Symantec™ Cluster Server Agent for IBM SVCCopyServices Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

5.0

June 2014

Symantec

Symantec Cluster Server Agent for IBM SVCCopyServices 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: 5.0.13.0

Document version: 5.0.13.0.0

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 website at the following URL:

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

https://sort.symantec.com/documents

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Contents

Chapter 1

Introducing the Symantec agent for IBM SVCCopyServices

This chapter includes the following topics:

About the agent for IBM SVCCopyServices

The Symantec High Availability agent for IBM SVCCopyServices manages replication relationships and consistency groups that are defined on SVC clusters. An SVC cluster brings storage devices together in a virtual pool to make all storage appear as one logical device to centrally manage and to allocate capacity as needed.

Each resource managed by the agent manages one replication relationship or one consistency group defined on a specific SVC cluster. The agent supports inter-cluster replication relationships. The agent does not support intra-cluster replication relationships or intra-cluster consistency groups.

The attributes of the resource managed by the SVCCopyServices agent contain the necessary information about the replication relationship or consistency group managed by the resource. For example, the SVC cluster IP address that is used to communicate with the SVC cluster; the absolute path of the SSH identity key file

location, and the absolute path of the SSH binary required for communicating with the SVC cluster.

The SVCCopyServices agent supports MetroMirror (synchronous replication) and Global Mirror (asynchronous replication).

Note: The SVCCopyServices agent also supports IBM Storwize V7000.

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 information on the software versions that the agent for IBM SVCCopyServices supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Supported hardware for IBM SVCCopyServices

The agent also supports SSH access to SVC.

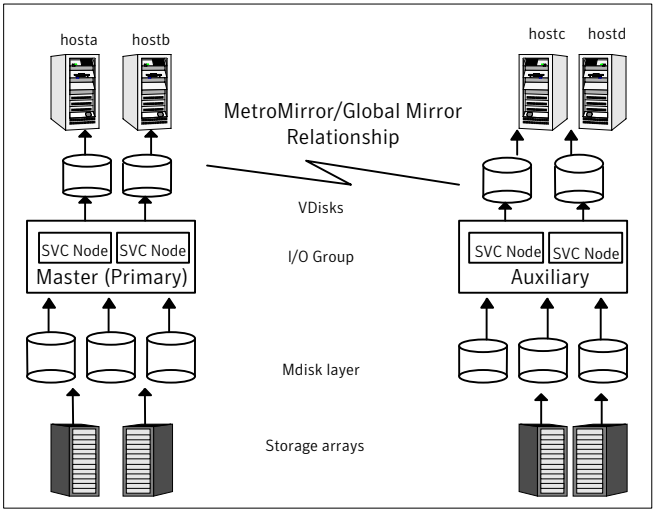
In environments using Symantec Storage Foundation for Oracle RAC, the arrays must support SCSI-3 persistent reservations.

Note: Refer to the IBM SVC documentation for more information on the distance limitations of the SVC metro mirror and global mirror configuration.

Typical IBM SVCCopyServices setup in a VCS cluster

Figure 1-1 displays a typical setup in a SVCCopyServices environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a SVCCopyServices environment typically consists of the following hardware infrastructure:

- 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 array.
- In the SVC cluster, one node acts as the point of contact or the preferred node. Each SVC cluster has a preferred node, through which replication occurs across the fiber.
- To access an SVC cluster from a host, you need an SSH identity file on that host. The SVCCopyServices agent assumes that that the SVC cluster has the information about the host and the public key (generated as a counterpart of the private key on the host) has been uploaded to the SVC cluster. This ensures that the SVC cluster can identify the host from which the agent invokes the SVC commands via SSH.
- In parallel applications like Symantec Storage Foundation for Oracle RAC, all hosts that are attached to the same array must be part of the same GAB membership. Symantec Storage Foundation for Oracle RAC is supported with SVC only in a global cluster environment and not in a replicated data cluster environment.

SVCCopyServices agent functions

The VCS agent for IBM SVCCopyServices manages the replication relationships or consistency groups that are defined on an SVC cluster.

The agent performs the following functions:

online	If the state of all local devices is read-write enabled, the agent creates a lock file on the local host to indicate that the resource is online. See "About the SVCCopyServices agent's online function" on page 13.
offline	The agent removes the lock file that was created for the resource by the online function. The agent does not run any SVCCopyServices commands because taking the resource offline does not indicate that the direction of the replication needs to be reversed or even that the replication should be stopped.
monitor	Verifies the existence of the lock file to determine the resource status. If the lock file exists, the agent reports the status of the resource as online. If the lock file does not exist, the agent reports the status of the resource as offline.
clean	The agent removes the lock file from the local host. The agent does not run any SVCCopyServices commands because taking the resource offline does not indicate that the direction of the replication needs to be reversed or even that the replication should be stopped.
action / update	The update action is invoked to resync the SVC disks at the primary site with the up to date data from the secondary site. A need to resync the data arises when the agent brings the SVCCopyServices resource online on the secondary and the replication is in a stopped or disconnected state. The action updates and resynchronizes the differences in the data between the primary and secondary sites. It allows the user to determine which site should be maintained as the primary site in the replication and updates it with the data from the secondary site. The update action supports the following commands: ■ `startrcrelationship` ■ `startrcconsistgrp` The action needs one argument i.e. the SVC cluster (master or auxiliary) that the user wants to retain as the Primary. See "About the SVCCopyServices agent's update action function" on page 16.

action/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. If running the PreSwitch action fails, the failover should not occur. This minimizes the application downtime and data loss . For more information on the PreSwitch action and the PreSwitch feature in the VCS engine, refer to the *Symantec Cluster Server User's Guide.*
open	Removes the online lock file on the host where the entry point is called. This function prevents potential concurrency violation if the service group fails over to another node while this host is down. The agent does not remove the lock file if the agent was started after running the `hastop -force` command.
info	Reports the detailed status of the replication relationship or consistency group being monitored by the agent. See "About the SVCCopyServices agent's info function" on page 17.

About the SVCCopyServices agent's online function

If the local SVC cluster is the primary, the host has read/write access to the disks and the online entry point creates a lock file and exits.

If the local SVC cluster is not the primary, it may takeover the role of the primary in the replication. The takeover depends on the state of the relationship.

- Inconsistent Copying - In this state, the agent waits for the reminder of the online entry point time (before the online entry point times out) for the replication to move out of this state. If it does not move out of the inconsistent_copying state, the online entry point times out. Else, the online entry point takes an appropriate action based on the current state of the replication.
- Idling / Idling Disconnected - The online entry point exits without taking any action since neither of the SVC clusters is the primary and read-write access to the disks is enabled from both SVC clusters.
- Consistent Stopped - There are two possible scenarios in this state:
  When the primary and secondary are in sync and if StopTakeOver = 1: The online entry point runs the `switchrc` command to switch roles of the primary and secondary sites.

When the primary and secondary are not in sync and if StopTakeOver = 1: The online entry point runs the `stoprc` command with the `-access` option.

If the switch between the primary and secondary, or the `stoprc` command with the `-access` option is successful, the online entry point creates the lock file and exits.

If StopTakeover = 0, or if the `switchrc` command fails, or if the `stoprc` command with the `-access` option fails, the online entry point exits without creating the online lock file.

- Consistent Synchronized - The online entry point runs the `switchrc` command to switch the roles of replication.

  If the switch is successful, the online entry point creates the lock file, else the online entry point exits without creating the lock file.

- Consistent Disconnected - The online entry point takes action only if the attribute DisconnectTakeover = 1. If DisconnectTakeover = 1, the online entry point runs the `stoprc` command with the `-access` option.

  If the `stoprc` command is successful, then the online entry point creates the lock file and exits, else the online entry point exits without creating the lock file.

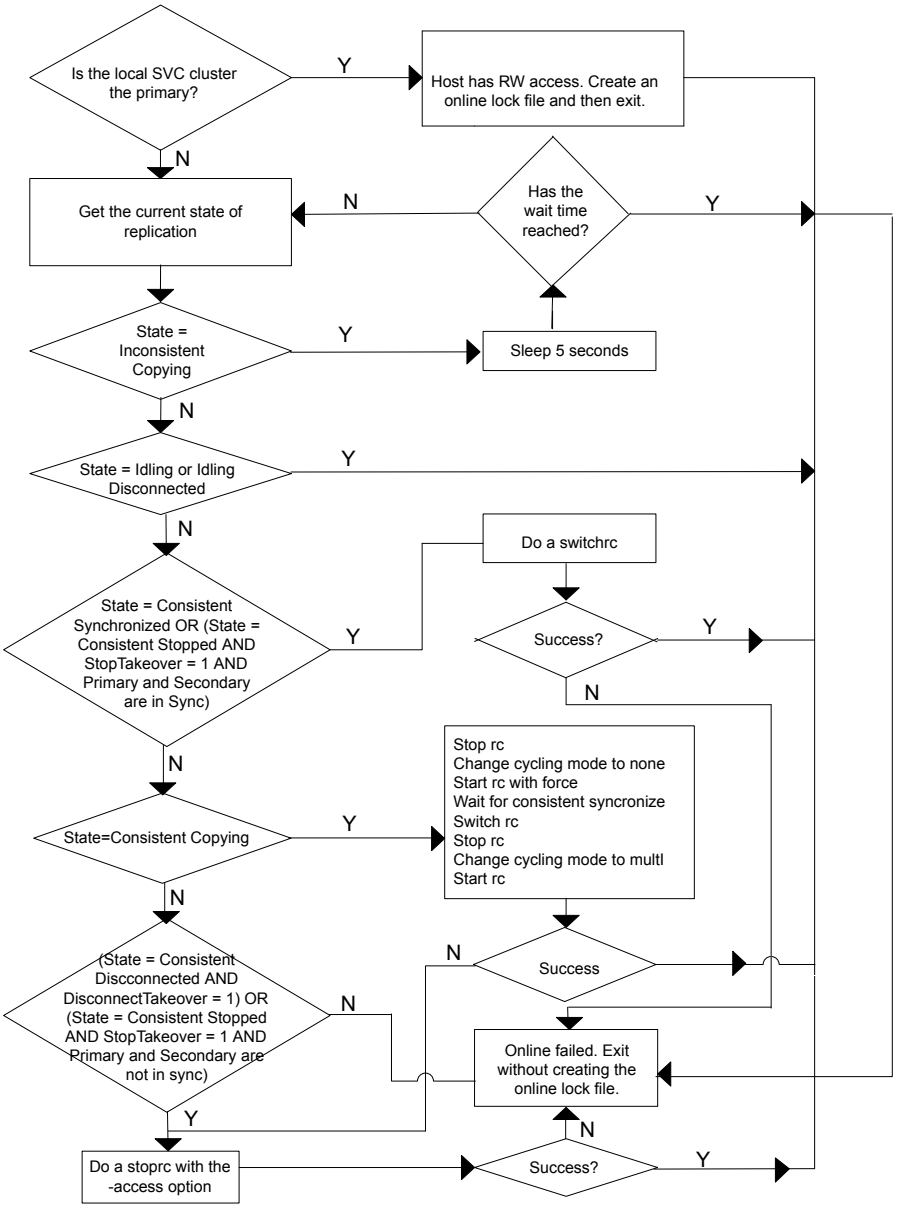
- Inconsistent Stopped / Inconsistent Disconnected - The online entry point does not do anything to enable read/write access to the local SVC cluster. The online entry point simply exits in these states.

- Consistent Copying - If the value of the CopyTakeover attribute is set to 1, the online entry point does the following:

  - Runs the `stoprc` command.
  - Changes the cycling mode to none.
  - Runs the `startrc` command with the `-force` option.
  - Waits for the state to change to consistent_synchronized.
  - Runs the `switchrc` command to change the direction of replication.
  - Runs the `stoprc` command.
  - Changes the cycling mode back to multi.
  - Runs the `startrc` command.

  If these actions fail, the online entry point runs the `stoprc` command with the `-access` option. If the `stoprc` command is successful, the online entry point creates the lock file and exits. If the `stoprc` command fails, the online entry point exits without creating the lock file.

Figure 1-2 The algorithm for the online entry point



About the SVCCopyServices agent's update action function

The update action is invoked when the agent brings the SVCCopyServices resource online on the secondary site. It resynchronizes the data between the primary and secondary sites.

Warning: Symantec recommends that the update action is run only when the resource is offline on both the primary and secondary sites.

The action requires exactly one argument i.e. the SVC cluster (master or auxiliary), which the user wants to retain as the primary. Alternately, the action requires no arguments, in which case the existing primary is retained. However, if you do not specify the direction of replication, there is a possibility of data corruption.

- Idling / Idling Disconnected - In these states, there is no primary defined for the replication relationship or the consistency group. The update action expects exactly one argument i.e. the SVC cluster that the user wants to retain as the primary (one of master or auxiliary) for the replication relationship or the consistency group. The action fails with an appropriate error message if any other value is used. The update action starts the replication by specifying the primary.

  For example: Assume that the application is defined by the global service group, grp_oradb and the replication resource in this global service group is defined by the SVCCopyServices resource svc_mmrel. If the replication relationship managed by the resource svc_mmrel is in the idling or idling_disconnected state:

  - Ensure that the application global service group grp_oradb is offline on all the clusters (assuming that the user wants to make the master SVC cluster the primary for the relationship).
  - Then, start the update action for svc_mmrel on system hosta using the following command: `hares -action svc_mmrel update -actionargs master -sys hosta`

- Consistent Stopped / Consistent Disconnected /Consistent Copying- There is a primary already defined for the replication or the consistency group. The update action expects no arguments. In this state, the action simply starts the replication and ignores any argument that may be used. The direction of the replication remains unchanged.

  For example: Assume that the application is defined by the global service group, grp_oradb and the replication resource in this global service group is defined by the SVCCopyServices resource svc_mmrel. If the replication relationship managed by the resource svc_mmrel is in the consistent_stopped, consistent_disconnected, or consistent_copying state:

- Ensure that the application global service group grp_oradb is offline on all the clusters.
- Then, start the update action for svc_mmrel on system hosta using the following command: `hares -action svc_mmrel update -sys hosta.`

When the primary and secondary are not in sync, the update action uses the `-force` flag to start the replication.

Symantec recommends that the update action is run only after the status of the replication changes to online. If the update action is run as soon as the link is restored, it may fail because the status of the replication is io_channel_offline.

About the SVCCopyServices agent's info function

The info entry point captures the entire output from `svcinfo lsrcrelationship` or the `svcinfo lsrcconsistgrp` for the replication relationship or consistency group monitored by the SVCCopyServices resource.

The output updates as the value of the ReplicationStatus key in the ResourceInfo attribute for the SVCCopyServices resource.

To view the current replication status as stored in the ResourceInfo attribute on system hosta, use the command: `hares -value svc_mmrel ResourceInfo -sys hosta.`

When the resource faults or goes offline, the ResourceInfo attribute for that resource is marked as stale. This indicates that the value in the ResourceInfo attribute is not the latest information but from some time in the past. The TS key in the attribute has the timestamp of when the ResourceInfo was last modified. Therefore, it is likely that the command `svcinfo lsrcrelationship` runs on the SVC cluster and results in a different output from what is stored in the ResourceInfo attribute.

The info entry point for a resource does not get invoked on a system where the resource is not currently online.

Note: The attributes ActionTimeout and InfoTimeout for the action and info entry points do not influence the SVCCopyServices agent. The agent always allows the action and info entry points to run.

Chapter 2

Installing and removing the agent for IBM SVCCopyServices

This chapter includes the following topics:

Before you install the agent for IBM SVCCopyServices

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

Set up replication and the required hardware infrastructure.

See "Typical IBM SVCCopyServices setup in a VCS cluster" on page 10.

Installing the agent for IBM SVCCopyServices

You must install the IBM SVCCopyServices agent on each node in the cluster. In global cluster environments, install the agent on each node in each cluster.

These instructions assume that you have already installed VCS or SF for Oracle RAC.

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/svccopyservices_agent/`*`agent_version`*`/pkgs/`
HP-UX (PA)	`cd1/hpux/generic/vcs/replication/svccopyservices_agent/`*`agent_version`*`/PA/depot/`
HP-UX (IA)	`cd1/hpux/generic/vcs/replication/svccopyservices_agent/`*`agent_version`*`/IA/depot`
Linux	`cd1/linux/generic/vcs/replication/svccopyservices_agent/`*`agent_version`*`/rpms/`
Solaris	`cd1/solaris/dist_arch/vcs/replication/svccopyservices_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 VRTSvcssvc.rte.bff VRTSvcssvc.rte`
HP-UX (IA/PA)	`# swinstall -s 'pwd' VRTSvcssvc`
Linux	`# rpm -ihv \` `VRTSvcssvc-`*`AgentVersion`*`-Linux_GENERIC.noarch.rpm`
Solaris	`# pkgadd -d . VRTSvcssvc`

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

Upgrading the agent for IBM SVCCopyServices

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 IBM SVCCopyServices" on page 20.

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

   See "Installing the agent for IBM SVCCopyServices" on page 18.

5. Copy the file SVCCopyServicesTypes.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 IBM SVCCopyServices

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 VRTSvcssvc.rte`
HP-UX	`# swremove VRTSvcssvc`
Linux	`# rpm -e VRTSvcssvc`
Solaris	`# pkgrm VRTSvcssvc`

Chapter 3

Configuring the agent for IBM SVCCopyServices

This chapter includes the following topics:

Before you configure the agent for IBM SVCCopyServices

Before you configure the agent, review the following information:

- Set up the SSH identity file on the VCS hosts prior to configuring the service group. Use the SSH keygen, if required. Generate a public and private key pair using the ssh-keygen utility. Copy the public key on the SVC cluster.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical IBM SVCCopyServices 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 22.

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

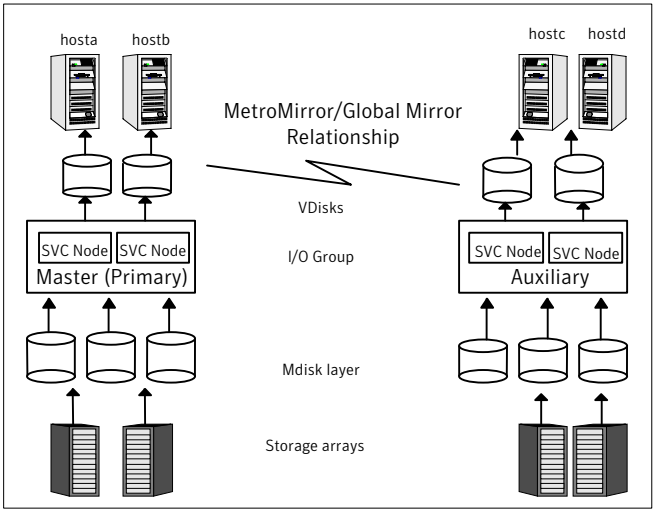
In a replicated data cluster, you can prevent unnecessary SVCCopyServices failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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

Figure 3-1 depicts a sample configuration where hosta and hostb are in one system zone, and hostc and hostd are in another system zone.

Use the SystemZones attribute to create these zones.

Figure 3-1 Example system zone configuration



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

About preventing split-brain

Split-brain occurs when all heartbeat links between the primary and secondary hosts are cut. In this situation, each side mistakenly assumes that the other side is down. You can minimize the effects of split-brain by ensuring that the cluster

heartbeat links pass through a similar physical infrastructure as the replication links. When you ensure that both pass through the same infrastructure, if one breaks, so does the other.

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

Configuration concepts for the SVCCopyServices agent

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

Resource type definition for the SVCCopyServices agent

Following is the resource type definition for the SVCCopyServices agent:

```
type SVCCopyServices (
        static keylist SupportedActions = { update, PreSwitch }
        static int OfflineMonitorInterval = 0
        static int OnlineTimeout = 600
        static int OpenTimeout = 180
        static int RestartLimit = 1
        static str ArgList[] = { SSHBinary, SSHPathToIDFile,
        GroupName, IsConsistencyGroup, SVCClusterIP, SVCUserName,
        DisconnectTakeover, StopTakeover, CopyTakeover }
        str SSHBinary = "/usr/bin/ssh"
        str SSHPathToIDFile
        str GroupName
        int IsConsistencyGroup = 1
        str SVCClusterIP
        str SVCUserName = "admin"
        int DisconnectTakeover = 0
        int StopTakeover = 0
        int CopyTakeover = 0
        temp str VCSResLock
)
```

Attribute definitions for the SVCCopyServices agent

The descriptions of the agent attributes are as follows:

GroupName	Name of the replication relationship or consistency group that is managed by the agent. Type-dimension: string-scalar
IsConsistency Group	Indicates whether the value specified in the GroupName attribute is the name of a single replication relationship or of a consistency group consisting of several replication relationships. Attribute value is either 0 or 1. Default is 1. Type-dimension: integer-scalar
SSHBinary	Contains the absolute path to the SSH binary. SSH is the mode of communication with the SVC cluster that is connected to the node. Default is "/usr/bin/ssh". Type-dimension: string-scalar
SSHPathToID File	Contains the absolute path to the identity file used for authenticating the host with the SVC cluster. The corresponding public key must be uploaded on the SVC cluster so that the SVC cluster can correctly authenticate the host. Type-dimension: string-scalar
SVCClusterIP	The IP address or name that is used to manage the SVC cluster in the dot notation. The agent uses this IP address to communicate with the SVC cluster. Type-dimension: string-scalar
SVCUserName	User name that authenticates the SSH connection with the SVC cluster. Default is admin. Type-dimension: string-scalar

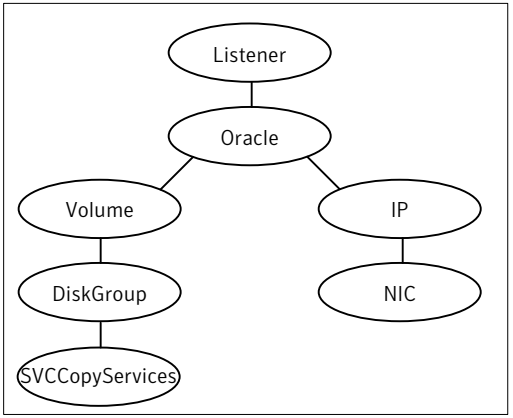
StopTakeover	Determines whether the agent makes read-write access available to the host when the replication is in a stopped state (i.e. consistent_stopped). The status of the replication goes into a stopped state when the user fires the `stoprcrelationship` or the `stoprcconsistgrp` command. Thus, no replication occurs between the primary and secondary SVC clusters. Attribute value is either 0 or 1. Default value is 0. If it is set to 1, there is a possibility for data loss, if after the replication was stopped, the application continues to write data on the Primary. Thus, when the agent enables read/write access on the secondary SVC cluster, the secondary SVC cluster does not have up-to-date data on it. The possible stopped states are: inconsistent_stopped consistent_stopped When the state of the replication is consistent_stopped and StopTakeover = 1 , the agent enables read-write access for the SVC cluster. When the state of the replication is inconsistent_stopped, the agent does not enable read-write access for the SVC cluster. Type-dimension: integer-scalar
Disconnect Takeover	Determines whether the agent makes read-write access available to the host when the replication is in a disconnected state (i.e. consistent_disconnected). The status of the replication goes into a disconnected state when the primary and secondary SVC clusters lose communication with each other. Thus, no replication occurs between the primary and secondary SVC clusters. Attribute value is either 0 or 1. Default is 0. The possible disconnected states are: idling_disconnected inconsistent_disconnected consistent_disconnected When the state of the replication is consistent_disconnected and DisconnectTakeover = 1, then the agent enables read/write access for the SVC cluster.When the state of the replication is idling_disconnected, the agent does not enable read-write access for the SVC cluster. Type-dimension: integer-scalar

CopyTakeover	Determines whether the agent makes read-write access available to the host when the replication is in a consistent_copying state. The agent attempts to synchronize the data before making read/write access available. The status of the replication is in a consistent_copying state when the multi cycling mode is used. In this mode, the data is always consistent, but can lag behind. The value of this attribute can be set to 0 or 1. If it is set to 1, and the application continues to write data on the primary even after replication was stopped, there is a possibility of data loss. In such a case, when the agent enables read/write access on the secondary SVC cluster, the secondary SVC cluster does not have the most current data. Type-dimension: integer-scalar Default value: 0
VCSResLock	This attribute is used for internal purpose. Type-dimension: temporary string

Sample configuration for the IBM SVCCopyServices agent

Figure 3-2 shows a dependency graph of a VCS service group that has a resource of type SVCCopyServices.

Figure 3-2 VCS service group with resource type SVCCopyServices



The sample SVCCopyServices resource configuration to manage a relationship is:

```
SVCCopyServices oradata_svc_relationship
                (
                GroupName = oradata_svc_relationship
```

```
    SVCClusterIP = "<IP address>"
    IsConsistencyGroup = 0
    )
```

The sample SVCCopyServices resource configuration to manage a consistency group is:

```
SVCCopyServices oradata_svc_consistency_grp
               (
                GroupName = oradata_svc_consistency_grp
                SVCClusterIP = "<IP address>"
               )
```

Configuring the agent for IBM SVCCopyServices

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

- Converting their devices to SVCCopyServices devices
- Synchronizing the devices
- Adding the IBM SVCCopyServices agent to the service group

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

Note: You must not change the replication state of devices primary to secondary and viceversa, outside of a VCS setup. The agent for IBM SVCCopyServices fails to detect a change in the replication state if the role reversal is done externally, and RoleMonitor is disabled.

Configuring the agent manually in a global cluster

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

To configure the agent in a global cluster

1. Start Cluster Manager (Java Console) and log on to the cluster.
2. Add a resource of type SVCCopyServices at the bottom of the service group.
3. Configure the attributes of the SVCCopyServices resource.
4. If the service group is not configured as a global service group, configure the service group using the Global Group Configuration Wizard.

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

5 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.

6 Repeat step 2 through step 5 for each service group in each cluster that uses replicated data.

Configuring the agent in an SF for Oracle RAC environment or Storage Foundation Cluster File System (SFCFS) environment

To configure the agent to manage the volumes that Symantec Storage Foundation for Oracle RAC uses, do the following:

To configure the agent in a Storage Foundation for Oracle RAC or SFCFS environment:

1 Configure the SupportedActions attribute for the CVMVolDg resource.

2 Add the following keys to the list: import, deport, vxdctlenable.

3 Use the following commands to add the entry points to the CVMVolDg resource:

```
haconf -makerw

hatype -modify CVMVolDg SupportedActions

import deport vxdctlenable

haconf -dump -makero
```

Note that SupportedActions is a resource type attribute and defines a list of action tokens for the resource.

Chapter 4

Managing and testing clustering support for IBM SVCCopyServices

This chapter includes the following topics:

Typical test setup for the IBM SVCCopyServices agent

A typical test environment includes the following characteristics:

- A master SVC cluster is attached to the storage at the back end and the application hosts at the front end.
- An auxiliary SVC cluster is attached to the storage at the back end and the application hosts at the front end.
- Two hosts (hosta and hostb) are attached to the master SVC cluster.
- Two hosts (hostc and hostd) are attached to the auxiliary SVC cluster.

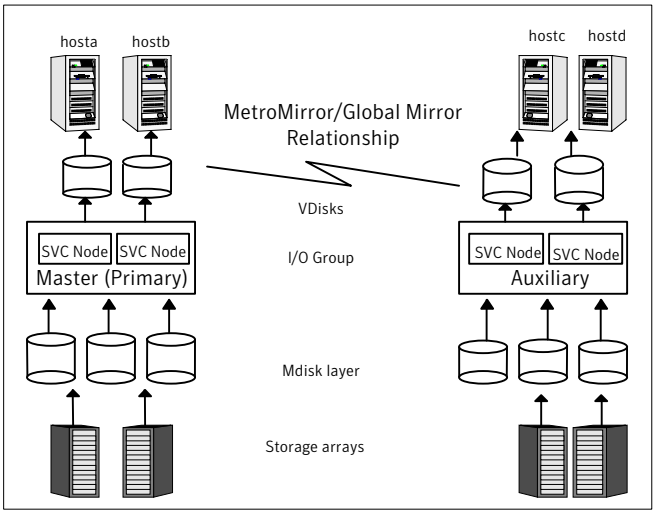
- SSH configuration is established on hosts (hosta and hostb) and the master SVC cluster so that the hosts (hosta and hostb) can communicate via SSH with the master SVC cluster.
- SSH configuration on hosts (hostc and hostd) and the auxiliary SVC cluster so that the hosts (hostc and hostd) can communicate via SSH with the auxiliary SVC cluster.
- The application runs on hosta which is connected to the master SVC cluster, also the primary for the replication relationship being managed by the IBM SVCCopyServices agent.

To verify that the host can communicate with the SVC cluster via SSH, run the following command from the host:

```
ssh -1<username> -i <path_to_ssh_id_file_on_host> <SVC ClusterName
or IP address> <SVC command>
```

Figure 4-1 depicts a typical test environment.

Figure 4-1 Typical test setup



Testing service group migration

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

To perform the service group migration test

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

   Migrate the service group to a host (hostb) that is attached to the primary SVC cluster.

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

   Migrate the service group to a host (hostc) that is attached to a different SVC cluster (auxiliary SVC cluster).

3. Click **Switch To**, and click the system (hostc) that is connected to the auxiliary SVC cluster.

   The service group comes online on hostc. The state of the replication stays online but the auxiliary SVC cluster now becomes the primary.

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

   Migrate the service group back to its original host.

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

   The service group comes online on hosta that is attached to the master SVC cluster. The state of the replication is online and the master SVC cluster now becomes the primary again.

Note: If the replication stops or the replication link is disconnected, set the DisconnectTakeover attribute to 1 for a successful failback between the primary and secondary.

Testing host failure

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

To perform the host failure test

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

   The application fails over to hostb, also located in the primary site. The IBM SVCCopyServices performs no operation on the online entry point as hostb is attached to the primary SVC cluster.

2. Halt or shut down hostb.

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

   The online entry point of the IBM SVCCopyServices attempts to switch roles of replication or at least enable read write access to the storage on the secondary so that the application comes up successfully on the secondary site.

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

Testing cluster failure

In this scenario, the primary cluster fails i.e. the nodes in the cluster are shut down.

To perform the cluster failure test

1. Halt or shut down the master i.e. primary, where the application runs (hosta).
2. If you cannot halt hosta, disable all the ports on the switch or switches connected to the SVC cluster.

   Wait for a few minutes for the VCS agents to detect the loss of storage connectivity and for VCS to initiate the service group failover.

   The service group fails to come online in the primary site.
3. Set the attribute DisconnectTakeOver = 1 to bring the service group online on the secondary site.

   In a replicated data cluster, the service group automatically fails over to the secondary site (hostc or hostd) depending upon the FailOverPolicy in the cluster.

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

Performing a disaster test

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

To perform a disaster test

1 Shut down all hosts, the SVC cluster, and the storage arrays connected to the backend of the SVC cluster.

If you cannot shut down the storage arrays or the SVC cluster, disconnect the replication link between the SVC clusters on the two sites. The action mimics a disaster scenario to the secondary site.

2 VCS fails over to the hosts on the secondary site (hostc or hostd).

Performing the failback test

You can set up your cluster for a failback test.

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

To perform a failback test

1 Reconnect the replication link and reboot the hosts on the primary site.

2 Take the service group offline.

3 Manually resynchronize the data between the primary and secondary sites.

If the current primary is retained as the primary for the replication relationship and the replication is not in a stopped state, stop the replication manually.

- Use the `stoprcrelationship` or the `stoprcconsistgrp` command, without the `-access` option.
- Use the `startrcrelationship` or the `startrcconsistgrp` command with the `-force` option on the SVC cluster that the user wants to retain as primary.
- Alternatively, use the update action entry point with no arguments specified.

If you change the primary for the replication relationship, stop the replication manually (if it is not stopped already).

- Enable read / write access on both SVC clusters by using the `stoprcrelationship` or the `stoprcconsistgrp` command with the `-access` option.
- Use the `startrcrelationship` or the `startrcconsistgrp` command with both the `-force` and `-primary` options.

- Alternatively, use the update action entry point with exactly one argument that is the SVC cluster, which the user retains as primary.

4 After the resynchronization is complete, migrate the application back to the original primary side.

Failure scenarios for IBM SVCCopyServices

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

Site disaster

In a total site failure, all hosts, the SVC cluster, and storage arrays are completely disabled, either temporarily or permanently.

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

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

All host or all application failure

If all hosts on the primary side are disabled or if the application cannot start successfully on any primary host, the service group fails over.

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

In replicated data cluster environments, site failure is detected the same way as a total host failure, that is, the loss of all LLT heartbeats. This type of failure is communicated by the VCS engine to the other site.

In a global cluster environment, VCS detects the failure by the loss of the ICMP heartbeat between the clusters. This type of failure is communicated by the wac process to the other site.

Cluster failure

If all hosts on the primary side are disabled or if the application cannot start successfully on any primary host, the replication relationship transitions to a disconnected state.

Any VCS agent, DiskGroup, Volume or Mount that monitors the storage infrastructure detects the loss of storage connectivity.

When VCS detects a fault in one of the storage resources (DiskGroup, Volume or Mount), the service group is taken offline and declared faulted on hosta.

VCS initiates a failover to hostb, which is also in the primary site and connected to the same SVC cluster as hosta.

The service group fails to come online on hostb since the SVC cluster is shut down.

The service group is brought online on the secondary site (either on hostc or hostd), only if the DisconnectTakeover attribute is set to 1.

If the attribute DisconnectTakeover = 1, there is a possibility of data loss since the replication is in a disconnected state and indicates that the data on the primary and secondary sites may not be in sync.

Warning: Symantec recommends caution when setting the DisconnectTakeover to 1 or StopTakeover to 1 for the replication resource.

Replication link failure

IBM SVCCopyServices does not monitor the replication link status and cannot detect link failures. When the replication link between the primary and secondary cluster fails, VCS takes no action. If the replication relationship does not stop after the link failure, the two SVC clusters are automatically resynchronized after the replication link is reconnected.

Split-brain in a SVCCopyServices environment

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

The user must resynchronize the data between the two clusters manually.

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

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 IBM SVCCopyServices, the SVCCopyServicesSnap 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 configurations

VCS supports the following fire drill configurations for the agent:

Gold

Runs the fire drill on a snapshot of the target array. The replicated device keeps receiving writes from the primary.

Symantec recommends this configuration because it does not affect production recovery.

In the Gold configuration, VCS does the following:

- Takes a snapshot of the target array on snapshot LUNs using FlashCopy.
- Modifies the disk group name in the snapshot.
- Brings the fire drill service group online using the snapshot data.

Silver

VCS takes a snapshot, but does not run the fire drill on the snapshot data. VCS breaks replication and runs the fire drill on the replicated target device.

In the Silver configuration, VCS does the following:

- Suspends replication.
- Takes a snapshot of the target array on snapshot LUNs using FlashCopy.
- Modifies the disk group name in the replicated target device.
- Brings the fire drill service group online using the data on the target array; the agent does not use the snapshot data for the fire drill.

Note: After running the silver fire drill for SVCCopyServices at the disaster recovery site, the replication target is resynchronized from the primary. After the resynchronization is complete, you must discard the snapshot to be able to bring the application service group online at the recovery site. If disaster happens before the resynchronization is complete, you must restore the replication target from the snapshot.

Bronze

VCS breaks replication and runs the fire drill test on the replicated target. VCS does not take a snapshot in this configuration.

If a disaster occurs while resynching data after the test, it may result in inconsistent data as there is no snapshot data.

In the Bronze configuration, VCS does the following:

- Suspends replication.
- Modifies the disk group name while importing.

About the SVCCopyServicesSnap agent

The SVCCopyServicesSnap agent is the fire drill agent for IBM SVCCopyServices.

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

The SVCCopyServicesSnap agent supports fire drill for storage devices that are managed using Veritas Volume Manager (VxVM). Additionally, on AIX, the SVCCopyServicesSnap agent supports LVM for Gold fire drill configurations. See "Configuring the agent for LVM support" on page 39.

Configuring the agent for LVM support

To configure the agent for LVM support:

1. Run the following command to set the Physical Volume Identifier (PVID) for all the FlashCopy disks:

   ```
   chdev -l <hdisk#> -a pv=yes
   ```

2. Run the `lspv` command to ensure that the output shows the PVID for the FlashCopy disks on all nodes of the cluster.
3. Create a Volume Group comprising of FlashCopy disks.
4. Vary on the Volume Group on any one node.
5. Run the following command:

   ```
   hares -action <SVCCopyServicesSnap resource name> getfcdisks
   -actionargs <FlashCopy Volume Group name> -sys
   <VCS system where the Volume Group is active>
   ```

6. The getfcdisks action function exports the FlashCopy Volume Group. The SVCCopyServicesSnap fire drill agent recreates the Volume Group during fire drill.

SVCCopyServicesSnap agent functions

The SVCCopyServicesSnap agent performs the following functions:

online	■ For Gold and Silver configurations, takes a local snapshot of the target LUN. ■ For Gold configuration,takes the fire drill service group online by mounting the snapshot LUN. ■ For Bronze and Silver configurations, takes the fire drill service group online by mounting the target LUN. ■ For Bronze and Silver configurations, suspends replication between the source and the target arrays. ■ Creates a lock file to indicate that the resource is online.
offline	■ Resumes the replication between the source and the target arrays. ■ 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	■ Resumes the replication between the source and the target arrays. ■ Removes the lock file created by the online function.
action/getfcdisks	Gets a list of target FlashCopy disks based on the Volume Group that is imported with FlashCopy target disks. This action entry point exports the Volume Group after successfully getting the (physical volume identifier (PVid) and disks required for fire drill. For more information on the role the getfcdisks action entry point plays when configuring the agent to support fire drill for LVM: See "Configuring the agent for LVM support" on page 39.

Resource type definition for the SVCCopyServicesSnap agent

Following is the resource type definition for the SVCCopyServicesSnap agent:

```
type SVCCopyServicesSnap (
        static keylist SupportedActions = { getfcdisks }
        static int MonitorInterval = 300
        static int OpenTimeout = 180
        static int NumThreads = 1
        static int OfflineMonitorInterval = 0
        static int OnlineTimeout = 6000
        static int RestartLimit = 1
        static str ArgList[] = { TargetResName, MountSnapshot,
```

```
UseSnapshot, RequireSnapshot, FCMapGroupName,
IsSpaceEfficientSnapshot }
str TargetResName
int MountSnapshot
int UseSnapshot
int RequireSnapshot
str FCMapGroupName
int IsSpaceEfficientSnapshot = 0
temp str Responsibility
temp str FDFile
)
```

Attribute definitions for the SVCCopyServicesSnap agent

To customize the behavior of the SVCCopyServicesSnap 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 SVCCopyServices resource if you want to take a snapshot of replicated data. Set this attribute to the name of the DiskGroup resource if the data is not replicated. For example, in a typical 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
UseSnapshot	Specifies whether the SVCCopyServicesSnap resource takes a local snapshot of the target array. Set this attribute to 1 Type-Dimension: integer-scalar See "About the Snapshot attributes" on page 42.

RequireSnapshot	Specifies whether the SVCCopyServicesSnap resource must take a snapshot before coming online. Set this attribute to 1 if you want the resource to come online only after it succeeds in taking a snapshot. Type-Dimension: integer-scalar **Note:** Set this attribute to 1 only if UseSnapshot is set to 1.
MountSnapshot	Specifies whether the resource uses the snapshot to bring the service group online. Set this attribute to 1. Type-Dimension: integer-scalar **Note:** Set this attribute to 1 only if UseSnapshot is set to 1.
FCMapGroupName	Name of the FlashCopy mapping or FlashCopy consistency group. If the target SVCCopyServices resource contains a consistency group, set FCMapGroupName to a flashcopy consistency group. If the target SVCCopyServices resource contains a relationship, set FCMapGroupName to a flashcopy mapping. This attribute is optional for Bronze configurations. Type-Dimension: string-scalar
IsSpaceEfficientSnapshot	Specifies whether the SVCCopyServices resource uses space-efficient snapshots. If you want space-efficient snapshots to be used for fire drill operations, set this attribute to 1. The SVCCopyServices resource can use space-efficient snapshots only if the snapshot target is thin-provisioned and copy rate is 0. **Note:** This attribute is applicable only to storage devices that are managed using Veritas Volume Manager (VxVM). Type-Dimension: integer-scalar

About the Snapshot attributes

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

Table 5-1 lists the snapshot attribute values for fire drill configurations:

Table 5-1 Snapshot attribute values for fire drill configurations

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

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

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 SVCCopyServices resource.
- Make sure the infrastructure to take snapshots is properly configured between the source and target arrays. This process involves associating FlashCopy mapping or consistency group and quiescing the application.
- If you plan to run a fire drill on SVCCopyServices devices, you must have a FlashCopy license.
- When you use the Gold or Silver configuration, make sure FlashCopy for IBM SVC is installed and configured at the target array.

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 46.

You can create the fire drill service group using one of the following methods:

- Cluster Manager (Java Console)
  See "Creating the fire drill service group using Cluster Manager (Java Console)" on page 44.

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' suffix. 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 SVCCopyServices resource and click **Delete**.
4. Add a resource of type SVCCopyServicesSnap 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 at the secondary site that does not have the application running.

   If the fire drill service group comes online, it action validates your disaster recovery configuration. The production service group can fail over to the secondary site in the event of an actual failure (disaster) at the primary site.
2. If the fire drill service group does not come online, review the VCS engine log for more information.
3. Take the fire drill offline after its functioning has been validated.

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

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 SVCCopyServicesSnap resource replaces the SVCCopyServices resource.

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

```
SVCCopyServicesSnap oradg_fd (
    TargetResName = oradg_cg
    MountSnapshot = 1
    UseSnapshot = 1
    RequireSnapshot = 1
    IsSpaceEfficientSnapshot = 1
    FCMapGroupName = fc_cg1
    )
```

Index

S

T

U