

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

Windows

5.0

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: 6.0.03400.0

Document version: 6.0.03400.0.0

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

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

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

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

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

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

Technical Support	4	
Chapter 1	Introducing the Symantec agent for IBM SVCCopyServices	9
	About the agent for IBM SVCCopyServices	9
	Supported software	10
	Typical IBM SVCCopyServices setup in a VCS cluster	10
	SVCCopyServices agent functions	11
	About the SVCCopyServices agent's online function	12
	About the SVCCopyServices agent's update action function	16
	About the SVCCopyServices agent's info function	17
Chapter 2	Installing and removing the agent for IBM SVCCopyServices	18
	Before you install the agent for IBM SVCCopyServices	18
	Installing the agent for IBM SVCCopyServices	18
	Removing the agent for IBM SVCCopyServices	19
Chapter 3	Configuring the agent for IBM SVCCopyServices	21
	Configuration concepts for the SVCCopyServices agent	21
	Sample configuration for the IBM SVCCopyServices agent	21
	Resource type definition for the SVCCopyServices agent	22
	Attribute definitions for the SVCCopyServices agent	23
	Before you configure the agent for IBM SVCCopyServices	25
	About cluster heartbeats	26
	About configuring system zones in replicated data clusters	26
	About preventing split-brain	27
	About PuTTY configuration for SVCCopyServices	28
	Configuring the agent for IBM SVCCopyServices	29
	Configuring the agent manually in a global cluster	30

Chapter 4	Managing and testing clustering support for IBM SVCCopyServices	31
	Typical test setup for the IBM SVCCopyServices agent	31
	Testing service group migration	32
	Testing host failure	33
	Performing a disaster test	34
	Performing the failback test	34
	Failure scenarios for IBM SVCCopyServices	35
	Site disaster	35
	All host or all application failure	35
	Cluster failure	36
	Replication link failure	36
	Split-brain in a SVCCopyServices environment	37
Chapter 5	Setting up a fire drill	38
	About fire drills	38
	Fire drill configurations	38
	About the SVCCopyServicesSnap agent	39
	SVCCopyServicesSnap agent functions	40
	Resource type definition for the SVCCopyServicesSnap agent	41
	Attribute definitions for the SVCCopyServicesSnap agent	41
	About the Snapshot attributes	43
	Sample configuration for a fire drill service group	43
	Before you configure the fire drill service group	44
	Verifying a successful fire drill	44
Index		45

Introducing the Symantec agent for IBM SVCCopyServices

This chapter includes the following topics:

- [About the agent for IBM SVCCopyServices](#)
- [Supported software](#)
- [Typical IBM SVCCopyServices setup in a VCS cluster](#)
- [SVCCopyServices agent functions](#)

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.

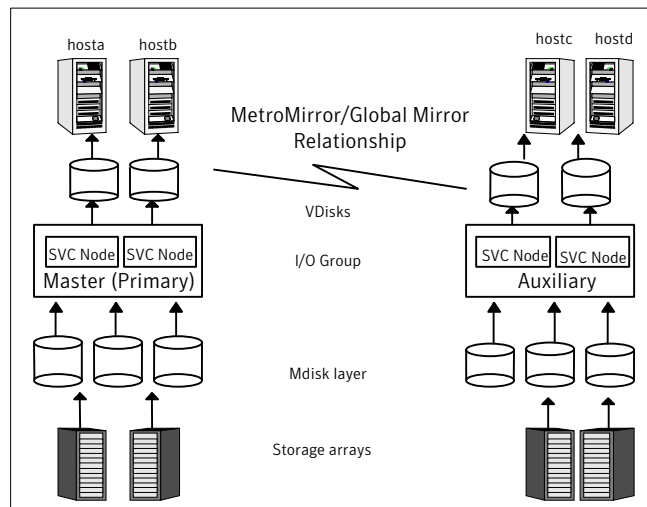
Supported software

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>.

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.

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 “About the SVCCopyServices agent's online function” on page 12.</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 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.</p> <p>The action updates and resynchronizes the differences in the data between the primary and secondary sites.</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">■ <code>starttrcrelationship</code>■ <code>starttrcconsistgrp</code> <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 “About the SVCCopyServices agent's update action function” on page 16.</p>
open	<p>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.</p> <p>The agent does not remove the lock file if the agent was started after running the <code>hastop -force</code> command.</p>
info	<p>Reports the detailed status of the replication relationship or consistency group being monitored by the agent.</p> <p>See “About the SVCCopyServices agent's info function” on page 17.</p>

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.

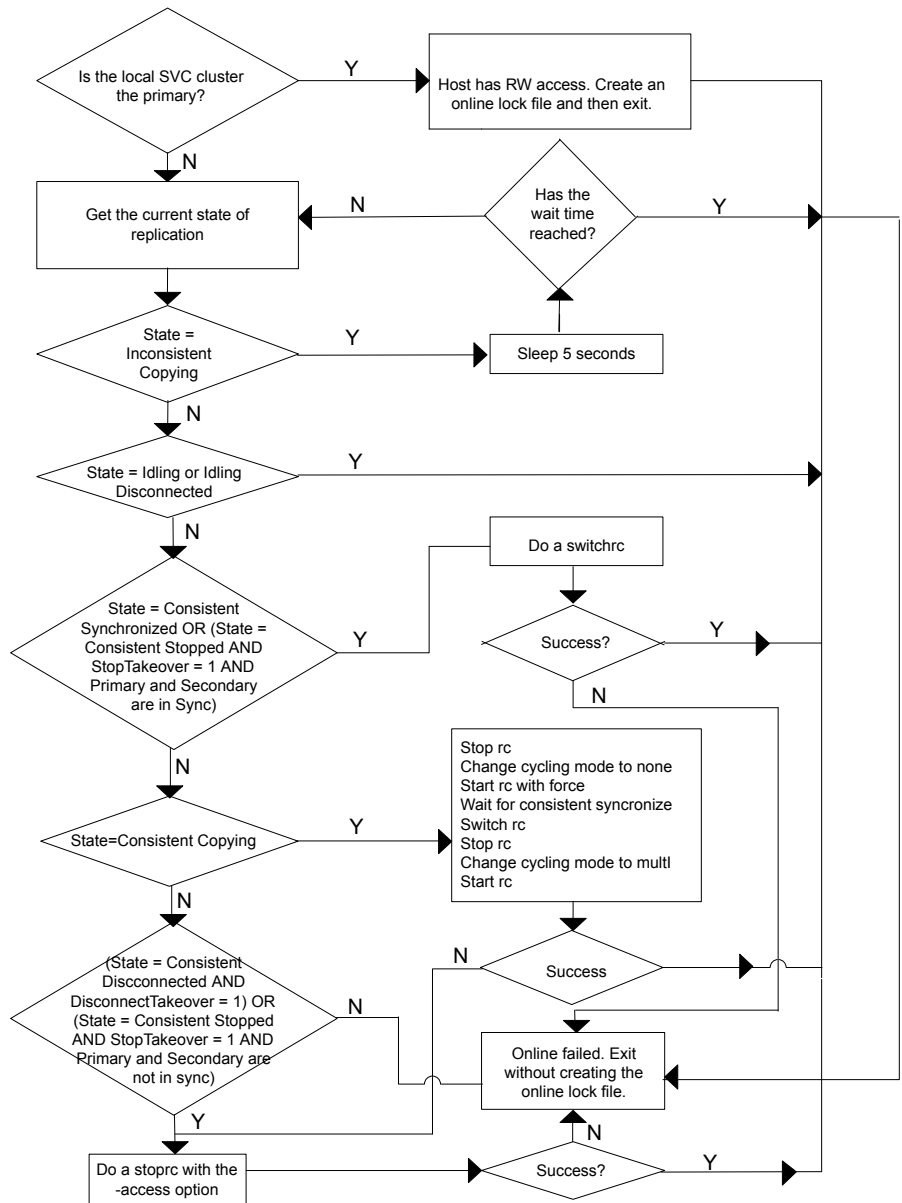
- **Inconsistent Copying** - In this state, the agent waits for the remainder of the online entry point time (before the online entry point times out) for the replication to move out of this state. If it does not move out of the `inconsistent_copying` state, the online entry point times out. Else, the 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.
- **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 `svcinfol srcrelationship` or the `svcinfol srconsistgrp` 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 `svcinfol srcrelationship` 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 IBM SVCCopyServices](#)
- [Installing the agent for IBM SVCCopyServices](#)
- [Removing the agent for IBM SVCCopyServices](#)

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.

To install the VCS agent for IBM SVCCopyServices from the Agent Pack release

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

Windows 2003 (x64)	<code>cdI\windows\w2k3x64\vcs\replication\svccopyservices_agent\vc_s_version\version_agent\pkgs</code>
-----------------------	--

Windows 2003 x86	<code>cdI\windows\w2k3x86\vc_s\ replication\svccopyservices_agent\vc_s_version\version_agent\pkgs</code>
---------------------	--

Windows 2008 x86	<code>cdI\windows\w2k8x86\vc_s\ replication\svccopyservices_agent\version_agent\pkgs</code>
---------------------	---

Windows 2008 x64	<code>cdI\windows\w2k8x64\vc_s\ replication\svccopyservices_agent\version_agent\pkgs</code>
---------------------	---

Windows 2008 IA64	<code>cdI\windows\w2k8IA64\vc_s\ replication\svccopyservices_agent\version_agent\pkgs</code>
----------------------	--

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

Removing the agent for IBM SVCCopyServices

This section describes steps for uninstalling the agent. Do not attempt to remove the agent if service groups accessing the shared storage are online.

To remove the agent for SVCCopyServices that was installed from an Agent Pack release

- 1** Open the Windows Control Panel and click **Add or Remove Programs** or **Uninstall a Program**.
- 2** Select VCS Agent for IBM SVCCopyServices or vrtsvcsvc.msi.
- 3** Click the **Remove** or **Uninstall** button.
- 4** Follow the instructions the installer provides to complete the uninstallation.

Configuring the agent for IBM SVCCopyServices

This chapter includes the following topics:

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

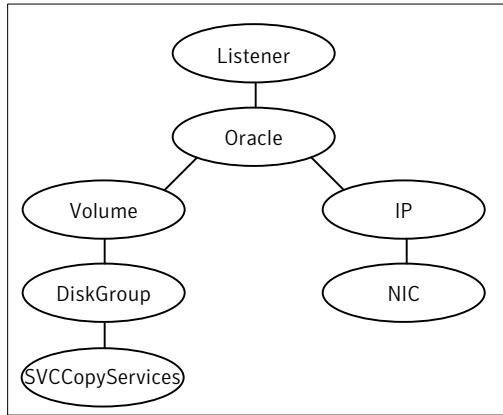
Configuration concepts for the SVCCopyServices agent

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

Sample configuration for the IBM SVCCopyServices 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>"
)
```

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 = "C:\\Program Files\\PuTTY\\plink.exe"
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	<p>Name of the replication relationship or consistency group that is managed by the agent.</p> <p>Type-dimension: string-scalar</p>
IsConsistencyGroup	<p>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.</p> <p>Attribute value is either 0 or 1. Default is 1.</p> <p>Type-dimension: integer-scalar</p>
SSHBinary	<p>Contains the absolute path to the SSH binary. SSH is the mode of communication with the SVC cluster that is connected to the node.</p> <p>Default is: "C:\Program files (x86)\PuTTY\Plink.exe"</p> <p>Type-dimension: string-scalar</p>
SSHPathToID File	<p>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.</p> <p>Type-dimension: string-scalar</p>
SVCClusterIP	<p>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.</p> <p>Type-dimension: string-scalar</p>

SVCUserName	<p>User name that authenticates the SSH connection with the SVC cluster.</p> <p>Default is admin.</p> <p>Type-dimension: string-scalar</p>
StopTakeover	<p>Determines whether the agent makes read-write access available to the host when the replication is in a stopped state (i.e. <code>consistent_stopped</code>).</p> <p>The status of the replication goes into a stopped state when the user fires the <code>stopprcrelationship</code> or the <code>stopprcconsistgrp</code> command. Thus, no replication occurs between the primary and secondary SVC clusters.</p> <p>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.</p> <p>The possible stopped states are:</p> <p><code>inconsistent_stopped</code></p> <p><code>consistent_stopped</code></p> <p>When the state of the replication is <code>consistent_stopped</code> and <code>StopTakeover = 1</code>, the agent enables read-write access for the SVC cluster.</p> <p>When the state of the replication is <code>inconsistent_stopped</code>, the agent does not enable read-write access for the SVC cluster.</p> <p>Type-dimension: integer-scalar</p>

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> <p><code>idling_disconnected</code></p> <p><code>inconsistent_disconnected</code></p> <p><code>consistent_disconnected</code></p> <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>
CopyTakeover	<p>Determines whether the agent makes read-write access available to the host when the replication is in a <code>consistent_copying</code> state.</p> <p>The agent attempts to synchronize the data before making read/write access available. The status of the replication is in a <code>consistent_copying</code> state when the multi cycling mode is used. In this mode, the data is always consistent, but can lag behind.</p> <p>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.</p> <p>Type-dimension: integer-scalar</p> <p>Default value: 0</p>
VCSResLock	<p>This attribute is used for internal purpose.</p> <p>Type-dimension: temporary string</p>

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 26.

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

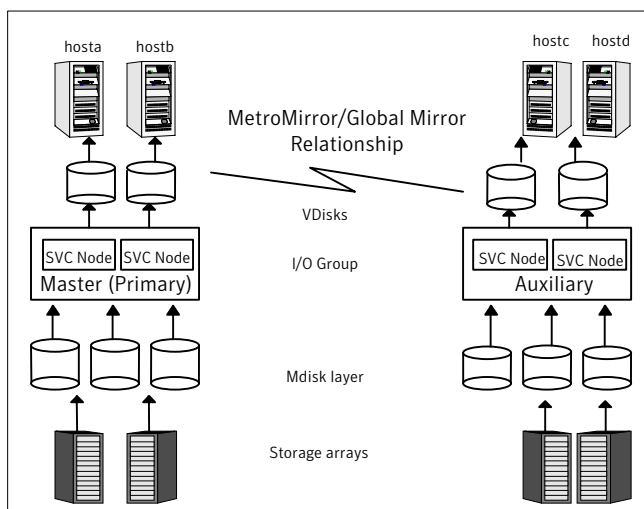
In a replicated data cluster, you can prevent unnecessary SVCCopyServices failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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



Modify the SystemZones attribute using the following command:

```
hagrp -modify grpname SystemZones hosta 0 hostb 0 hostc 1 hostd 1
```

The variable grpname represents the service group in the cluster.

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.

About PuTTY configuration for SVCCopyServices

IBM bundles PuTTY with the software provided for IBM SVCCopyServices. For more information on the process of creating public and private keys as well as securing communication with the SVC appliance, refer to IBM documentation.

The VCS agent for SVCCopyServices on Windows has qualified `plink` command from the PuTTY command tools. The agent works with PuTTY version .58.

Note: PuTTY versions .59 and .60 do not work with the agent for SVCCopyServices.

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

After communication with the SVC appliance is established, perform the following steps to accept the host certificate.

To accept the host certificate

- 1 Download Pstools from the sysinternals site and extract Pstools.
- 2 Run the following command:

```
psexec -i -s cmd.exe
```

This launches a command prompt under the local system account.

- 3 Run the following command at the command line session for the local system:

```
Plink -i <ppk file> -l <username> <IP of SVC appliance>
```

This displays the following information:

```
The server's host key is not cached in the registry.
You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 df:46:45:0a:e1:ea:7d:28:6a:8e:19:d3:ba:d7:e4:9f
```

Enter **y** to add the key to PuTTY's cache and continue connecting.

Enter **n** if you want to connect just once, without adding the key to the cache.

Press **Return** to abandon the connection in case you do not trust the host.

If you trust this host, enter "y" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, enter "n".

If you do not trust this host, press Return to abandon the connection.

Type **y** to cache the certificate.

```
Store key in cache? (y/n)
```

You must cache the certificate for every SVC appliance connected and for each user specified in the resources.

- 4 Delete the Pstools, if desired.
- 5 Repeat these steps on each cluster node where the service group containing the SVC resource is configured.

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.
- 7 The configuration must be identical on all cluster nodes, both primary and disaster recovery.

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](#)
- [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.

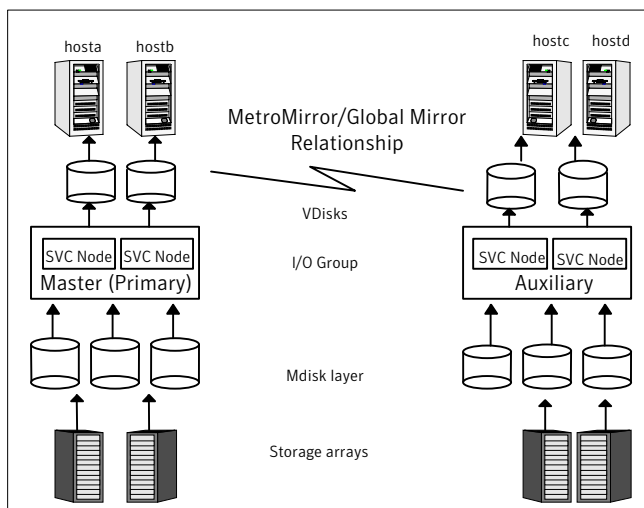
- SSH configuration is established on hosts (hosta and hostb) and the master SVC cluster so that the hosts (hosta and hostb) can communicate via SSH with the master SVC cluster.
- SSH configuration on hosts (hostc and hostd) and the auxiliary SVC cluster so that the hosts (hostc and hostd) can communicate 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 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.

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 `startprrelationship` or the `startprconsistgrp` 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](#)
- [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.

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"> ■ 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	<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.</p> <p>In the Silver configuration, VCS does the following:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p>
Bronze	<p>VCS breaks replication and runs the fire drill test on the replicated target. VCS does not take a snapshot in this configuration.</p> <p>If a disaster occurs while resynching data after the test, it may result in inconsistent data as there is no snapshot data.</p> <p>In the Bronze configuration, VCS does the following:</p> <ul style="list-style-type: none"> ■ 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 maintains 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
	<ul style="list-style-type: none"> ■ 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 <ul style="list-style-type: none"> ■ 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.
offline	Bronze Configuration
	<ul style="list-style-type: none"> ■ Splits 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.
	Gold Configuration
monitor	<ul style="list-style-type: none"> ■ Destroys the snapshot by synchronizing data between the target array and the device on which snapshot was taken. ■ Removes the lock file created by the online function.
	Silver Configuration
	<ul style="list-style-type: none"> ■ Resumes replication between the source and the target arrays. ■ 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. ■ Removes the lock file created by the online function.
clean	Bronze Configuration
	<ul style="list-style-type: none"> ■ Resumes the replication between the source and the target arrays.
	Verifies the existence of the lock file to make sure the resource is online.
	Restores the state of the LUNs to their original state after a failed online function.

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

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 database 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

MountSnapshot	<p>Specifies whether the resource uses the snapshot to bring the service group online. Set this attribute to 1.</p> <p>Type-Dimension: integer-scalar</p> <p>Note: Set this attribute to 1 only if UseSnapshot is set to 1.</p>
UseSnapshot	<p>Specifies whether the SVCCopyServicesSnap resource takes a local snapshot of the target array. Set this attribute to 1.</p> <p>Type-Dimension: integer-scalar</p> <p>See “About the Snapshot attributes” on page 43.</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>Type-Dimension: integer-scalar</p> <p>Note: Set this attribute to 1 only if UseSnapshot is set to 1.</p>
DiskGroupSnapList	<p>This is an optional attribute that lists the original disk group names and the fire drill disk group names.</p> <p>Type-dimension: string-scalar</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.

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.

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.

Index

A

- action/PreSwitch function 11
- action/update function 11
- application failure 35
- attribute definitions 23
- attributes 23
 - DisconnectTakeover attribute 23
 - GroupName attribute 23
 - IsConsistencyGroup attribute 23
 - SSHBinary attribute 23
 - SSHPATHToIDFile attribute 23
 - StopTakeover attribute 23
 - SVCClusterIP attribute 23
 - SVCUserName attribute 23

C

- clean function 11
- cluster
 - heartbeats 26
- cluster failure 36

D

- disaster test 34
- DisconnectTakeover attribute 23
- DiskGroupSnapList attribute 42

F

- failback test 34
- failure scenarios
 - all application failure 35
 - all host failure 35
 - cluster failure 36
 - replication link failure 36
 - total site disaster 35
- FDFFile attribute 42
- fire drill
 - about 38
 - configuration wizard 44
 - running 44
 - service group for 44

- fire drill *(continued)*

- supported configurations 38
 - SVCCopyServicesSnap agent 39

- functions

- action 11
 - clean 11
 - monitor 11
 - offline 11
 - online 11
 - open 11

G

- GroupName attribute 23

H

- host failure 35

I

- info function 11
- installing the agent
 - Windows systems 18
- IsConsistencyGroup attribute 23

M

- migrating service group 32
- monitor function 11
- MountSnapshot attribute 42

O

- offline function 11
- online function 11
- open function 11

R

- replication link failure 36
- RequireSnapshot attribute 42
- resource type definition
 - SVCCopyServices agent 22
 - SVCCopyServicesSnap agent 41

Responsibility attribute 42

S

sample configuration 21

service group

migrating 32

split-brain

handling in cluster 27

handling in clusters 37

SSHBinary attribute 23

SSHPATHToIDFile attribute 23

StopTakeover attribute 23

SVC CopyServices agent

attribute definitions 23

SVCClusterIP attribute 23

SVCCopyServices agent

type definition 22

SVCCopyServicesSnap agent

about 39

attribute definitions 41

operations 39

type definition 41

SVCCopyServicesSnap agent attributes 42

FDFFile 42

MountSnapshot 42

RequireSnapshot 42

Responsibility 42

UseSnapshot 42

SVCUserName attribute 23

T

testing

disaster 34

failback 34

total site disaster 35

type definition

SVCCopyServices agent 22

SVCCopyServicesSnap agent 41

U

uninstalling the agent

Windows systems 19

UseSnapshot attribute 42