

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

Windows

6.0

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

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

Agent Version: 6.0

Document version: 6.0 Rev 0

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, the Veritas Logo, InfoScale, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

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

Documentation

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

<https://sort.symantec.com/documents>

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Contents

Technical Support	3
Chapter 1 Introducing the agent for HP 3PAR Remote Copy	7
About the agent for HP 3PAR Remote Copy	7
Typical HP 3PAR Remote Copy setup in a VCS cluster	8
HP 3PAR Remote Copy agent functions	9
About the agent's online function	11
Chapter 2 Installing and removing the agent for HP 3PAR Remote Copy	13
Before you install the agent for HP 3PAR Remote Copy	13
Installing the agent for HP 3PAR Remote Copy	13
Removing the agent for HP 3PAR Remote Copy	14
Chapter 3 Configuring the agent	15
Configuration concepts for the 3PAR Remote Copy agent	15
Resource type definition for the 3PAR Remote Copy agent	15
Attribute definitions for the 3PAR Remote Copy agent	16
Sample configuration for the 3PAR Remote Copy agent	18
Before you configure the agent for HP 3PAR Remote Copy	18
About cluster heartbeats	19
About PuTTY configuration for 3PAR Remote Copy	19
Configuring the agent for HP 3PAR Remote Copy	21
Chapter 4 Managing and testing clustering support for HP 3PAR Remote Copy	22
Typical test setup for the HP 3PAR Remote Copy agent	23
Testing global service group migration between global clusters	24
Testing all hosts failure in a global cluster	25
Index	27

Introducing the agent for HP 3PAR Remote Copy

This chapter includes the following topics:

- [About the agent for HP 3PAR Remote Copy](#)
- [Typical HP 3PAR Remote Copy setup in a VCS cluster](#)
- [HP 3PAR Remote Copy agent functions](#)

About the agent for HP 3PAR Remote Copy

The Cluster Server agent for HP 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 HP 3PAR Remote Copy replication feature in VCS global clusters and replicated data clusters.

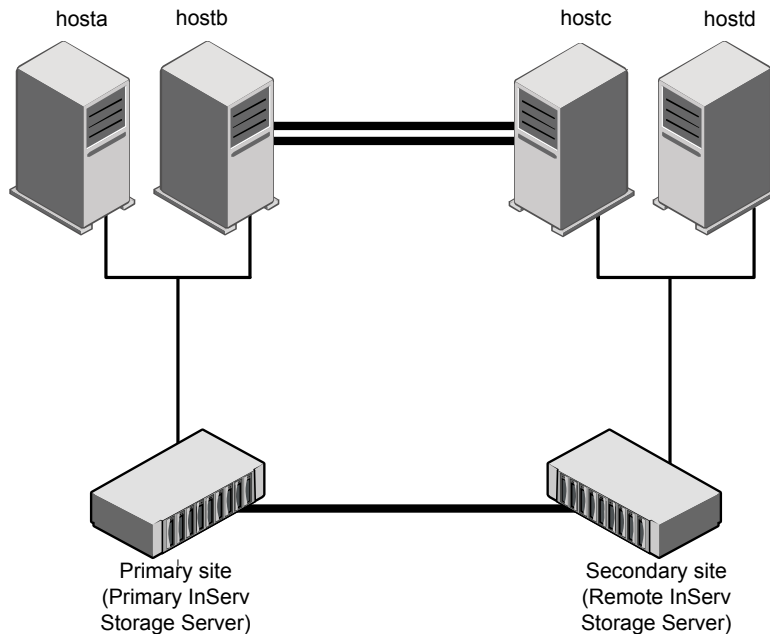
The agent supports the synchronous and periodic modes of replication with the mirror_config policy.

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.

Typical HP 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.

HP 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	<p>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 <code>setrcopygroup</code> command to enable read-write access to the volumes.</p> <p>See “About the agent's online function” on page 11.</p> <p>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.</p>
offline	<p>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.</p>
monitor	<p>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.</p>
open	<p>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.</p> <p>Note that the agent does not remove the lock file if the agent was started after running the following command:</p> <pre>hastop <-all -local> -force</pre>
clean	<p>Determines if it is safe to fault the resource if the online function fails or times out.</p>

info	<p>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.</p>
action/recover	<p>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.</p> <p>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.</p> <p>This action function executes the <code>setrcopygroups -recover <i>groupname</i></code> command.</p>
action/restore	<p>This action function is used on groups on which the recover operation has already been run.</p> <p>This action function returns specified groups to their natural direction and starts them.</p> <p>This action function executes the <code>setrcopygroups restore <i>groupname</i></code> command.</p>
action/revert	<p>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.</p> <p>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.</p> <p>This action function executes the <code>setrcopygroup reverse -current <i>groupname</i></code> command.</p> <p>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.</p>

action/startcopygroup	Starts remote copy for the specified group. The agent invokes the <code>startcopygroup</code> command to 3PAR InServe storage server.
action/PreSwitch	<p>This action function ensures that the remote site cluster can come online during a planned failover within a GCO configuration.</p> <p>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 <code>hagrp -switch</code> command. For this, the PreSwitch attribute must be set to 1. The option <code>-nopre</code> indicates that the VCS engine must switch the servicegroup regardless of the value of the PreSwitch service group attribute.</p> <p>If running the PreSwitch action fails, the failover should not occur. This minimizes the application downtime and data loss.</p> <p>For more information on the PreSwitch action and the PreSwitch feature in the VCS engine, refer to the <i>Cluster Server Administrator's Guide</i>.</p>
action/syncrcopy	Synchronizes the specified remote copy group. The agent invokes the <code>syncrcopy</code> command to the 3PAR InServe storage server.

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.

Installing and removing the agent for HP 3PAR Remote Copy

This chapter includes the following topics:

- [Before you install the agent for HP 3PAR Remote Copy](#)
- [Installing the agent for HP 3PAR Remote Copy](#)
- [Removing the agent for HP 3PAR Remote Copy](#)

Before you install the agent for HP 3PAR Remote Copy

Before you install the Cluster Server agent for HP 3PAR Remote Copy, ensure that you install and configure the 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 HP 3PAR Remote Copy setup in a VCS cluster”](#) on page 8.

Installing the agent for HP 3PAR Remote Copy

You must install the HP 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 Cluster Server agent for HP 3PAR Remote Copy from the Agent Pack release

- 1 Log on to any node in the cluster.
Ensure that the logged on user has the domain administrative privileges.
- 2 Download the Agent Pack from the Symantec Operations Readiness Tools (SORT) site: <https://sort.symantec.com/agents>.
You can download the complete Agent Pack zip file or the individual agent zip file.
- 3 Uncompress the file to a temporary location.
- 4 If you downloaded the complete Agent Pack zip file, navigate to the directory containing the package for the platform running in your environment.

```
Windows 2008      cd1\windows\w2k8x64\vcs\replication\3par_agent\  
x64              agentversion\pkgs
```

```
Windows 2012      cd1\windows\w2k12x64\vcs\replication\  
x64              3par_agent\agentversion\pkgs
```

- 5 Double-click **vrtsvcsremotecopy.msi**.
Follow the instructions that the install program provides, to complete the installation of the agent.

Removing the agent for HP 3PAR Remote Copy

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 for 3PAR Remote Copy that was installed from an Agent Pack release

- 1 Open the Windows Control Panel and click **Add or Remove Programs** or **Uninstall a Program**.
- 2 Select Cluster Server Agent for HP 3PAR RemoteCopy.
- 3 Click the **Remove** or **Uninstall** button.
- 4 Follow the instructions the installer provides to complete the uninstallation.

Configuring the agent

This chapter includes the following topics:

- [Configuration concepts for the 3PAR Remote Copy agent](#)
- [Before you configure the agent for HP 3PAR Remote Copy](#)
- [Configuring the agent for HP 3PAR Remote Copy](#)

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 SupportedActions = { PreSwitch, recover, revert,
    restore, startrcopygroup, syncrcopy }
    static str ArgList[] = { StorageServer, UserName, GroupName,
    SSHBinary, SSHPathToIDFile, AutoTakeover, SwapRoles, ForceSync,
    CLIBinary, PasswordFile }
    str StorageServer
    str UserName
    str GroupName
    str CLIBinary
    str PasswordFile
    str SSHBinary = "C:\\Program Files\\PuTTY\\plink.exe"
    str SSHPathToIDFile
    int AutoTakeover = 0
    int SwapRoles = 0
```

```
        int ForceSync = 0
    )
```

Attribute definitions for the 3PAR Remote Copy agent

Table 3-1 describes the required attributes for the HP 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 HP 3PAR password file that is used to connect to the 3PAR InServ Storage Server at the current site. Type-dimension: string-scalar Example: C:\3PAR\passfile
CLIBinary	Contains the absolute path to the HP 3PAR CLI binary. Type-dimension: string-scalar Example: C:\Program Files\3PAR\inform_cli_3.1.2\bin\cli.exe
SSHBinary	Contains the absolute path to the SSH binary. SSH is the mode of communication with the 3PAR InServ Storage Server. Default: C:\Program Files\PuTTY\plink.exe Type-dimension: string-scalar

Table 3-1 Required attributes (*continued*)

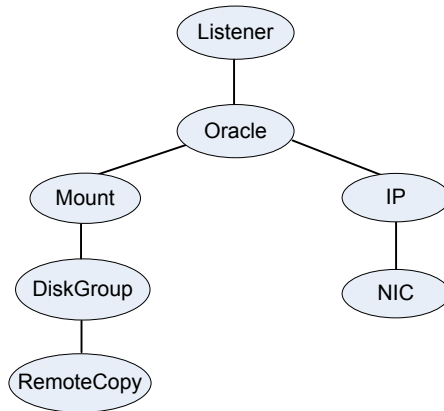
Attribute	Description
SSHPathToIDFile	<p>Contains the absolute path to the identity file that is used for authenticating the host with the 3PAR InServ Storage Server. The corresponding public key must be added on the storage server so that it can correctly authenticate the host.</p> <p>Type-dimension: string-scalar</p> <p>Example: C:\Program Files\PuTTY</p>
GroupName	<p>Specifies the group name in which Remote Copy is configured on the Storage Server.</p> <p>Type-dimension: string-scalar</p> <p>Example: Oracle_Grp</p>
AutoTakeover	<p>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).</p> <p>If it is set to 0, the agent will not enable read/write access when the replication is in an inactive state.</p> <p>Type-dimension: integer-scalar</p> <p>Default: 0</p>
SwapRoles	<p>Specifies if the roles of the Remote Copy group must be swapped at the time of failover.</p> <p>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.</p> <p>Roles are swapped only when the status of the target is Ready.</p> <p>Type-dimension: integer-scalar</p> <p>Default: 0</p>
ForceSync	<p>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.</p> <p>This attribute is applicable only to the periodic mode of replication.</p> <p>Type-dimension: integer-scalar</p> <p>Default: 0</p>

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

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 HP 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.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
See [“Typical HP 3PAR Remote Copy setup in a VCS cluster”](#) on page 8.
- Make sure that the cluster has an effective heartbeat mechanism in place.
See [“About cluster heartbeats”](#) on page 19.

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.

About PuTTY configuration for 3PAR Remote Copy

The VCS agent for 3PAR Remote Copy on Windows has qualified the `plink` command from the PuTTY command tools.

Note: You must complete this procedure on all the relevant VCS nodes and InServ storage servers. On nodes where this procedure is not completed, the agent fails to communicate with the InServ storage server, and therefore, might not run correctly.

To download and install PuTTY

- 1 Download the PuTTY 0.58 installer from the Internet.

Note: The agent works with PuTTY version .58. Other PuTTY versions do not work with the agent for 3PAR Remote Copy.

- 2 Extract the PuTTY installer and install it on the VCS node.

Make sure that this PuTTY folder contains the following files: `plink`, `putty`, `puttygen`.

Note: The steps are illustrative only. For other ways of configuring passwordless ssh, refer to PuTTY documentation.

To generate SSH keys on a VCS node and set up passwordless ssh to the InServ storage server:

- 1 Click **Start > Programs > PuTTY > PuTTYgen**.
- 2 Click **SSH-2 RSA** as the key to be generated.
- 3 Click **Generate**.
- 4 Move the cursor around the blank area of the Key section to generate a random number.

- 5 Copy the public key from the PuTTYgen window. Run the `setsshkey -add` command to add the public key on the InServ storage server.
- 6 Click **Save private key**.
- 7 Click **Yes** when you are prompted to confirm that you want to create the key without a pass phrase. Make sure that the extension to the private keys is **.ppk**. For example, `private.ppk`. Save the key in the default location: `C:\Program Files\PuTTY\private.ppk`.
- 8 Copy the private key file in the same location on all VCS nodes.

When `plink` command is used for the first time, it prompts you to accept the host certificate. You must accept the certificate for the local system account so that the agent can use it.

After communication with the InServ storage server is established, perform the following steps to accept the host certificate.

To accept the host certificate

- 1 Download PsTools from the sysinternals site.
- 2 Extract the PsTools.
- 3 Open a new command prompt window.
- 4 Using the command-line interface, navigate to the location of the directory where you have extracted PsTools.
- 5 Run the following command:

`psexec -i -s cmd.exe.`
- 6 Verify that the path of the newly-launched command prompt is
`C:\Windows\system32>.`

Navigate to the directory where PuTTY is installed.

- 7 Run the following command:

```
Plink -i <path to .ppk file> -l <InServ Storage Server User Name>  
<IP address of the InServ Storage Server>
```

For example, C:\Program Files\PuTTY>plink.exe -i private.ppk -l
admin 10.182.1.14.

The output of this command displays the following information:

```
The server's host key is not cached in the registry.  
You have no guarantee that the server is the computer you think it is.  
The server's rsa2 key fingerprint is: ssh-rsa 2048  
bd:f8:aa:34:43:8c:99:c4:d6:77:a6:65:54:5e:5a:b6  
If you trust this host, enter "y" to add the key to PuTTY's cache  
and carry on connecting. If you want to carry on connecting just  
once, without adding the key to the cache, enter "n". If you do  
not trust this host, press Return to abandon the connection.  
Store key in cache? (y/n)
```

- 8 Type **y** to cache the certificate and press **Enter**.
- 9 Close the command prompt and repeat these steps on each VCS node where the service group containing the HP 3PAR RemoteCopy resource is configured.

Configuring the agent for HP 3PAR Remote Copy

You can configure clustered application in a disaster recovery environment by:

- Converting their devices to 3PAR Remote Copy devices
- Synchronizing the devices
- Adding the HP 3PAR Remote Copy agent to the service group

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

See [“Sample configuration for the 3PAR Remote Copy agent”](#) on page 18.

Note: You must not change the replication state of devices from primary to secondary and from secondary to primary, outside of a VCS setup. The agent for HP 3PAR Remote Copy fails to detect a change in the replication state if the role reversal is done externally and RoleMonitor is disabled.

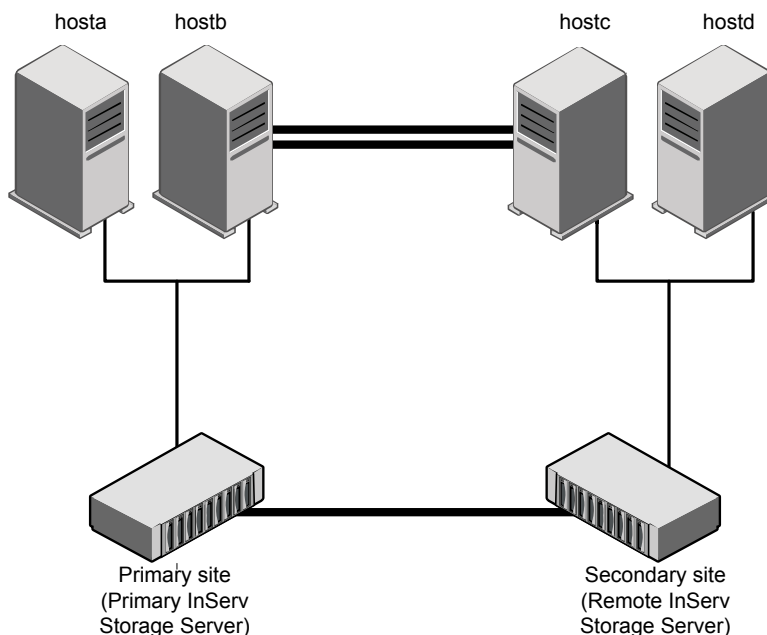
Managing and testing clustering support for HP 3PAR Remote Copy

This chapter includes the following topics:

- [Typical test setup for the HP 3PAR Remote Copy agent](#)
- [Testing global service group migration between global clusters](#)
- [Testing all hosts failure in a global cluster](#)

Typical test setup for the HP 3PAR Remote Copy agent

Figure 4-1 Typical test setup



A typical test environment includes the following characteristics:

- A primary site, an HP 3PAR RemoteCopy cluster, is attached to the primary storage and the primary application hosts.
- A secondary site, an HP 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 HP 3PAR InServ storage server.
- Two hosts (for example, Host C and Host D) are attached to the secondary site HP 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 HP 3PAR InServ storage server so

that the hosts can communicate by SSH with the primary site HP 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 HP 3PAR InServ storage server so that the hosts can communicate by SSH with the secondary site HP 3PAR InServ storage server.
- The application runs on Host A, which is connected to the primary site HP 3PAR InServ storage server.

Testing global service group migration between global clusters

After you configure the VCS agent for HP 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 HP 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 HP 3PAR Remote Copy devices at the secondary cluster 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.

Index

A

- action function 9
- attribute definitions
 - AutoTakeover 16
 - ForceSync 16
 - GroupName 16
 - SSHBinary 16
 - SSHPathToIDFile 16
 - StorageServer 16
 - SwapRoles 16
 - UserName 16

C

- clean function 9
- cluster
 - heartbeats 19

F

- functions
 - action 9
 - clean 9
 - monitor 9
 - offline 9
 - online 9
 - open 9

H

- HP 3PAR Remote Copy agent
 - about 7
 - attribute definitions 16
 - resource type definition 15
 - supported modes 7
 - typical setup 8

I

- installing the agent
 - Windows systems 13

M

- monitor function 9

O

- offline function 9
- online function 9
- open functions 9

S

- sample configuration 18

T

- Testing
 - all hosts failure in GCO 25
 - service group migration in GCO 24

U

- uninstalling the agent
 - Windows systems 14