

# Veritas™ Cluster Server Agent for IBM SVC Copy Services Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

5.0

# Veritas Cluster Server Agent for IBM SVC Copy Services 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: 5.0.04.0

Document version: 5.0.04.0.0

## Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014

<http://www.symantec.com>

# Technical Support

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

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Contacting Technical Support

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

[http://www.symantec.com/business/support/assistance\\_care.jsp](http://www.symantec.com/business/support/assistance_care.jsp)

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

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

## Licensing and registration

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

Customer Service is available to assist with the following types of issues:

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

## Maintenance agreement resources

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

Asia-Pacific and Japan	<a href="mailto:contractsadmin@symantec.com">contractsadmin@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportolutions@symantec.com</a>

## Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

[www.symantec.com](http://www.symantec.com)

Select your country or language from the site index.

# Contents

Technical Support .....	4	
Chapter 1	Introducing the Veritas agent for IBM SVCCopyServices .....	9
	About the agent for IBM SVCCopyServices .....	9
	What's new in this release .....	10
	Supported software and hardware .....	10
	Typical IBM SVCCopyServices setup in a VCS cluster .....	11
	SVCCopyServices agent functions .....	13
	About the SVC Copy Services agent's online function .....	14
	About the SVC Copy Services agent's update action function .....	17
	About the SVC Copy Services agent's info function .....	18
Chapter 2	Installing and removing the agent for IBM SVCCopyServices .....	19
	Before you install the agent for SVCCopyServices .....	19
	Installing the agent for SVCCopyServices .....	19
	Upgrading the agent for SVCCopyServices .....	22
	Removing the agent for SVCCopyServices .....	23
Chapter 3	Configuring the agent for IBM SVCCopyServices .....	25
	Configuration concepts for the SVC Copy Services agent .....	25
	Resource type definition for the SVC CopyServices agent .....	25
	Attribute definitions for the SVC CopyServices agent .....	26
	Sample configuration for the IBMSVCCopyServices agent .....	28
	Before you configure the agent for SVCCopyServices .....	29
	About cluster heartbeats .....	30
	About configuring system zones in replicated data clusters .....	30
	About preventing split-brain .....	31
	Configuring the agent for SVCCopyServices .....	31
	Configuring the agent manually in a global cluster .....	32

Chapter 4	Managing and testing clustering support for IBM SVCCopyServices .....	33
	Typical test setup for the IBM SVCCopyServices agent .....	33
	Testing service group migration .....	34
	Testing host failure .....	35
	Testing cluster failure .....	36
	Performing a disaster test .....	37
	Performing the failback test .....	37
	Failure scenarios for IBM SVCCopyServices .....	38
	Site disaster .....	38
	All host or all application failure .....	38
	Cluster failure .....	38
	Replication link failure .....	39
	Split-brain in a SVCCopyServices environment .....	39
Chapter 5	Setting up a fire drill .....	41
	About fire drills .....	41
	Fire drill configurations .....	42
	About the SVCCopyServicesSnap agent .....	43
	SVCCopyServicesSnap agent functions .....	43
	Resource type definition for the SVCCopyServicesSnap agent .....	44
	Attribute definitions for the SVCCopyServicesSnap agent .....	45
	About the Snapshot attributes .....	46
	Sample configuration for a fire drill service group .....	46
	Before you configure the fire drill service group .....	47
	Configuring the fire drill service group .....	47
	Creating the fire drill service group using Cluster Manager (Java Console ) .....	48
	Verifying a successful fire drill .....	50
Index	.....	51

# Introducing the Veritas agent for IBM SVCCopyServices

This chapter includes the following topics:

- [About the agent for IBM SVCCopyServices](#)
- [What's new in this release](#)
- [Supported software and hardware](#)
- [Typical IBM SVCCopyServices setup in a VCS cluster](#)
- [SVCCopyServices agent functions](#)

## About the agent for IBM SVCCopyServices

The VCS enterprise 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 agent also supports parallel applications, such as Veritas Storage Foundation for Oracle RAC.

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

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

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

## What's new in this release

The Veritas agent for IBM SVCCopyServices includes the following new or enhanced features:

- The Veritas agent for IBM SVCCopyServices supports Veritas Storage Foundation for Oracle RAC in this release.

## Supported software and hardware

The agent for IBM SVCCopyServices supports the following software versions:

Veritas Cluster Server

- VCS 5.0 and 5.0 MP1 on AIX
- VCS 5.0 and 5.0 MP1 on HP-UX 11i v2
- VCS 5.0 and 5.0 MP1 on Red Hat Enterprise Linux
- VCS 5.0 and 5.0 MP1 on SUSE Linux Enterprise Server
- VCS 5.0 and 5.0 MP1 on Solaris SPARC

See *Veritas Cluster Server Release Notes* for more details on the supported architectures and the operating system versions.

- Veritas SF for Oracle RAC
- SF Oracle RAC 5.0 and 5.0 MP1 on AIX
  - SF Oracle RAC 5.0 and 5.0 MP1 on HP-UX 11i v2
  - SF Oracle RAC 5.0 and 5.0 MP1 on Red Hat Enterprise Linux
  - SF Oracle RAC 5.0 and 5.0 MP1 on SUSE Linux Enterprise Server
  - SF Oracle RAC 5.0 and 5.0 MP1 on Solaris SPARC

See *Veritas Storage Foundation for Oracle RAC Release Notes* for more details on the supported architectures and the operating system versions.

- Veritas Volume Manager
- VxVM 5.0 MP1  
On AIX, Symantec recommends using VxVM 5.0 MP1 RP3.

Firmware levels on the SVC cluster nodes 4.1.1.2 or higher

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

---

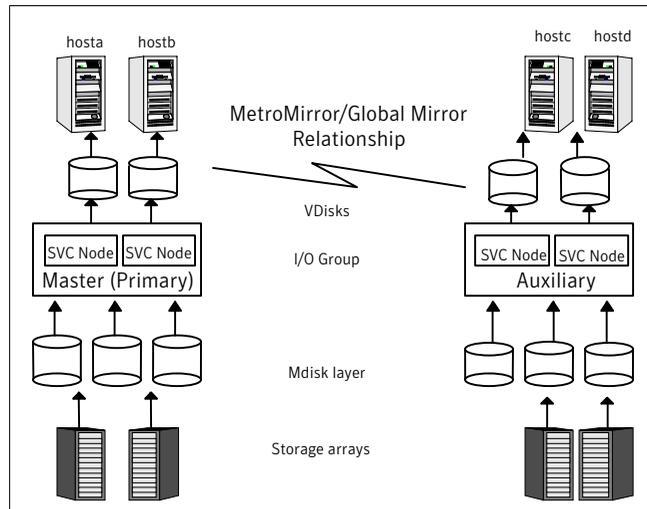
**Note:** Refer to the IBM SVC documentation for more information on the distance limitations of the SVC metro mirror and global mirror configuration.

---

## 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 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 Veritas Storage Foundation for Oracle RAC, all hosts that are attached to the same array must be part of the same GAB membership. Veritas 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	<p>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.</p> <p>See <a href="#">“About the SVC Copy Services agent’s online function”</a> on page 14.</p>
offline	<p>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.</p>
monitor	<p>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.</p>
clean	<p>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.</p>
action / update	<p>The update action is invoked when the agent brings the SVCCopyServices resource online on the secondary and the replication is in a stopped or disconnected state.</p> <p>The action updates and resynchronizes the differences in the data between the primary and secondary sites, when the SVCCopyServices resource is brought online on the secondary site.</p> <p>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.</p> <p>The update action supports the following commands:</p> <ul style="list-style-type: none"><li>■ starttrcrelationship</li><li>■ starttrcconsistgrp</li></ul> <p>The action needs one argument i.e. the SVC cluster (master or auxiliary) that the user wants to retain as the Primary.</p> <p>See <a href="#">“About the SVC Copy Services agent’s update action function”</a> on page 17.</p>

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 <code>hastop -force</code> command.
info	Reports the detailed status of the replication relationship or consistency group being monitored by the agent.  See <a href="#">“About the SVC Copy Services agent’s info function”</a> on page 18.

## About the SVC Copy Services 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 remainder 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.

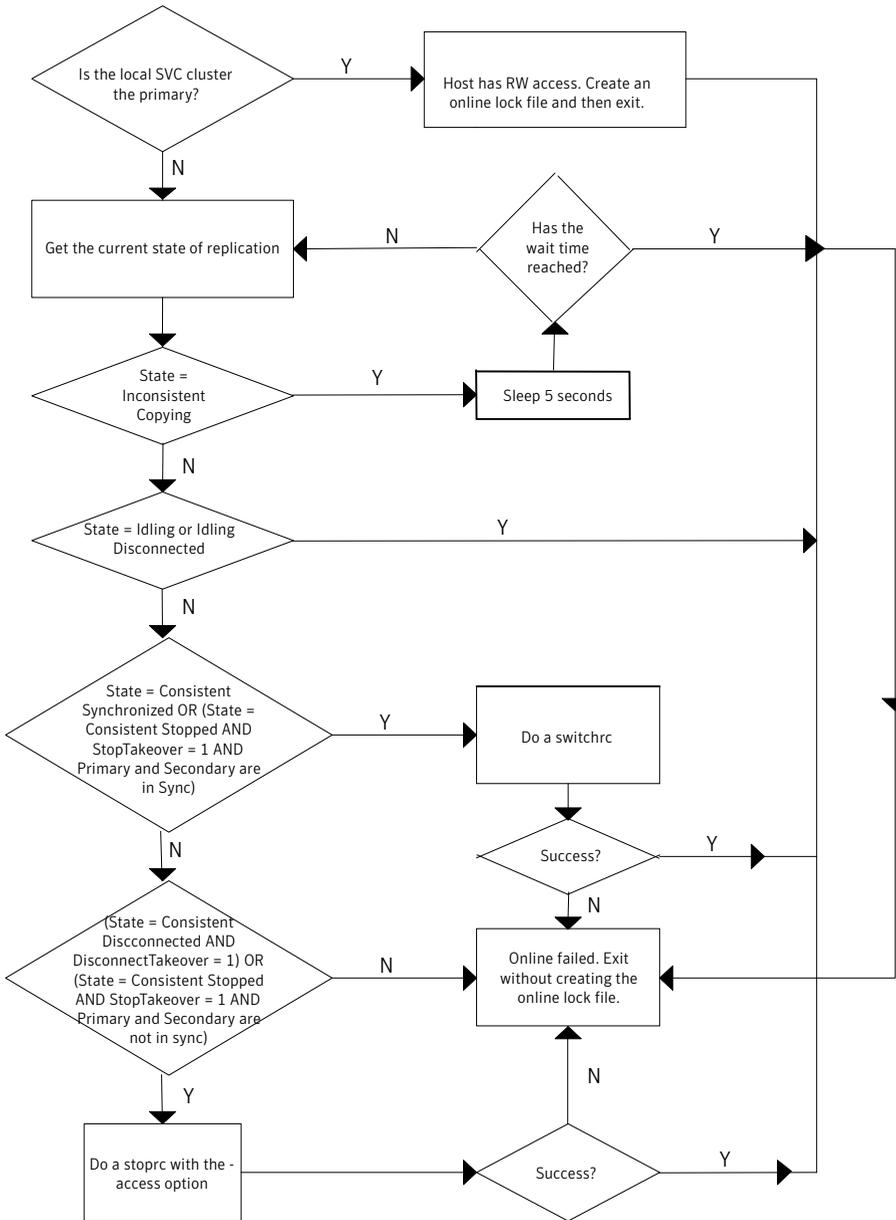
- Consistent Disconnected - The online entry point takes action only if the attribute `DisconnectTakeover = 1`. If `DisConnectTakeover = 1`, the online entry point runs the `stoprc` command with the `-access` option.

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.

See [Figure 1-2](#) on page 16.

**Figure 1-2** The algorithm for the online entry point



## About the SVC Copy Services 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.

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.

- **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 service group, `grp_oradb` and the replication resource in this 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 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 -action_args master -sys hosta.
```
- **Consistent Stopped / Consistent Disconnected** - 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 service group, `grp_oradb` and the replication resource in this group is defined by the SVCCopyServices resource `svc_mmrel`. If the replication relationship managed by the resource `svc_mmrel` is in the `consistent_stopped` or `consistent_disconnected` state:

- Ensure that the application 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 SVC Copy Services agent's info function

The info entry point captures the entire output from `svcinfolsrcrelationship` or the `svcinfolsrcconsistgrp` 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 `svcinfolsrcrelationship` 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.

---

# Installing and removing the agent for IBM SVCCopyServices

This chapter includes the following topics:

- [Before you install the agent for SVCCopyServices](#)
- [Installing the agent for SVCCopyServices](#)
- [Upgrading the agent for SVCCopyServices](#)
- [Removing the agent for SVCCopyServices](#)

## Before you install the agent for SVCCopyServices

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 IBM SVCCopyServices setup in a VCS cluster](#)” on page 11.

## Installing the agent for 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 on AIX systems

- 1 Determine the device access name of the disc drive.

```
# cd /dev  
# lsdev -C -c cdrom
```

The output resembles:

```
cd0 Available 10-60-00-4,0 16 Bit SCSI Multimedia CD-ROM Drive
```

In this example, the CD device access name is cd0.

- 2 Insert the disc into the system's drive.
- 3 Mount the disc.

```
# mkdir -p /cdrom  
# mount -V cdrfs -o ro /dev/cd0 /cdrom
```

- 4 Navigate to the location of the agent packages:

```
# cd /cdrom/aix/replication/svccopyservices_agent/version/pkg
```

The variable *version* represents the version of the agent.

- 5 Add the filesets for the software.

```
# installp -ac -d VRTSvcssvc.rte.bff VRTSvcssvc
```

### To install the agent on HP-UX systems

- 1 Insert the disc into the system's drive.
- 2 Create a mount point directory. For example, /cdrom. The directory must have read-write permissions.
- 3 Determine the block device file for the disc drive.

```
# ioscan -fnC disk
```

For example, the listing may indicate the block device is /dev/dsk/c1t2d0.

- 4 Start the Portable File System (PFS).

```
# nohup pfs_mountd &  
# nohup pfsd &
```

- 5 Mount the disc.

```
# /usr/sbin/pfs_mount -t rrip /dev/dsk/c#t#d# /cdrom
```

The variable */c#t#d#* represents the location of the drive.

- 6 Install the agent software. Type one of the following commands depending on the operating system on the node.

```
HP-UX (PA)      # swinstall -s /cdrom/hpux/replication\  
                /svccopyservices_agent/version/PA/depot VRTSvcssvc
```

```
HP-UX (IA)      # swinstall -s /cdrom/hpux/replication\  
                /svccopyservices_agent/version/IA/depot VRTSvcssvc
```

The variable *version* represents the version of the agent.

#### To install the agent on Linux systems

- 1 Log in as superuser.
- 2 Insert the disc into the system's drive.
- 3 Mount the disc, if the disc does not automatically mount.

```
# mount -o ro /dev/cdrom /mnt/cdrom
```

- 4 Navigate to the */mnt* directory.

```
# cd /mnt/cdrom
```

- 5 Navigate to the location of the agent package.

```
# cd linux/replication/svccopyservices_agent  
/version/rpms/
```

The variable *version* represents the version of the agent.

- 6 Install the agent software:

```
# rpm -ivh agentrpm
```

The variable *agentrpm* represents the agent package in the *rpms* directory.

### To install the agent on Solaris systems

- 1 Insert the disc into the system's drive.

```
# cd /cdrom/cdrom0
```

- 2 Navigate to the location of the agent package.

```
# cd solaris/platform/replication/svccopyservices_agent  
/version/pkgs/
```

The following are the *platform* values:

- x64
- sparc

The variable *version* represents the version of the agent.

- 3 Install the agent binaries.

```
pkgadd -d . VRTSvcssvc
```

## Upgrading the agent for 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 SVCCopyServices”](#) on page 23.

- 3 Delete the file `/etc/VRTSvcs/conf/config/SVCCopyServicesTypes.cf`.

- 4 Install the current version of the agent.

See [“Installing the agent for SVCCopyServices”](#) on page 19.

- 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 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 from an AIX cluster

- ◆ Type the following command on each node to remove the agent. Answer prompts accordingly:

```
# installp -u VRTSvcssvc.rte
```

### To remove the agent from an HP-UX cluster

- ◆ Type the following command on each node to remove the agent. Answer prompts accordingly:

```
# swremove VRTSvcssvc
```

### To remove the agent from a Linux cluster

- ◆ Type the following command on each node to remove the agent. Answer prompts accordingly:

```
# rpm -e VRTSvcssvc
```

### To remove the agent from a Solaris cluster

- ◆ Type the following command on each node to remove the agent. Answer prompts accordingly:

```
# pkgrm VRTSvcssvc
```



# Configuring the agent for IBM SVCCopyServices

This chapter includes the following topics:

- [Configuration concepts for the SVC Copy Services agent](#)
- [Before you configure the agent for SVCCopyServices](#)
- [Configuring the agent for SVCCopyServices](#)

## Configuration concepts for the SVC Copy Services agent

Review the configuration concepts and failure scenarios for the agent.

## Resource type definition for the SVC CopyServices agent

Following is the resource type definition for the SVCCopyServices agent:

```
type SVC CopyServices (
    str GroupName
    temp str VCSResLock
    int IsConsistencyGroup = 1
    str SSHBinary = "/usr/bin/ssh"
    str SSHPathToIDFile
    str SVCClusterIP
    str SVCUserName = admin
    int StopTakeover = 0
    int DisconnectTakeover = 0
    static str ArgList[] = {GroupName, IsConsistencyGroup, SSHBinary,
```

```
        SSHPathToIDFile, SVCClusterIP, SVCUserName, StopTakeover,  
        DisconnectTakeover}  
    )
```

## Attribute definitions for the SVC CopyServices 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 of 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 `stopprrelationship` or the `stopprconsistentgrp` 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.

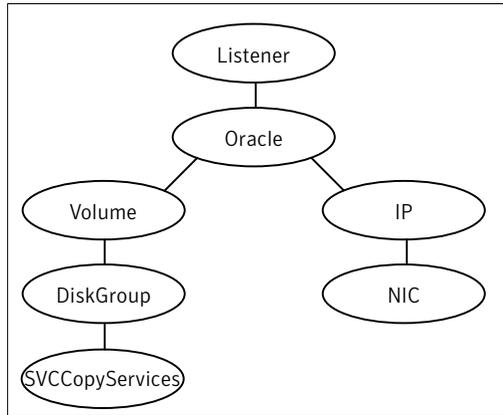
Type-dimension: integer-scalar

Disconnect Takeover	<p>Determines whether the agent makes read-write access available to the host when the replication is in a disconnected state (i.e. <code>consistent_disconnected</code>).</p> <p>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.</p> <p>Attribute value is either 0 or 1. Default is 0.</p> <p>The possible disconnected states are:</p> <ul style="list-style-type: none"><li><code>idling_disconnected</code></li><li><code>inconsistent_disconnected</code></li><li><code>consistent_disconnected</code></li></ul> <p>When the state of the replication is <code>consistent_disconnected</code> and <code>DisconnectTakeover = 1</code>, then the agent enables read/write access for the SVC cluster. When the state of the replication is <code>idling_disconnected</code>, the agent does not enable read-write access for the SVC cluster.</p> <p>Type-dimension: integer-scalar</p>
VCSResLock	<p>The agent uses the <code>VCSResLock</code> attribute to serialize commands across nodes in case of a parallel application like RAC.</p> <p>The serialized commands are used to change the direction of replication, as well as import and deport the <code>CVMVolDg</code> resources that depend on the SVC resource.</p> <p>Type-dimension: temporary string</p>

## Sample configuration for the IBMSVCCopyServices agent

[Figure 3-1](#) shows a dependency graph of a VCS service group that has a resource of type `SVCCopyServices`.

**Figure 3-1** 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>"
)
  
```

## Before you configure the agent for 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.
- Review the configuration concepts, which describe the agent's type definition and attributes.

See [“Configuration concepts for the SVC Copy Services agent”](#) on page 25.

- 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 11.
- Make sure that the cluster has an effective heartbeat mechanism in place.  
See [“About cluster heartbeats”](#) on page 30.
- Set up system zones in replicated data clusters.  
See [“About configuring system zones in replicated data clusters”](#) on page 30.

## 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

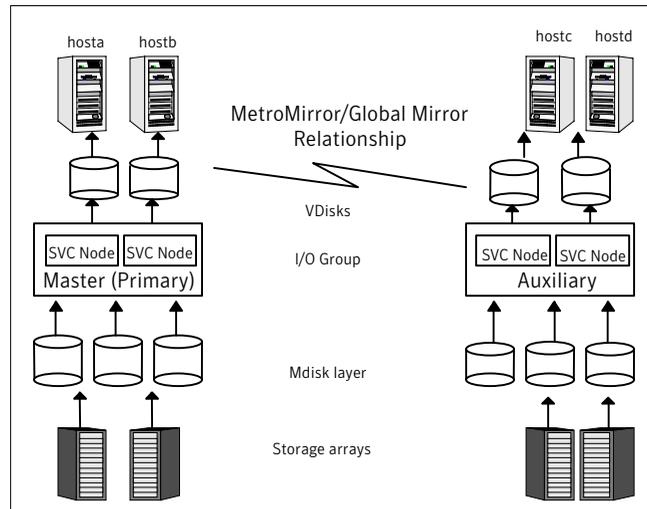
In a replicated data cluster, you can prevent unnecessary SVCCopyServices failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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

[Figure 3-2](#) depicts a sample configuration where `hosta` and `hostb` are in one system zone, and `hostc` and `hostd` are in another system zone.

Use the `SystemZones` attribute to create these zones.

**Figure 3-2** Example system zone configuration



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.

## Configuring the agent for 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.

## 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 (SVCCopyServices) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:  
`/etc/VRTSvcs/conf/SVCCopyServicesTypes.cf.`
- 3 Click **Import**.
- 4 Save the configuration.
- 5 Add a resource of type SVCCopyServices at the bottom of the service group.
- 6 Configure the attributes of the SVCCopyServices resource.
- 7 If the service group is not configured as a global group, configure the service group using the Global Group Configuration Wizard.  
  
See the *Veritas Cluster Server User's Guide* for more information.
- 8 To configure the agent to manage the volumes that Veritas Storage Foundation for Oracle RAC uses:
  - Configure the SupportedActions attribute for the CVMVolDg resource
  - Add the following keys to the list: import, deport.Note that SupportedActions is a resource type attribute and defines a list of action tokens for the resource.
- 9 Change the ClusterFailOverPolicy from the default, if necessary. Symantec recommends keeping the default, which is Manual, to minimize the chance of failing over on a split-brain.
- 10 Repeat step 5 through step 9 for each service group in each cluster that uses replicated data.

# Managing and testing clustering support for IBM SVCCopyServices

This chapter includes the following topics:

- [Typical test setup for the IBM SVCCopyServices agent](#)
- [Testing service group migration](#)
- [Testing host failure](#)
- [Testing cluster failure](#)
- [Performing a disaster test](#)
- [Performing the failback test](#)
- [Failure scenarios for IBM SVCCopyServices](#)

## 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.

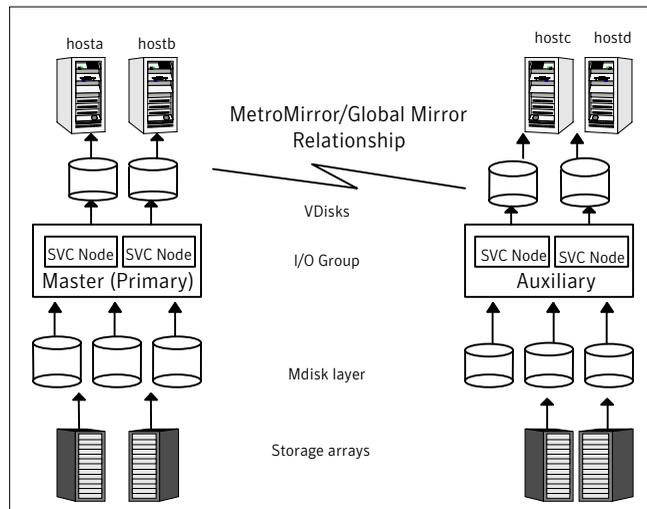
- SSH configuration is established on hosts (hosta and hostb) and the master SVC cluster so that the hosts (hosta and hostb) can communicate via SSH with the master SVC cluster.
- SSH configuration on hosts (hostc and hostd) and the auxiliary SVC cluster so that the hosts (hostc and hostd) can communicate 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 -l<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 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 `stopprrelationship` or the `stopprconsistgrp` command, without the `-access` option.
- Use the `startprrelationship` or the `startprconsistgrp` 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 `stopprrelationship` or the `stopprconsistgrp` command with the `-access` option.

- Use the `starttrcrelationship` or the `starttrcconsistgrp` 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.



# Setting up a fire drill

This chapter includes the following topics:

- [About fire drills](#)
- [Fire drill configurations](#)
- [About the SVCCopyServicesSnap agent](#)
- [Before you configure the fire drill service group](#)
- [Configuring the fire drill service group](#)
- [Verifying a successful fire drill](#)

## 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.

The SVCCopyServicesSnap agent supports fire drills for storage devices that are managed using Veritas Volume Manager 5.0 MP1 RP2, which is a component of Veritas Storage Foundation.

---

**Note:** The agent does not support fire drills in a RAC environment.

---

## Fire drill configurations

VCS supports the following fire drill configurations for the agent:

- |        |   |
|--------|---|
| Gold   | <p>Runs the fire drill on a snapshot of the target array. The replicated device keeps receiving writes from the primary.</p> <p>Symantec recommends this configuration because it does not affect production recovery.</p> <p>In the Gold configuration, VCS does the following:</p> <ul style="list-style-type: none"><li>■ Takes a snapshot of the target array on snapshot LUNs using FlashCopy.</li><li>■ Modifies the disk group name in the snapshot.</li><li>■ Brings the fire drill service group online using the snapshot data.</li></ul> <p>For non-replicated devices:</p> <ul style="list-style-type: none"><li>■ You must use Veritas Volume Manager.</li><li>■ You must use the Gold configuration without the option to run in the Bronze mode.</li></ul> |
| Silver | <p>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. If a disaster occurs while resynching data after running the fire drill, you must switch to the snapshot for recovery.</p> <p>In the Silver configuration, VCS does the following:</p> <ul style="list-style-type: none"><li>■ Takes a snapshot of the target array on snapshot LUNs using FlashCopy.</li><li>■ Modifies the disk group name in the snapshot.</li><li>■ 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.</li></ul>  |

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.
- Brings the fire drill service group online using the data on the target array.

## 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.

### SVCCopyServicesSnap agent functions

The SVCCopyServicesSnap agent performs the following functions:

online

Gold Configuration

- Takes a local snapshot of the target LUN.
- Takes the fire drill service group online by mounting the replication target LUN.
- Creates a lock file to indicate that the resource is online.

Silver Configuration

- Takes a local snapshot of the target LUN.
- Takes the fire drill service group online by mounting the target LUN.
- Creates a lock file to indicate that the resource is online.

Bronze Configuration

- Suspends replication between the source and the target arrays.
- Takes the fire drill service group online using the target array.
- Creates a lock file to indicate that the resource is online.

offline	<p>Gold Configuration</p> <ul style="list-style-type: none"><li>■ Destroys the snapshot by synchronizing data between the target array and the device on which snapshot was taken.</li><li>■ Removes the lock file created by the online function.</li></ul> <p>Silver Configuration</p> <ul style="list-style-type: none"><li>■ Resumes replication between the source and the target arrays.</li><li>■ Synchronizes data between the target array and the device on which the snapshot was taken. Destroys the snapshot of the target array after the data is synchronized.</li><li>■ Removes the lock file created by the online function.</li></ul> <p>Bronze Configuration</p> <ul style="list-style-type: none"><li>■ Resumes the replication between the source and the target arrays.</li></ul>
monitor	Verifies the existence of the lock file to make sure the resource is online.
clean	Restores the state of the LUNs to their original state after a failed online function.
action	For internal use.

## Resource type definition for the SVCCopyServicesSnap agent

Following is the resource type definition for the SVCCopyServicesSnap agent:

```
type SVCCopyServicesSnap (  
    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 }  
    str TargetResName  
    int MountSnapshot  
    int UseSnapshot  
    int RequireSnapshot  
    temp str FDFile  
    str FCMapGroupName  
    temp str Responsibility  
)
```

## Attribute definitions for the SVCCopyServicesSnap agent

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

TargetResName	<p>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.</p> <p>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.</p> <p>Type-dimension: string-scalar</p>
UseSnapshot	<p>Specifies whether the SVCCopyServicesSnap resource takes a local snapshot of the target array. Set this attribute to 1 for Gold and Silver configurations. For Bronze, set this attribute to 0.</p> <p>Type-Dimension: integer-scalar</p> <p>See <a href="#">“About the Snapshot attributes”</a> on page 46.</p>
RequireSnapshot	<p>Specifies whether the SVCCopyServicesSnap resource must take a snapshot before coming online.</p> <p>Set this attribute to 1 if you want the resource to come online only after it succeeds in taking a snapshot.</p> <p>Set this attribute to 0 if you do want the resource to come online even if it fails to take a snapshot. Setting this attribute to 0 creates the Bronze configuration.</p> <p>Type-Dimension: integer-scalar</p> <p><b>Note:</b> Set this attribute to 1 only if UseSnapshot is set to 1.</p>
MountSnapshot	<p>Specifies whether the resource uses the snapshot to bring the service group online. Set this attribute to 1 for Gold configuration. For Silver and Bronze configurations, set the attribute to 0.</p> <p>Type-Dimension: integer-scalar</p> <p><b>Note:</b> Set this attribute to 1 only if UseSnapshot is set to 1.</p>
Responsibility	<p>Do not modify. For internal use only.</p> <p>Used by the agent to keep track of resynchronizing snapshots.</p> <p>Type-Dimension: temporary string</p>

FDFile	<p>Do not modify. For internal use only.</p> <p>Used by the agent to store the absolute pathname to the file with the latest fire drill report on the local system.</p> <p>Type-Dimension: temporary string</p>
FCMapGroupName	<p>Name of the FlashCopy mapping or FlashCopy consistency group.</p> <p>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.</p> <p>Type-dimension: string-scaler</p>

## 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.

## 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.

The following configuration creates a Gold fire drill configuration.

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
FCMapGroupName = fc_cg1
)
```

## 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.
- For the Gold configuration, you must use Veritas Volume Manager to import and deport the storage.

## 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.

The fire drill service group uses a point-in-time snapshot of the application data.

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 48.

## 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 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 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.

You can also view the fire drill log, which is located at `/tmp/fd-servicegroup`.

- 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.

# Index

## A

- application failure 38
- attribute definitions
  - SVC CopyServices 26

## C

- cluster
  - heartbeats 30
- cluster failure 38

## D

- disaster test 37

## F

- failback test 37
- failure scenarios
  - all application failure 38
  - all host failure 38
  - cluster failure 38
  - replication link failure 39
  - total site disaster 38
- FDFFile attribute 46
- fire drill
  - about 41
  - configuration wizard 47
  - running 50
  - service group for 47
  - supported configurations 42
  - SVCCopyServicesSnap agent 43

## H

- host failure 38

## I

- installing the agent
  - AIX systems 19
  - HP-UX systems 19
  - Linux systems 19
  - Solaris systems 19

## M

- migrating service group 34
- MountSnapshot attribute 45

## R

- replication link failure 39
- RequireSnapshot attribute 45
- resource type definition
  - SVC CopyServices agent 25
  - SVCCopyServicesSnap agent 44
- Responsibility attribute 45

## S

- sample configuration 28
- service group
  - migrating 34
- split-brain
  - handling in cluster 31
  - handling in clusters 39
- SVC CopyServices agent
  - attribute definitions 26
  - type definition 25
- SVCCopyServicesSnap agent
  - about 43
  - attribute definitions 45
  - operations 43
  - type definition 44
- SVCCopyServicesSnap agent attributes
  - FDFFile 46
  - MountSnapshot 45
  - RequireSnapshot 45
  - Responsibility 45
  - UseSnapshot 45

## T

- testing
  - disaster 37
  - failback 37
- total site disaster 38

type definition

- SVC CopyServices agent 25
- SVCCopyServicesSnap agent 44

**U**

uninstalling the agent

- AIX systems 23
  - HP-UX systems 23
  - Linux systems 23
  - Solaris systems 23
- UseSnapshot attribute 45