRPOData.

About the agent's online function

The agent checks the role of the volume group that is specified in the Group Information.

If the role is Primary or Primary-rev, the agent comes online directly.

If the role is Secondary or Secondary-Rev, the agent validates that the Sync status is not New or NotSynced. After validating the Sync status, the agent checks the target status.

If the target status is Ready and Sync status is Synced, the agent attempts to switch the roles in the following manner:

- If the value of the ForceSync attribute is 0, the agent does not run the `syncrcopy` command to synchronize the logical virtual volumes of a group.
- If the value of the ForceSync attribute is 1, the agent runs the `syncrcopy` command to synchronize the logical virtual volumes of a group.

Note: The ForceSync attribute is applicable only to the periodic mode of replication.

- If the value of the SwapRole attribute is 0, the agent retains the natural direction of replication as is and switches the role.
- If the value of the SwapRole attribute is 1, the agent reverses the natural direction of replication to switch the roles.

If the target status is Failed and Sync status is Stopped or Stale, the agent attempts to change the roles in the following manner:

- If the value of the AutoTakeover attribute is 0, the agent does not take any action.
- If the value of the AutoTakeover attribute is 1, the agent executes the failover command.

After the switch role or change role commands are successfully executed, the agent brings the RemoteCopy resource online.

Chapter 2

Installing and removing the agent for HPE 3PAR Remote Copy

This chapter includes the following topics:

- Before you install the agent for HPE 3PAR Remote Copy
- Installing the agent for HPE 3PAR Remote Copy
- Upgrading the agent for HPE 3PAR Remote Copy
- Removing the agent for HPE 3PAR Remote Copy

Before you install the agent for HPE 3PAR Remote Copy

Before you install the VCS agent for HPE 3PAR Remote Copy, ensure that you install and configure VCS on all nodes in the cluster.

Set up replication and the required hardware infrastructure.

For information about setting up Oracle RAC environment, refer to the *Storage Foundation for Oracle RAC Configuration and Upgrade Guide*.

See “Typical HPE 3PAR Remote Copy setup in a VCS cluster” on page 7.

Installing the agent for HPE 3PAR Remote Copy

You must install the HPE 3PAR Remote Copy agent on each node in the cluster. In global cluster environments, install the agent on each node in each cluster.

To install the agent in a VCS environment

1. Download the Agent Pack from the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.
2. Log in as a superuser.
3. Install the package.

AIX	`# installp -ac -d VRTSvcsrc.rte.bff VRTSvcsrc.rte`
HP-UX (IA/PA)	`# swinstall -s 'pwd' VRTSvcsrc`
Linux	`# rpm -ihv VRTSvcsrc-AgentVersion-Linux_GENERIC.noarch.rpm`
Solaris	`# pkgadd -d . VRTSvcsrc`

Note: On successful installation of the agent, if VCS is running, the agent types definition is automatically added to the VCS configuration.

Installing the agent IPS package on Oracle Solaris 11 systems

To install the agent IPS package on an Oracle Solaris 11 system

1. Copy the `VRTSvcsrc.p5p` package from the pkgs directory to the system in the `/tmp/install` directory.
2. Disable the publishers that are not reachable as package install may fail if any of the already added repositories are unreachable.

   ```
   # pkg set-publisher --disable <publisher name>
   ```

   where the publisher name is obtained using the pkg publisher command.
3. Add a file-based repository in the system.

   ```
   # pkg set-publisher -g /tmp/install/VRTSvcsrc.p5p Symantec
   ```
4. Install the package.

   ```
   # pkg install --accept VRTSvcsrc
   ```

5 Remove the publisher from the system.

```
# pkg unset-publisher Symantec
```

6 Enable the publishers that were disabled earlier.

```
# pkg set-publisher --enable <publisher name>
```

Installing agent packages on Solaris brand non-global zones

With Oracle Solaris 11, you must install the agent package inside non-global zones. The native non-global zones are known as Solaris brand zones.

To install the agent package on Solaris brand non-global zones

1 Ensure that the SMF service svc:/application/pkg/system-repository:default and svc:/application/pkg/zones-proxyd:default are online on the global zone.

```
# svcs svc:/application/pkg/system-repository:default

# svcs svc:/application/pkg/zones-proxyd:default
```

2 Log on to the non-global zone as a superuser.

3 Ensure that the SMF service svc:/application/pkg/zones-proxy-client:default is online inside non-global zone:

```
# svcs svc:/application/pkg/zones-proxy-client:default
```

4 Copy the VRTSvcsrc.p5p package from the pkgs directory to the non-global zone (for example, to the /tmp/install directory).

5 Disable the publishers that are not reachable, as package install may fail if any of the already added repositories are unreachable.

```
# pkg set-publisher --disable <publisher name>
```

6 Add a file-based repository in the non-global zone.

```
# pkg set-publisher -g/tmp/install/VRTSvcsrc.p5p Symantec
```

7 Install the package.

```
# pkg install --accept VRTSvcsrc
```

8 Remove the publisher on the non-global zone.

```
# pkg unset-publisher Symantec
```

9 Clear the state of the SMF service, as setting the file-based repository causes the SMF service svc:/application/pkg/system-repository:default to go into the maintenance state.

```
# svcadm clear svc:/application/pkg/system-repository:default
```

10 Enable the publishers that were disabled earlier.

```
# pkg set-publisher --enable <publisher>
```

Note: Perform steps 2 through 10 on each non-global zone.

Upgrading the agent for HPE 3PAR Remote Copy

You must upgrade the agent on each node in the cluster.

To upgrade the agent software

1 Save the VCS configuration.

```
# haconf -dump -makero
```

2 Stop the agent if it is running.

```
# haagent -stop RemoteCopy -force -sys system
```

3 Verify the status of the agent and ensure that it is not running.

```
# haagent -display RemoteCopy | grep Running
```

The command output resembles the following:

```
RemoteCopy Running No
```

4 Upgrade the agent.

- For Linux, run the following commands:

```
# rpm -Uvh VRTSvcsrc-AgentVersion-Linux_GENERIC.noarch.rpm
```

- For AIX, HP-UX (IA/PA), and Solaris, perform the following steps:
  - Remove the previous version of the agent from the node.
    See "Removing the agent for HPE 3PAR Remote Copy" on page 17.
  - Delete the file `/etc/VRTSvcs/conf/config/RemoteCopyTypes.cf`.
  - Install the latest version of the agent.

See "Installing the agent for HPE 3PAR Remote Copy" on page 13.

- Copy the file `RemoteCopyTypes.cf` from the `/etc/VRTSvcs/conf/` to the `/etc/VRTSvcs/conf/config` directory.
- Repeat these four substeps that are mentioned earlier on each node.
- From a node in the cluster, edit the `/etc/VRTSvcs/conf/config/main.cf` configuration file. Configure the new attributes, if applicable.
- Verify the configuration by running the following command:

  ```
  # hacf -verify config
  ```

5 Start the agent.

```
# haagent -start RemoteCopy -sys system
```

6 Verify the status of the agent and ensure that it is running.

```
# haagent -display RemoteCopy | grep Running
```

The command output resembles the following:

```
RemoteCopy Running Yes
```

Removing the agent for HPE 3PAR Remote Copy

Before you attempt to remove the agent, make sure the application service group is not online.

You must remove the 3PAR Remote Copy agent from each node in the cluster.

To uninstall the agent in a VCS environment

- To remove the agent, type the following command on each node. Answer prompts accordingly:

AIX	`# installp -u VRTSvcsrc.rte`
HP-UX	`# swremove VRTSvcsrc`
Linux	`# rpm -e VRTSvcsrc`
Solaris	`# pkgrm VRTSvcsrc`

Chapter 3

Configuring the agent

This chapter includes the following topics:

- Configuration concepts for the 3PAR Remote Copy agent
- Before you configure the agent for HPE 3PAR Remote Copy
- To set up a passwordless SSH

Configuration concepts for the 3PAR Remote Copy agent

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

Resource type definition for the 3PAR Remote Copy agent

```
type RemoteCopy (
    static keylist RegList = { ComputeDRSLA }
    static keylist SupportedActions = { PreSwitch, recover,
      revert, restore, startrcopygroup, syncrcopy, ReportRPOData,
      StartWriter, GetCurrentRPO, StartRPOComputation,
      StopRPOComputation, getremoteinfo }
    static str ArgList[] = { StorageServer, UserName, GroupName,
      SSHBinary, SSHPathToIDFile, AutoTakeover, SwapRoles,
      ForceSync, ComputeDRSLA, CLIBinary, PasswordFile }
    str StorageServer
    str UserName
    str GroupName
    str CLIBinary
    str PasswordFile
    str SSHBinary = "/usr/bin/ssh"
    str SSHPathToIDFile
```

```
    int AutoTakeover = 0
    int SwapRoles = 0
    int ForceSync = 0
    int ComputeDRSLA = 0
    temp str VCSResLock
    temp str CurrentRPO
)
```

Attribute definitions for the 3PAR Remote Copy agent

Table 3-1 describes the required attributes for the HPE 3PAR Remote Copy agent.

Table 3-1 Required attributes

Attribute	Description
StorageServer	Specifies the name or the IP address of the 3PAR InServ Storage Server at the current site. Type-dimension: string-scalar Example: 10.182.200.100 Example: c1062-inserv-f400
UserName	Specifies the user name that is used to connect to the 3PAR InServ Storage Server at the current site. Type-dimension: string-scalar Example: admin
Password	Specifies the HPE 3PAR password file that is used to connect to the 3PAR InServ Storage Server at the current site. Type-dimension: string-scalar Example: `/3par/passfile`
CLIBinary	Contains the absolute path to the HPE 3PAR CLI binary. Type-dimension: string-scalar Example: `/opt/3PAR/inform_cli_3.2.1/cli`
SSHBinary	Contains the absolute path to the SSH binary. SSH is the mode of communication with the 3PAR InServ Storage Server. Default: `/usr/bin/ssh` Type-dimension: string-scalar

Table 3-1 Required attributes *(continued)*

Attribute	Description
SSHPathToIDFile	Contains the absolute path to the identity file that is used for authenticating the host with the 3PAR InServ Storage Server. The corresponding public key must be added on the storage server so that it can correctly authenticate the host. Type-dimension: string-scalar Example: `/keys/rpa_rsa`
GroupName	Specifies the group name in which Remote Copy is configured on the Storage Server. Type-dimension: string-scalar Example: Oracle_Grp
AutoTakeover	Indicates if the agent should enable read/write access to the local group in the replication relationship when the Group is in an inactive state (Stopped). If it is set to 0, the agent will not enable read/write access when the replication is in an inactive state. Type-dimension: integer-scalar Default: 0
SwapRoles	Specifies if the roles of the Remote Copy group must be swapped at the time of failover. If it is set to 1, the primary group is set to Secondary and vice-versa. If it is set to 0, the roles remain the same. Roles are swapped only when the status of the target is Ready. Type-dimension: integer-scalar Default: 0
ForceSync	Determines if Remote Copy groups must be synchronized before failover. If the value of this attribute is set to 1, groups are forced to synchronize before failover. This attribute is applicable only to the periodic mode of replication. Type-dimension: integer-scalar Default: 0

Note: Communication to the HPE 3PAR InServ Storage Server can occur either through CLI or SSH. For SSH mode of communication, ensure that SSHBinary and SSHPathToIDFile attibutes are configured. For CLI mode of communication, ensure that CLIBinary and Password attributes are configured.

Table 3-2 describes the optional attributes for the HPE 3PAR Remote Copy agent.

Table 3-2 Optional attributes

Attribute	Description
ComputeDRSLA	Used to enable or disable Recovery Point Objective (RPO) computation. Set this attribute on any one node in the disaster recovery (DR) cluster. Setting this attribute to 1 starts the RPO computation process. Setting this attribute to 2 starts the RPO computation process and stores the RPO value in the CurrentRPO attribute. Ensure that you reset this attribute to 0 after you use the GetCurrentRPO action function to check the RPO. Type-dimension: integer-scalar Default: 0

Table 3-3 describes the internal attributes for the HPE 3PAR Remote Copy agent.

Note: Do not modify internal attributes.

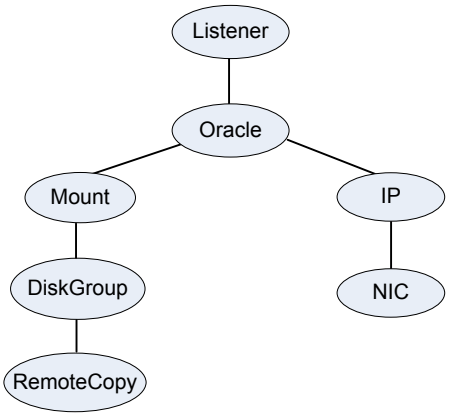
Table 3-3 Internal attributes

Attribute	Description
Tagging	Used for maintaining the process of computing RPO. Type-dimension: temporary boolean
VCSResLock	Used to ensure the serialized management in case of a parallel application. Type-dimension: temporary string
CurrentRPO	Used to store the RPO value. Type-dimension: temporary string

Sample configuration for the 3PAR Remote Copy agent

Figure 3-1 shows the dependency graph for a VCS service group with a resource of type RemoteCopy.

Figure 3-1 Sample configuration for the 3PAR Remote Copy agent



Before you configure the agent for HPE 3PAR Remote Copy

Before you configure the agent, review the following information:

- Set up the passwordless ssh from all VCS hosts to the 3PAR InServ storage server.
  See "To set up a passwordless SSH" on page 23.
- Verify that you have installed the agent on all the cluster nodes.
- Verify the hardware setup for the agent.
  See "Typical HPE 3PAR Remote Copy setup in a VCS cluster" on page 7.
- Make sure that the cluster has an effective heartbeat mechanism in place.
  See "About cluster heartbeats" on page 22.

About cluster heartbeats

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.

To minimize the chances of split-brain, use the steward process.

To set up a passwordless SSH

To generate SSH keys on a VCS node and setup passwordless ssh to the 3PAR InForm Storage Server perform the following steps:

1. Log on to host (VCS node).
2. Generate public and private RSA keys using ssh-keygen with no passphrase. For example:

```
bash-3.00# ssh-keygen -b 1024 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (//.ssh/id_rsa): test_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in test_rsa.
Your public key has been saved in test_rsa.pub.
The key fingerprint is:
05:c1:ce:d0:f7:a1:9f:d1:33:20:bf:c2:9b:35:c8:43 root@thor393
```

3. Copy the above-generated public key and add it on the 3PAR InForm Storage Server using the `setsshkey -add` command.
4. To cache the Storage Server key on to the host for further use, run the following command from the host

```
#/usr/bin/ssh -i <path to RSA private key file> -l
<Storage server user name> <IP address of the Storage server >
<dummy_remotecopy_command>
```

   For example:`# /usr/bin/ssh -i /test_rsa -l 3paradm 10.182.1.29 showversion`

   A message appears, asking you to cache the host key with that of the Storage Server.
5. Type **Yes** and press **Enter**.
6. Repeat the above steps on each VCS node where the service group contains the Remote Copy resource.

Chapter 4

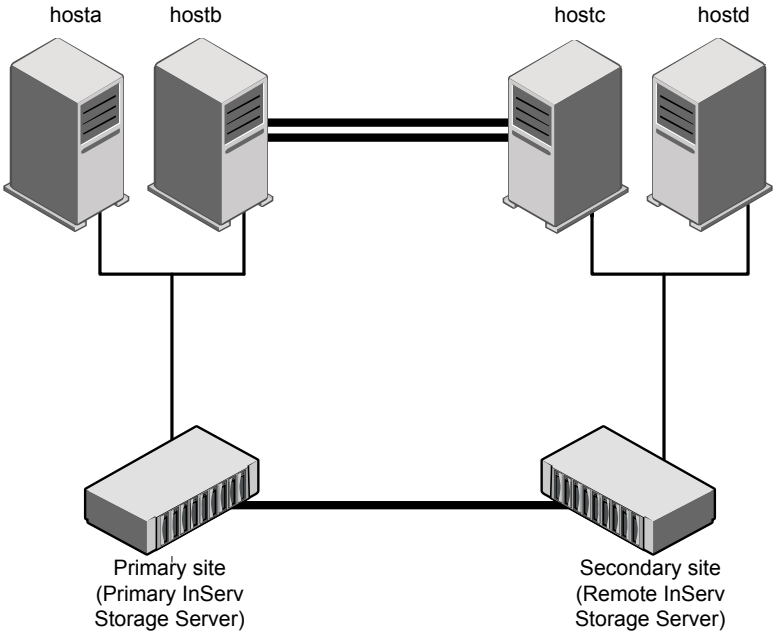
Managing and testing clustering support for HPE 3PAR Remote Copy

This chapter includes the following topics:

- Typical test setup for the HPE 3PAR Remote Copy agent
- How VCS recovers from various disasters in an HA/DR setup with HPE 3PAR Remote Copy
- Testing global service group migration between global clusters
- Testing service group migration between replicated data clusters
- Testing all hosts failure in a global cluster
- Testing all hosts failure in a replicated data cluster

Typical test setup for the HPE 3PAR Remote Copy agent

Figure 4-1 Typical test setup



A typical test environment includes the following characteristics:

- A primary site, an HPE 3PAR RemoteCopy cluster, is attached to the primary storage and the primary application hosts.
- A secondary site, an HPE 3PAR RemoteCopy cluster, is attached to the secondary storage and the secondary application hosts.
- Remote replication is established between the InServ storage servers at the primary and secondary sites.
- Two hosts (for example, Host A and Host B) are attached to the primary site HPE 3PAR InServ storage server.
- Two hosts (for example, Host C and Host D) are attached to the secondary site HPE 3PAR InServ storage server.
- At the primary site, passwordless SSH configuration is established on the hosts (Host A and Host B) and the primary site HPE 3PAR InServ storage server so

that the hosts can communicate by SSH with the primary site HPE 3PAR InServ storage server.

- Similarly, at the secondary site, passwordless SSH is established on the hosts (Host C and Host D) and the secondary site HPE 3PAR InServ storage server so that the hosts can communicate by SSH with the secondary site HPE 3PAR InServ storage server.
- The application runs on Host A, which is connected to the primary site HPE 3PAR InServ storage server.

How VCS recovers from various disasters in an HA/DR setup with HPE 3PAR Remote Copy

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

Global clusters (GCO configuration)	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 HPE 3PAR Remote Copy ensures safe and exclusive access to the configured HPE 3PAR Remote Copy devices.
Replicated data clusters (RDC configuration)	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 HPE 3PAR Remote Copy ensures safe and exclusive access to the configured HPE 3PAR Remote Copy devices.

Failure scenarios in global clusters and replicated data clusters

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

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

Table 4-1 Failure scenarios in global cluster and replicated data cluster configurations with the Cluster Server agent for HPE 3PAR Remote Copy

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 Write enables the devices at the secondary site.
	■ If the value of the SwapRoles attribute of the resource is 1, the agent changes the role of the secondary site to Primary and the role of the original primary site to Secondary.
	■ If the value of the SwapRoles attribute of the resource is 0, the agent changes the role of the secondary site to Primary-Rev and the role of the original primary to Secondary-Rev.

Table 4-1 Failure scenarios in global cluster and replicated data cluster configurations with the Cluster Server agent for HPE 3PAR Remote Copy *(continued)*

Failure	Description and VCS response

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 write enables the devices at the secondary site.
	■ Depending on the value of the SwapRoles attribute of the resource, the agent does the following:
	  ■ If the value of the SwapRoles attribute of the resource is 1, the agent changes the role of the secondary site to Primary and the role of the original primary site to Secondary.
	  ■ If the value of the SwapRoles attribute of the resource is 0, the agent changes the role of the secondary site to Primary-Rev and the role of the original primary to Secondary-Rev.
	■ If the replication mode is Periodic, then depending on the value of the ForceSync attribute, the agent does the following:
	  ■ If the value of the ForceSync attribute is 1, the resource fails to come online.
	  ■ If the value of the ForceSync attribute is 0, the resource comes online.

Table 4-1 Failure scenarios in global cluster and replicated data cluster configurations with the Cluster Server agent for HPE 3PAR Remote Copy *(continued)*

Failure	Description and VCS response

Site failure	All hosts and the storage at the primary site fail.
	A site failure renders the target node in a FAILED state.
	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: If the target status is Failed and Sync status is Stopped or Stale, the agent attempts to change the roles in the following manner:
	■ If the value of the AutoTakeover attribute is 0, the agent does not take any action.
	■ If the value of the AutoTakeover attribute is 1, the agent executes the failover command.

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. The site-wide split brain 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: Veritas 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.
	Agent response: Similar to the site failure.

Table 4-1 Failure scenarios in global cluster and replicated data cluster configurations with the Cluster Server agent for HPE 3PAR Remote Copy *(continued)*

Failure	Description and VCS response

Storage failure	The array at the primary site fails.
	A storage failure at the primary site renders the target node in the Failed state.
	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: Similar to the site failure.

Testing global service group migration between global clusters

After you configure the VCS agent for HPE 3PAR Remote Copy, verify that the global service group can migrate to hosts across the clusters.

To test the global service group migration in global cluster setup using the VCS GUI

1. In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the global service group and click **Online** to bring the service group online on the primary cluster.
2. To switch over the global service group from the primary cluster to the secondary cluster, right-click the service group and select **Remote Switch**.

   The global service group comes online on the secondary cluster. Now the secondary cluster role changes to Primary-Rev and the original primary cluster role changes to Secondary-Rev. If the SwapRoles attribute is set to 1, the secondary cluster role changes to Primary and the original primary cluster role changes to Secondary.

   The latest data is available after migration.
3. To switch back the global service group to its original primary cluster, right-click the service group and select **Remote Switch**.

   The global service group comes online on its original primary cluster, and the latest data is available.

To test the global service group migration in global cluster setup using the command line interface (CLI)

1. Switch over the global service group from the primary cluster to the secondary cluster.

   Perform the following steps:

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

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

     VCS brings the global service group online on a node at the secondary cluster.
   - Verify that the HPE 3PAR Remote Copy devices at the secondary cluster are write-enabled.
2. Switch back the global service group from the secondary cluster to the primary cluster.

   Perform the following steps:

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

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

     VCS brings the global service group online at the primary cluster.

- Verify that the HPE 3PAR Remote Copy devices at the secondary cluster are write-enabled.

Testing service group migration between replicated data clusters

After you configure the VCS agent for HPE 3PAR Remote Copy, verify that the service group can migrate to hosts across the sites.

To test the service group migration in replicated data cluster setup using the VCS GUI

1. In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group and click **Online** to bring the service group online on the primary site.
2. To switch over the service group from the primary site to the secondary site, right-click the service group and select **Switch To**.

   The service group comes online on the secondary site. Now the secondary site role changes to Primary-Rev and the original primary site role changes to Secondary-Rev. If the SwapRoles attribute is set to 1, the secondary site role changes to Primary and the original primary site role changes to Secondary.

   The latest data is available after migration.
3. To switch back the service group to its original primary site, right-click the service group and select **Switch To**.

   The service group comes online on its original primary site, and the latest data is available.

To test the service group migration in replicated data cluster setup using the command line interface (CLI)

1. Switch 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 HPE 3PAR Remote Copy devices at the secondary site are write-enabled
2. Switch 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 the primary site.

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

  VCS brings the service group online at the primary site.
- Verify that the HPE 3PAR Remote Copy devices at the secondary site are write-enabled.

Testing all hosts failure in a global cluster

Perform the following procedure to test how VCS recovers after all hosts at the primary cluster fail.

To test disaster recovery for all hosts failure in global cluster setup, using the VCS GUI

1. Halt or shut down all the hosts at the primary cluster.

   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 cluster.
   - Manual or Connected—You must bring the global service group online at the secondary cluster.
     In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group and click **Online**.
2. Verify that the 3PAR Remote Copy devices at the secondary cluster are write-enabled.

   Verify that the latest data is available.

To test disaster recovery for all hosts failure in global cluster setup, using the command line interface (CLI)

1. Halt the hosts at the primary cluster.

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

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

2 Run the following command to verify that the global service group is online at the secondary cluster:

```
hagrp -state global_group
```

3 Verify that the 3PAR Remote Copy devices at the secondary cluster are write-enabled.

Verify that the latest data is available.

Testing all hosts failure in a replicated data cluster

Perform the following procedure to test how VCS recovers after all hosts at the primary site fail.

To test disaster recovery for all hosts failure in replicated data cluster setup, using the VCS GUI

1 Halt or shut down all 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.
  In the Service Groups tab of the Cluster Explorer configuration tree, right-click the service group and click **Online**.

2 Verify that the 3PAR Remote Copy devices at the secondary site are write-enabled.

Verify that the latest data is available.

To test disaster recovery for all hosts failure in replicated data cluster setup, using the command line interface (CLI)

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 service_group sys_name
```

2. Run the following command to verify that the global service group is online at the secondary site:

   ```
   hagrp -state service_group
   ```

3. Verify that the 3PAR Remote Copy devices at the secondary site are write-enabled.

   Verify that the latest data is available.