Veritas™ Cluster Server Agent for HP EVA Continuous Access Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

5.0

June 2012

Symantec™

Veritas Cluster Server Agent for HP EVA Continuous Access 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: 5.0.01.0

Document version: 5.0.01.0.2

Legal Notice

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 Web site at the following URL:

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

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

Contacting Technical Support

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

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

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

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

About Symantec Connect

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

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

Contents

Chapter 1

Introducing the Veritas agent for HP EVA Continuous Access

This chapter includes the following topics:

About the agent for HP EVA Continuous Access

The Veritas agent for HP Storage Works EVA Continuous Access provides support for application failover and recovery. The agent provides this support in environments that use HP Enterprise Virtual Array Continuous Access (EVA CA) to manage replication relationships in real time over a storage area network (SAN).

The agent manages all the replication relationships between the virtual disks of the two EVA storage arrays.

The agent for HP EVA Continuous Access enables a DR (Data replication) group to failover, thereby enabling a reversal of the replication direction of a DR group when Enterprise Virtual Array Continuous Access (EVA CA) is configured in a VCS environment.

The agent monitors and manages the state of replicated virtual disks within EVA arrays that are attached to VCS nodes. SSSU (Storage System Scripting Utility) is installed on each of the VCS cluster nodes from where the EVA arrays can be monitored. The SSSU communicates with the Command View EVA management server.

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

The agent supports both synchronous and asynchronous modes.

See the following Technical Support TechNote for the latest updates or software issues for this agent:

http://seer.entsupport.symantec.com/docs/282004.htm

Supported software for the HP EVA Continuous Access agent

For information on the software versions that the agent for HP EVA Continuous Access supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Supported hardware for HP EVA Continuous Access

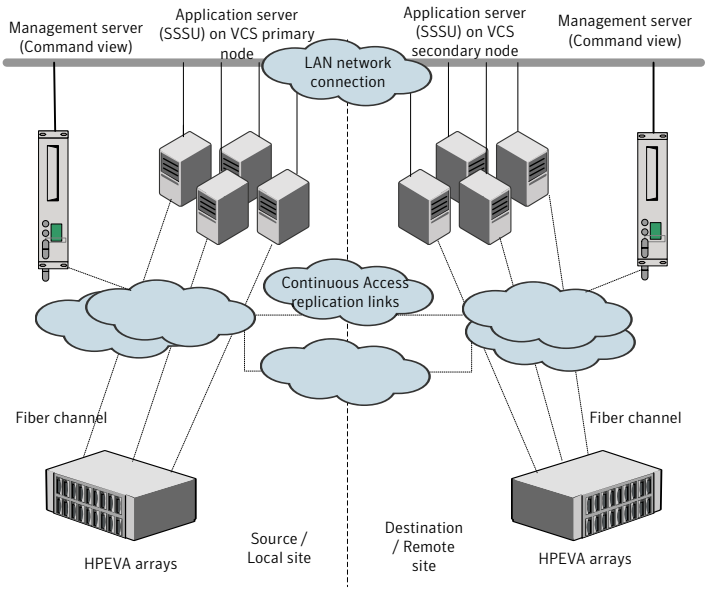
The agent supports HP EVA Continuous Access on HP Storage Works Enterprise Virtual Arrays EVA 4400 and EVA 4100/6100/8100.

It also supports Command view 8.0 or later on the management server and SSSU (Storage System Scripting Utility) on application servers.

Typical HP EVA Continuous Access setup in a VCS cluster

Figure 1-1 displays a typical cluster setup in a HP EVA Continuous Access environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a HP EVA Continuous Access environment typically consists of the following hardware infrastructure:

- EVA (4100, 4400...) arrays with SAN (Storage Area Network) / Fiber Channel (FC connectivity) between them attached to a windows server (Command View Management server) and application servers (linux boxes).
- A fabric connection between the local and remote arrays and a software (DR group) connection between the source and destination virtual disks.
- A data replication (DR) group is a logical container that includes LUNs from EVA arrays.
- The virtual disks in the DR group fail over together, replicate to the same specified destination storage array, share a write history log (DR group log), preserve write order within the data replication collection groups, and share a log disk.
- All virtual disks used for replication must belong to a DR group, and a DR group must contain at least one virtual disk.
- Network heartbeating between the two data centers to determine their health; this network heartbeating could be LLT or TCP/IP.
  See "About cluster heartbeats" on page 23.

- 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 EVA array.

HP EVA Continuous Access agent functions

The agent for HP EVA Continuous Access handles the reversal of replication relationship of a DR group when Enterprise Virtual Array Continuous Access (EVA CA) is configured in a VCS environment.

The agent performs the following functions:

online

Checks if the role or mode of the DR group is source or destination.

If the role or mode of the DR group is source, the online function:

- Creates a lock file on the local host to indicate that the resource is online. This makes the devices writeable for the application.

If the role or mode of the DR group is destination, the online function performs the following checks:

- If the replication link is broken and the value of the AutoTakeover attribute is set to 1, it runs the `failover` command.
- If the replication is suspended and the value of the SplitTakeover attribute is set to 1, it runs the `failover` command.
- If the replication mode or write mode is asynchronous, it is set to synchronous so that the secondary becomes up-to-date. While the log merges or full copy is performed, the online function waits for synchronization to complete till the OnlineTimeout expires. If the secondary is up-to-date, it runs the `failover` command.

Note: The HP Command View Storage System Scripting Utility (SSSU) does not allow DR group failover when replication is suspended and the write mode is synchronous. Hence, in the case of synchronous replication even when the replication is suspended and the attribute SplitTakeover is set to 1, the agent will fail to bring the EVACA resource online if the DR group role is "destination."

After a successful failover, the online function creates the lock file. If the online function changed the write mode of the DR group, it tries to restore it. In short, if the write mode was changed to the synchronous mode, after the failover attempt, it tries to revert to the asynchronous mode.

offline	Removes the online lock file from the host. The agent does not run any commands because taking the resource offline is not indicative of the intention to give up the devices.
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. There is no detailed monitoring.
clean	Determines if it is safe to fault the resource if the online function fails or times out. Removes the lock file.
open	Removes the lock file if none of the parent resources or parent service groups are online.
info	Modifies or adds the resource information of the EVACA resource for attribute ReplicationStatus. This includes DR group role, write mode, operational state. If the write mode is synchronous, it also includes failsafe setting (i.e. enabled or disabled).
actions/PreSwitch	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. The operation exits with error if the replication link is down or the data at secondary site is not up-to-date. If running the PreSwitch action fails, the failover should not occur. This minimizes the application downtime and data loss.

actions/addCVUser

Adds the Command View user to the password file. You must execute it after configuring the agent and prior to using agent functionality. It takes an input file as an argument.

You must create an input file with the Command View server name, username as specified by agent attributes and the password. For example:

```
# cat input
  servername
  username
  password
```

Symantec recommends that you delete this file after executing the addCVUser function.

changeWriteMode

Changes the write mode of the source DR Group. Typically, it can be used to revert back the write mode to asynchronous, in case the online function failed to do so.

Chapter 2

Installing and removing the agent for HP EVA Continuous Access

This chapter includes the following topics:

Before you install the agent for HP EVA Continuous Access

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 HP EVA Continuous Access setup in a VCS cluster" on page 10.

Installing the agent for HP EVA Continuous Access

You must install the HP EVA Continuous Access 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 Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

   You can download the complete Agent Pack tar file or the individual agent tar file.

2. Uncompress the file to a temporary location, say /tmp.

3. If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

AIX	`cd1/aix/vcs/replication/evaca_agent/`*`agent_version`*`/pkgs/`
HP-UX (PA)	`cd1/hpux/generic/vcs/replication/evaca_agent/`*`agent_version`*`/PA/depot/`
HP-UX (IA)	`cd1/hpux/generic/vcs/replication/evaca_agent/`*`agent_version`*`/IA/depot`
Linux	`cd1/linux/generic/vcs/replication/evaca_agent/`*`agent_version`*`/rpms/`
Solaris	`cd1/solaris/dist_arch/vcs/replication/evaca_agent/`*`agent_version`*`/pkgs/`

   If you downloaded the individual agent tar file, navigate to the pkgs directory (for AIX, HP-UX, and Solaris), or rpms directory (for Linux).

4. Log in as superuser.

5. Install the package.

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

Upgrading the agent for HP EVA Continuous Access

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

To upgrade the agent software

1. Save the VCS configuration and stop the VCS engine.

   ```
   # haconf -dump -makero
   # hastop -all -force
   ```

2. Remove the agent from the node.

   See "Removing the agent for HP EVA Continuous Access" on page 17.

3. Delete the file /etc/VRTSvcs/conf/config/EVACATypes.cf.
4. Install the current version of the agent.

   See "Installing the agent for HP EVA Continuous Access" on page 15.

5. Copy the file EVACATypes.cf from the directory /etc/VRTSvcs/conf/ to the /etc/VRTSvcs/conf/config directory.
6. Repeat step 2 through step 5 on each node.
7. From a node in the cluster, edit your configuration file /etc/VRTSvcs/conf/config/main.cf.

   Configure the new attributes, if applicable.

8. Verify the configuration

   ```
   # hacf -verify config
   ```

9. Start VCS on local node first.
10. Start VCS on other nodes.

Removing the agent for HP EVA Continuous Access

Before you attempt to remove the agent, make sure the application service group is not online. You must remove the agent from each node in the cluster.

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

AIX	`# installp -u VRTSvcsca.rte`
HP-UX	`# swremove VRTSvcsca`

Linux	`# rpm -e VRTSvcsca`
Solaris	`# pkgrm VRTSvcsca`

Configuring LVM on AIX

To support failover of the LVM volume groups to the secondary site during a disaster or normal switch, you must have the AIX ODM repository at the secondary populated with the LVM volume group entries. This must be done as part of an initial setup process before VCS starts controlling the replication.

To configure LVM on AIX

1. Start the replication. When it is synchronized, use any one of the below methods at the secondary site :
   - Create a MirrorClone of VDisks being replicated at the secondary site. When the MirrorClone is in synch with the source Vdisk, fracture the MirrorClone and present it to the hosts at secondary sites.
   - Create a SnapShot of VDisks being replicated at the secondary site. After the SnapShot is created, present it to the hosts at the secondary site.
2. At the secondary site, run the `chdev -l <diskname> -a pv=yes` command for each disk inside the replicated device group lvmdg. This gets the physical volume identity (PVID) from within the disk and updates the ODM with this value. Now these disks have the same PVIDs as their counterparts at the primary site.
3. Run the `importvg -y <vgname> -n <diskname>` command for each volume group.
4. Delete the MirrorClone(s) and SnapShot(s) created in step 1.
5. Start VCS.

Chapter 3

Configuring the agent for HP EVA Continuous Access

This chapter includes the following topics:

Configuration concepts for the HP EVA Continuous Access agent

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

Resource type definition for the HP EVA Continuous Access agent

The EVACA resource type represents the HP EVA Continuous Access agent in VCS.

```
type EVACA (
 static keylist SupportedActions = { PreSwitch, addCVUser,
 changeWriteMode }
 static int OfflineMonitorInterval = 0
 static int InfoInterval = 300
 static int OnlineTimeout = 600
 static int OpenTimeout = 180
 static int RestartLimit = 1
 static str ArgList[] = { ManagementServer, UserName,
 StandbyManagementServer, StandbyUserName, LocalEVAName,
```

```
 DRGroupName, SSSUPath, SplitTakeover, AutoTakeover }
 str ManagementServer
 str UserName = "hpadmin"
 str StandbyManagementServer
 str StandbyUserName = "hpadmin"
 str LocalEVAName
 str DRGroupName
 str SSSUPath
    int SplitTakeover = 0
    int AutoTakeover = 1
)
```

Attribute definitions for the HP EVA Continuous Access agent

Review the description of the agent attributes.

Required attributes

You must assign values to required attributes.

Management server	Specifies the name of the Command View management server. Type-dimension: string-scalar
UserName	Specifies the user name to access the management server. The default value is: hpadmin. Type dimension: string-scalar
LocalEVAName	Specifies the name of the local Enterprise Virtual Array (EVA). Type-dimension: string-scalar
DRGroupName	Specifies the data replication group name. Type-dimension: string-scalar
SSSUPath	Specifies the path to the Storage System Scripting Utility (SSSU) along with the binary name. Type-dimension: string-scalar

Optional attributes

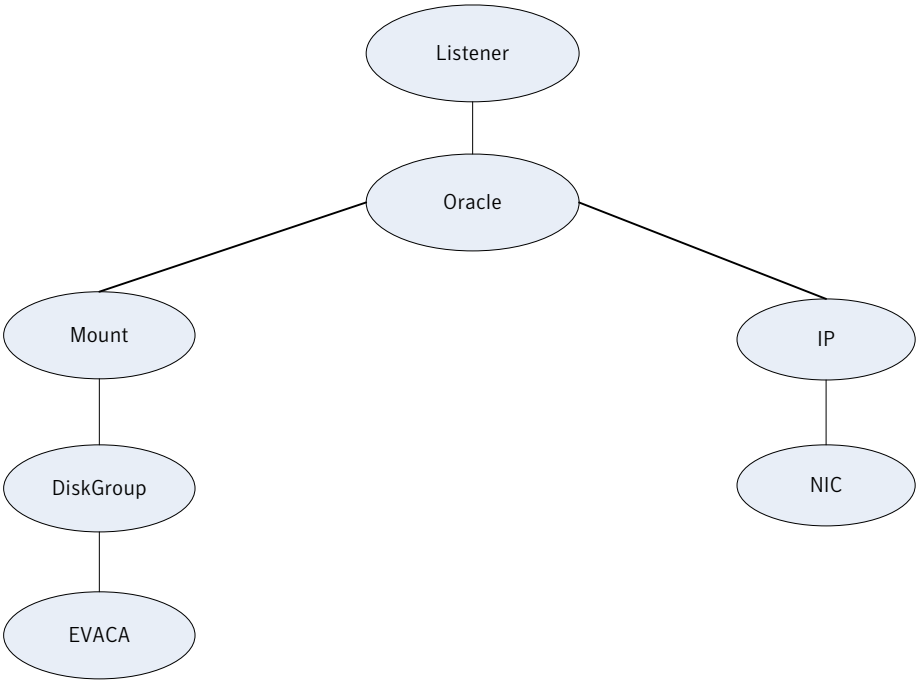
Optionally assign values to these attributes.

StandbyManagementServer	Specifies the name of the standby Command View management server. When executing any agent functions, the agent uses this server name in the following circumstance: ■ if the local array is actively managed by this server, and not by the management server that is specified in the Management server attribute. Type-dimension: string-scalar
StandbyUserName	Specifies the user name that is required to connect to the standby Command View management server. The default value is "hpadmin" Type-dimension: string-scalar
AutoTakeover	Indicates whether the failover should occur when the replication link is broken. The default value is 1. Type-dimension: integer-scalar
SplitTakeover	Indicates whether the failover should occur when the replication link is suspended. The default value is 0. Type-dimension: integer-scalar

Sample configuration for the HP Storage Works EVA Continuous Access agent

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

Figure 3-1 Sample configuration for the HP EVA Continuous Accessagent



The DiskGroup resource depends on the EVACA resource.

You can configure a resource of type EVACA as follows in main.cf:

```
EVACA EVACA_oraprod_evaca (
  ManagementServer = "EVAMgmtServer"
  LocalEVAName = localeva
  DRGroupName = DRGrp1
  SSSUPath = "/opt/Hewlett-Packard/sssu_linux_x86"
  )
```

Before you configure the agent for HP EVA Continuous Access

Before you configure the agent, review the following information:

- Review the configuration concepts, which describe the agent's type definition and attributes.

See "Configuration concepts for the HP EVA Continuous Access 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 HP EVA Continuous Access 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 23.
- The agent for HP EVA Continuous Access uses Command View Manager username and password to connect to the management server. This is required by the SSSU commands. The agent leverages the SSSU password file, instead of passing the password in each SSSU command it executes. You must add the Command View username to the password file before leveraging agent functionality.
  You must do this by running the `SSSU -a` command on each cluster node, after installing SSSU on VCS nodes. This command requires the management server name, user name, and password as parameters. After you run this command successfully, specify the same management server name and user name when you are configuring the EVACA resource. Similarly, if you are using a standby management server, you must add this server's user name to the SSSU password file on each VCS cluster node.
  Optionally, you may run the addCVUser function on each VCS node after the EVACA resource is configured.
  See "HP EVA Continuous Access agent functions" on page 12.

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.

About configuring system zones in replicated data clusters

In a replicated data cluster, you can prevent unnecessary HP EVA Continuous Access 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.

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.

Configuring the agent for HP EVA Continuous Access

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

- Converting their devices to HP EVA Continuous Access devices
- Synchronizing the devices
- Adding the HP EVA Continuous Access agent to the service group

Configure EVA volumes as resources of type EVACA.

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

See "Sample configuration for the HP Storage Works EVA Continuous Access agent" on page 21.

Note: You must not change the replication state of devices primary to secondary and viceversa, outside of a VCS setup. The agent for HP Storage Works EVA Continuous Access fails to detect a change in the replication state if the role reversal is done externally.

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 (EVACA) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

   /etc/VRTSvcs/conf/EVACATypes.cf.

3 Click **Import**.

4 Save the configuration.

5 Add a resource of type EVACA at the bottom of the service group.

6 Configure the attributes of the EVACA resource.

7 If the user, who is specified in the username attribute, is not already added to the SSSU password file, run the addCVUser action entry point on each of the cluster nodes for which the resource is configured.

See "HP EVA Continuous Access agent functions" on page 12. .

Optionally, you may run the `sssu -a` command from the command line. You must provide the same values for the management server name and user name, as configured in the resource's attributes, before using the agent functionality.

8 If the service group is not configured as a global service group, configure the service group using the Global Group Configuration Wizard.

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

9 Change the ClusterFailOverPolicy attribute from the default, if necessary. Symantec recommends keeping the default, which is Manual, to minimize the chance of failing over on a split-brain.

10 Repeat step 5 through step 9 for each service group in each cluster that uses replicated data.

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 (EVACA) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

/etc/VRTSvcs/conf/EVACATypes.cf.

3 Click **Import**.

4 Save the configuration.

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

6 Configure the attributes of the EVACA resource. Note that some attributes must be localized to reflect values for the hosts that are attached to different arrays.

7 If the user, who is specified in the username attribute, is not already added to the SSSU password file, run the addCVUser action entry point on each of the cluster nodes for which the resource is configured.

See "HP EVA Continuous Access agent functions" on page 12. .

Optionally, you may run the `sssu -a` command from the command line. You must provide the same values for the management server name and user name, as configured in the resource's attributes, before using the agent functionality.

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

Chapter 4

Managing and testing clustering support for HP EVA Continuous Access

This chapter includes the following topics:

How VCS recovers from various disasters in an HA/DR setup with HP EVA Continuous Access

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

Global clusters	When a site-wide global service group or system fault occurs, VCS failover behavior depends on the value of the ClusterFailOverPolicy attribute for the faulted global service group. The VCS agent for HP EVA Continuous Access ensures safe and exclusive access to the configured HP EVA Continuous Access devices. See "Failure scenarios in global clusters" on page 28.
Replicated data clusters	When service group or system faults occur, VCS failover behavior depends on the value of the AutoFailOver attribute for the faulted service group. The VCS agent for HP EVA Continuous Access ensures safe and exclusive access to the configured HP EVA Continuous Access devices. See "Failure scenarios in replicated data clusters" on page 32.

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

Failure scenarios in global 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.

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

Table 4-1 Failure scenarios in a global cluster configuration with VCS agent for HP EVA Continuous Access

Failure	Description and VCS response

Application failure	Application cannot start successfully on any hosts at the primary site.
	VCS response at the secondary site:
	■ Causes global service group at the primary site to fault and displays an alert to indicate the fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto or Connected—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual—No action. You must bring the global group online at the secondary site.
	Agent response:
	■ Write enables the devices at the secondary site.
	■ The agent does the following:
	  ■ In case the replication is suspended and the value of the SplitTakeover attribute is set to 0, no action is taken by agent.
	  ■ In case the write mode is asynchronous, the agent sets it to synchronous and waits for the replicated data at the secondary side to become up-to-date.
	  ■ Swaps the Source/Destination role of the DR Group.
	  ■ Restarts the replication from the Source DR group on the secondary site to the Destination DR group at the primary site.
	See "Performing failback after a node failure or an application failure" on page 38.

Table 4-1 Failure scenarios in a global cluster configuration with VCS agent for HP EVA Continuous Access *(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:
	■ Write enables the devices at the secondary site.
	■ The agent does the following:
	  ■ In case the replication is suspended and the value of the SplitTakeover attribute is set to 0, no action is taken by agent.
	  ■ In case the write mode is asynchronous, the agent sets it to synchronous and waits for the replicated data at the secondary side to become up-to-date.
	  ■ Swaps the Source/Destination role of the DR Group.
	  ■ Restarts the replication from the Source DR group on the secondary site to the Destination DR group at the primary site.
	See "Performing failback after a node failure or an application failure" on page 38.

Site failure	All hosts and the storage at the primary site fail.
	VCS response at the secondary site:
	■ Displays an alert to indicate the cluster fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual or Connected—No action. You must bring the global group online at the secondary site.
	Agent response: The agent does the following based on the value of the AutoTakeover attribute of the EVACA resource:
	■ 1—The agent issues the `failover` command to make the EVACA devices write-enabled at the secondary site.
	■ 0—No action is taken by the agent. The EVACA resource is faulted.
	See "Performing failback after a site failure" on page 39.

Table 4-1 Failure scenarios in a global cluster configuration with VCS agent for HP EVA Continuous Access *(continued)*

Failure	Description and VCS response
Replication link failure	Replication link between the arrays at the two sites fails. VCS response: No action. Agent response: The agent does the following based on the value of the AutoTakeover attribute of the EVACA resource: ■ 1—The agent issues the `failover` command to make the EVACA devices write-enabled at the secondary site. ■ 0—No action is taken by the agent. The EVACA resource is faulted.
Network failure	The network connectivity and the replication link between the sites fail. VCS response at the secondary site: ■ VCS at each site concludes that the remote cluster has faulted. ■ Does the following based on the ClusterFailOverPolicy global service group attribute: ■ Manual or Connected—No action. You must confirm the cause of the network failure from the cluster administrator at the remote site and fix the issue. ■ Auto—VCS brings the global group online at the secondary site which may lead to a site-wide split brain. This causes data divergence between the devices on the primary and the secondary arrays. When the network (wac and replication) connectivity restores, you must manually resync the data. **Note:** Symantec recommends that the value of the ClusterFailOverPolicy attribute is set to Manual for all global groups to prevent unintended failovers due to transient network failures. Agent response: Similar to the site failure.
Storage failure	The array at the primary site fails. VCS response at the secondary site: ■ Causes the global service group at the primary site to fault and displays an alert to indicate the fault. ■ Does the following based on the ClusterFailOverPolicy global service group attribute: ■ Auto or Connected—VCS automatically brings the faulted global service group online at the secondary site. ■ Manual—No action. You must bring the global group online at the secondary site. Agent response: Similar to the site failure

Failure scenarios in replicated data clusters

Table 4-2 lists the failure scenarios in a replicated data cluster configuration, and describes the behavior of VCS and the agent in response to the failure.

Table 4-2 Failure scenarios in a replicated data cluster configuration with VCS agent for HP EVA Continuous Access

Failure	Description and VCS response

Application failure	Application cannot start successfully on any hosts at the primary site.
	VCS response:
	■ Causes the service group at the primary site to fault.
	■ Does the following based on the AutoFailOver attribute for the faulted global service group:
	  ■ 1—VCS automatically brings the faulted global service group online at the secondary site.
	  ■ 2—You must bring the global service group online at the secondary site.
	Agent response:
	■ Write enables the devices at the secondary site.
	■ The agent does the following:
	  ■ In case the replication is suspended and the value of the SplitTakeover attribute is set to 0, no action is taken by agent.
	  ■ In case the write mode is asynchronous, the agent sets it to synchronous and waits for the replicated data at the secondary side to become up-to-date.
	  ■ Swaps the Source/Destination role of the DR Group.
	  ■ Restarts the replication from the Source DR group on the secondary site to the Destination DR group at the primary site.
	See "Performing failback after a node failure or an application failure" on page 38.

Table 4-2 Failure scenarios in a replicated data cluster configuration with VCS agent for HP EVA Continuous Access *(continued)*

Failure	Description and VCS response

Host failure	All hosts at the primary site fail.
	VCS response:
	■ Causes the service group at the primary site to fault.
	■ Does the following based on the AutoFailOver attribute for the faulted service group:
	  ■ 1—VCS automatically brings the faulted service group online at the secondary site.
	  ■ 2—You must bring the service group online at the secondary site.
	Agent response:
	■ Write enables the devices at the secondary site.
	■ The agent does the following:
	  ■ In case the replication is suspended and the value of the SplitTakeover attribute is set to 0, no action is taken by agent.
	  ■ In case the write mode is asynchronous, the agent sets it to synchronous and waits for the replicated data at the secondary side to become up-to-date.
	  ■ Swaps the Source/Destination role of the DR Group.
	  ■ Restarts the replication from the Source DR group on the secondary site to the Destination DR group at the primary site.
	See "Performing failback after a node failure or an application failure" on page 38.

Site failure	All hosts and the storage at the primary site fail.
	VCS response:
	■ Causes the service group at the primary site to fault.
	■ Does the following based on the AutoFailOver attribute for the faulted service group:
	  ■ 1—VCS automatically brings the faulted service group online at the secondary site.
	  ■ 2—You must bring the service group online at the secondary site.
	Agent response: The agent does the following based on the value of the AutoTakeover attribute of the EVACA resource:
	■ 1—The agent issues the `failover` command to make the EVACA devices write-enabled at the secondary site.
	■ 0—No action is taken by the agent. The EVACA resource is faulted.
	See "Performing failback after a site failure" on page 39.

Table 4-2 Failure scenarios in a replicated data cluster configuration with VCS agent for HP EVA Continuous Access *(continued)*

Failure	Description and VCS response
Replication link failure	Replication link between the arrays at the two sites fails. VCS response: No action. Agent response: The agent does the following based on the value of the AutoTakeover attribute of the EVACA resource: ■ 1—The agent issues the `failover` command to make the EVACA devices write-enabled at the secondary site. ■ 0—No action is taken by the agent. The EVACA resource is faulted.
Network failure	The LLT and the replication links between the sites fail. VCS response: ■ VCS at each site concludes that the nodes at the other site have faulted. ■ Does the following based on the AutoFailOver attribute for the faulted service group: ■ 2—No action. You must confirm the cause of the network failure from the cluster administrator at the remote site and fix the issue. ■ 1—VCS brings the service group online at the secondary site which leads to a cluster-wide split brain. This causes data divergence between the devices on the arrays at the two sites. When the network (LLT and replication) connectivity is restored, VCS takes all the service groups offline on one of the sites and restarts itself. This action eliminates concurrency violation where in the same group is online at both the sites. **Note:** Symantec recommends that the value of the AutoFailOver attribute is set to 2 for all service groups to prevent unintended failovers due to transient network failures. Agent response: Similar to the site failure.
Storage failure	The array at the primary site fails. VCS response: ■ Causes the service group at the primary site to fault and displays an alert to indicate the fault. ■ Does the following based on the AutoFailOver attribute for the faulted service group: ■ 1—VCS automatically brings the faulted service group online at the secondary site. ■ 2—You must bring the service group online at the secondary site. Agent response: Similar to the site failure

Testing the global service group migration

After you configure the VCS agent for HP EVA Continuous Access, verify that the global service group can migrate to hosts across the sites. Depending on your DR configuration, perform one of the following procedures.

To test the global service group migration in global cluster setup

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

Perform the following steps:

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

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

VCS brings the global service group online on a node at the secondary site.

- Verify that the EVACA devices at the secondary site are write-enabled, and the DR group role is Source.

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

Perform the following steps:

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

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

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

- Verify that the EVACA devices at the secondary site are write-enabled, and the DR group role is Source.

To test service group migration in replicated data cluster setup

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

Perform the following steps:

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

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

VCS brings the service group online on a node at the secondary site.

- Verify that the EVACA devices at the secondary site are write-enabled, and the DR group role is Source.

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

Perform the following steps:

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

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

  VCS brings the service group online on a node at the primary site.
- Verify that the EVACA devices at the primary site are write-enabled, and the DR group role is Source.

Testing disaster recovery after host failure

Review the details on host failure and how VCS and the agent for HP EVA Continuous Access behave in response to the failure.

See "Failure scenarios in global clusters" on page 28.

See "Failure scenarios in replicated data clusters" on page 32.

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

To test disaster recovery for host failure in global cluster setup

1. Halt the hosts at the primary site.

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

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

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

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

   ```
   hagrp -state global_group
   ```

3. Verify that the EVACA devices at the secondary site are write-enabled, and the DR group role is Source.

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

1. Halt the hosts at the primary site.

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

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

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

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

```
hagrp -state global_group
```

3 Verify that the EVACA devices at the secondary site are write-enabled, and the DR group role is Source.

Testing disaster recovery after site failure

Review the details on site failure and how VCS and the agent for HP EVA Continuous Access behave in response to the failure.

See "Failure scenarios in global clusters" on page 28.

See "Failure scenarios in replicated data clusters" on page 32.

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

To test disaster recovery for site failure in global cluster setup

1 Halt all nodes and the arrays at the primary site.

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

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

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

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

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

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

```
hagrp -state global_group
```

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

1 Halt all hosts and the arrays at the primary site.

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

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

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

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

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

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

```
hagrp -state global_group
```

Performing failback after a node failure or an application failure

Review the details on node failure and application failure and how VCS and the agent for HP EVA Continuous Access behave in response to these failures.

See "Failure scenarios in global clusters" on page 28.

See "Failure scenarios in replicated data clusters" on page 32.

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

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

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

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

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

2 Verify that the EVACA devices at the primary site are write-enabled, and the DR group role is Source.

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

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

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

VCS brings the global service group online on a node at the primary site.

2 Verify that the EVACA devices at the primary site are write-enabled, and the DR group role is Source.

Performing failback after a site failure

After a site failure at the primary site, the hosts and the storage at the primary site are down. VCS brings the global service group online at the secondary site and the HP EVA Continuous Access agent write enables the secondary devices.

Review the details on site failure and how VCS and the agent for HP EVA Continuous Access behave in response to the failure.

See "Failure scenarios in global clusters" on page 28.

See "Failure scenarios in replicated data clusters" on page 32.

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

To perform failback after a site failure in global cluster

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

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

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

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

   This again swaps the role of the Source and the Destination DR group.

To perform failback after a site failure in replicated data cluster

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

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

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

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

   This again swaps the role of the Source and the Destination DR group.

Chapter 5

Setting up a fire drill

This chapter includes the following topics:

About fire drills

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

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

In clusters employing HP EVA Continuous Access, the EVACASnap resource manages the replication relationship during a fire drill.

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

Fire drill configuration

VCS supports fire drill that runs on a snapshot of the target array.

VCS performs the following tasks for fire drill:

- Suspends replication to get consistent snapshots of the DR group members.
- Takes snapshots of all replicated virtual disks in a DR group using the Business Copy feature, and then presents the snapshot disks to the local host.
- Resumes replication.
- Modifies the disk group name in the snapshot.
- Brings the fire drill service group online using the snapshot data.

You must use Veritas Volume Manager or LVM on AIX to import and deport the storage.

About the EVACASnap agent

The EVACASnap agent is the fire drill agent for HP EVA Continuous Access.

The agent manages the replication relationship between the source and target arrays when running a fire drill. Configure the EVACASnap resource in the fire drill service group, in place of the EVACA resource.

EVACASnap agent functions

The EVACASnap agent performs the following functions:

online	■ Suspends replication between the source and the target arrays. ■ Takes a local snapshot of the target LUN for each DR group member, and then presents the snapshots to the host. ■ Resumes the replication between the arrays. ■ Takes the fire drill service group online by mounting the replication target LUN. ■ Creates a lock file to indicate that the resource is online.
offline	■ Unpresents the snapshot to the host and then deletes it. ■ Removes the lock file created by the online function.
monitor	Verifies the existence of the lock file to make sure the resource is online.

clean	■ Tries to unpresent and delete snapshots taken during an unsuccessful online operation. ■ Removes the lock file created by the Online operation.
open	If the lock file does not exist, the agent takes no action. If the lock file exists: ■ If any resources that depend on the EVACASnap are online, the agent does not take any action. ■ If any resources that depend on the EVACASnap are not online, the agent removes the lock file.

Resource type definition for the EVACASnap agent

Following is the resource type definition for the EVACASnap agent:

```
type EVACASnap (
 static int OpenTimeout = 180
 static int NumThreads = 1
 static int RestartLimit = 1
 static str ArgList[] = { TargetResName }
 str TargetResName
 temp str Responsibility
 temp str FDFile
)
```

Attribute definitions for the EVACASnap agent

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

TargetResName	Name of the resource managing the LUNs that you want to take snapshot of. Set this attribute to the name of the EVACA resource if you want to take a snapshot of the replicated data. Set this attribute to the name of the VxVM DiskGroup resource if the data is not replicated. For example, in a typical Oracle setup, you might replicate data files and redo logs, but you may choose to avoid replicating temporary tablespaces. The temporary tablespace must still exist at the DR site and may be part of its own disk group. Type-Dimension: string-scalar

Before you configure the fire drill service group

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

- Make sure the application service group is configured with a EVACA resource.
- Make sure the infrastructure to take snapshots is properly configured.

Configuring the fire drill service group

On the secondary site, the initial steps create a fire drill service group that closely follows the configuration of the original application service group. The fire drill service group uses a point-in-time copy of the production data. Bringing the fire drill service group online on the secondary site demonstrates the ability of the application service group to fail over and come online at the secondary site, should the need arise.

See "Sample configuration for a fire drill service group" on page 47.

Creating the fire drill service group using Cluster Manager (Java Console)

This section describes how to use Cluster Manager (Java Console) to create the fire drill service group. After creating the fire drill service group, you must set the failover attribute to false so that the fire drill service group does not fail over to another node during a test.

To create the fire drill service group

1. Open the Veritas Cluster Manager (Java Console).
2. Log on to the cluster and click **OK**.
3. Click the **Service Group** tab in the left pane and click the **Resources** tab in the right pane.
4. Right-click the cluster in the left pane and click **Add Service Group**.
5. In the Add Service Group dialog box, provide information about the new service group.
   - In Service Group name, enter a name for the fire drill service group
   - Select systems from the Available Systems box and click the arrows to add them to the Systems for Service Group box.
   - Click **OK.**

To disable the AutoFailOver attribute

1. Click the **Service Group** tab in the left pane and select the fire drill service group.
2. Click the **Properties** tab in the right pane.
3. Click the **Show all attributes** button.
4. Double-click the **AutoFailOver** attribute.
5. In the Edit Attribute dialog box, clear the **AutoFailOver** check box.
6. Click **OK** to close the Edit Attribute dialog box.
7. Click the **Save and Close Configuration** icon in the tool bar.

Adding resources to the fire drill service group

Add resources to the new fire drill service group to recreate key aspects of the application service group.

To add resources to the service group

1. In Cluster Explorer, click the **Service Group** tab in the left pane, click the application service group and click the **Resources** tab in the right pane.
2. Right-click the resource at the top of the tree, select **Copy > Self and Child Nodes**.
3. In the left pane, click the fire drill service group.
4. Right-click the right pane, and click **Paste**.
5. In the Name Clashes dialog box, specify a way for the resource names to be modified, for example, insert an FD_ prefix. Click **Apply**.
6. Click **OK**.

Configuring resources for fire drill service group

Edit the resources in the fire drill service group so they work properly with the duplicated data. The attributes must be modified to reflect the configuration at the remote site. Bringing the service group online without modifying resource attributes is likely to result in a cluster fault and interruption in service.

To configure the fire drill service group

1. In Cluster Explorer, click the **Service Group** tab in the left pane.
2. Click the fire drill service group in the left pane and click the **Resources** tab in the right pane.
3. Right-click the EVACA resource and click **Delete**.

4 Add a resource of type EVACASnap and configure its attributes.

5 Right-click the resource to be edited and click **View > Properties View**. If a resource to be edited does not appear in the pane, click **Show All Attributes**.

6 Edit attributes to reflect the configuration at the remote site. For example, change the Mount resources so that they point to the volumes that are used in the fire drill service group.

Enabling the FireDrill attribute

You must edit certain resource types so they are FireDrill-enabled. Making a resource type FireDrill-enabled changes the way that VCS checks for concurrency violations. Typically, when FireDrill is not enabled, resources cannot come online on more than one node in a cluster at a time. This behavior prevents multiple nodes from using a single resource or from answering client requests. Fire drill service groups do not interact with outside clients or with other instances of resources. They can safely come online even when the application service group is online.

Typically, you would enable the FireDrill attribute for the resource type that is used to configure the agent. For example, in a service group monitoring Oracle, enable the FireDrill attribute for the Oracle resource type.

To enable the FireDrill attribute

1 In Cluster Explorer, click the Types tab in the left pane, right-click the type to be edited, and click **View > Properties View**.

2 Click **Show All Attributes**.

3 Double click **FireDrill**.

4 In the Edit Attribute dialog box, enable **FireDrill** as required, and click **OK**.

5 Repeat the process of enabling the FireDrill attribute for all required resource types.

Verifying a successful fire drill

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

To verify a successful fire drill

1. Bring the fire drill service group online on a node that does not have the application running. Verify that the fire drill service group comes online.

   This action validates your disaster recovery configuration. The production service group can fail over to the secondary site in the event of an actual failure (disaster) at the primary site.

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

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

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

Sample configuration for a fire drill service group

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

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

```
EVACASnap oradg_fd {
TargetResName = "ora_evaca"
}
```

Index