

Cluster Server Agent for IBM DS6000/8000 Metro Mirror and Global Mirror Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

6.2

Cluster Server Agent for IBM DS6000/8000 Metro Mirror and Global Mirror 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: 6.2

Document version: 6.2 Rev 0

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

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

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

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Documentation

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

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

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

doc_feedback@symantec.com

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

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

About Symantec Connect

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

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

Contents

Technical Support	3	
Chapter 1	Introducing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	8
	About the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	8
	Supported software	9
	Supported hardware for IBM DS6000/8000 Metro Mirror and Global Mirror	9
	Typical IBM DS6000/8000 Metro Mirror and Global Mirror in a VCS cluster	9
	IBM Metro Mirror agent functions	11
	IBM Global Mirror agent functions	12
Chapter 2	Installing and removing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	14
	Before you install the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	14
	Installing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	15
	Upgrading the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	16
	Removing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	17
Chapter 3	Configuring the agent for IBM DS6000/8000 Metro Mirror and Global Mirror	18
	Configuration concepts for the Metro Mirror agent	18
	Resource type definition for the Metro Mirror agent	18
	Attribute definitions for the Metro Mirror agent	19
	Sample configuration for the Metro Mirror agent	22
	Configuration concepts for the IBM Global Mirror agent	23
	Resource type definition for the Global Mirror agent	23

	Attribute definitions for the Global Mirror agent	24
	Sample configuration for the Global Mirror agent	26
	Before you configure the agent for IBM DS6000/8000 Metro Mirror and	
	Global Mirror	27
	About cluster heartbeats	28
	About configuring system zones in replicated data clusters	28
	Configuring the agent for IBM DS6000/8000 Metro Mirror and Global	
	Mirror	29
	Configuring the agent manually in a global cluster	30
	Configuring the agent manually in a replicated data cluster	30
	Configuring the agent for IBM Global Mirror to compute	
	RPO	31
Chapter 4	Managing and testing clustering support for IBM	
	DS6000/8000 Metro Mirror and Global	
	Mirror	32
	Typical test setup for the IBM DS6000/8000 Metro Mirror and Global	
	Mirror agent	32
	Testing service group migration	33
	Testing host failure	34
	Performing a disaster test	35
	Performing the failback test	36
Chapter 5	Setting up a fire drill	38
	About fire drills	38
	Fire drill configuration for Metro Mirror	39
	About the Metro MirrorSnap agent	39
	Metro MirrorSnap agent functions	39
	Resource type definition for the Metro MirrorSnap agent	40
	Attribute definitions for the Metro MirrorSnap agent	40
	Before you configure the fire drill service group	41
	Configuring the fire drill service group	42
	Creating the fire drill service group using Cluster Manager (Java	
	Console)	42
	Verifying a successful fire drill	44
	Sample configuration for a fire drill service group	45
Index		46

Introducing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

This chapter includes the following topics:

- [About the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)
- [Supported software](#)
- [Supported hardware for IBM DS6000/8000 Metro Mirror and Global Mirror](#)
- [Typical IBM DS6000/8000 Metro Mirror and Global Mirror in a VCS cluster](#)
- [IBM Metro Mirror agent functions](#)
- [IBM Global Mirror agent functions](#)

About the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

The Cluster Server agent for IBM Metro Mirror and Global Mirror provides support for application failover and recovery. The agent provides this support in the environments that use metro_mirror to replicate data between IBM DS6000 and DS8000 arrays.

The agent monitors and manages the state of replicated DS8000 and DS6000 volumes that are attached to VCS nodes. The agent ensures that the system that has the metro_mirror resource online also has safe and exclusive access to the configured volumes.

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

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

The agent supports Metro Mirror that is synchronous replication as well as Global Mirror that is 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>

Supported software

For information on the software versions that the agent for IBM DS6000/8000 Metro Mirror and Global Mirror supports, see the Symantec Operations Readiness Tools (SORT) site: <https://sort.symantec.com/agents>.

Supported hardware for IBM DS6000/8000 Metro Mirror and Global Mirror

The agent supports metro_mirror on all microcode levels on all IBM DS6000/8000 arrays.

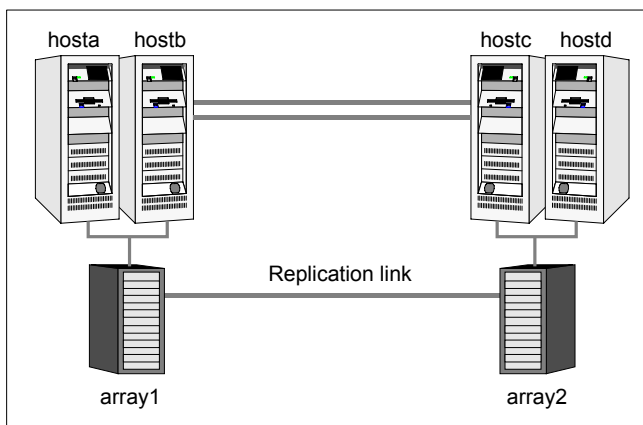
This support only exists if the host, the HBA, and the array combination is in IBM's hardware compatibility list.

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

Typical IBM DS6000/8000 Metro Mirror and Global Mirror in a VCS cluster

[Figure 1-1](#) displays a typical cluster setup in a metro_mirror environment.

Figure 1-1 Typical clustering setup for the agent



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

- The primary array (array1) has one or more primary hosts. A Fibre Channel or SCSI directly attaches these hosts to the IBM DS6000/8000 array that contains the Metro Mirror/Global Copy source volumes.
- The secondary array (array2) has one or more secondary hosts. A Fibre Channel or SCSI directly attaches these hosts to the IBM DS6000/8000 array that contains Metro Mirror/Global Copy target volumes. The target volumes are paired with the primary volumes in the primary array (array 1). The secondary hosts and arrays must be at a significant distance to survive a disaster that may occur at the primary side.

For Global Mirror, additional Flash Copy volumes have to be paired with the Global Copy source volumes as documented in the *IBM DS6000/8000 Command Line Interface Users Guide*.

- IBM supports only a single Global Mirror master session per replicated array pair. This limits the VCS configuration to a single resource of type GlobalMirror for all cluster nodes attached to the same array pair.

Network heartbeating between the two data centers to determine their health could be LLT or TCP/IP.

See “[About cluster heartbeats](#)” on page 28.

- 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 IBM DS6000/8000 array.

- In parallel applications, all hosts that are attached to the same array must be part of the same GAB membership.
- In parallel applications like Storage Foundation for Oracle RAC, all hosts that are attached to the same array must be part of the same GAB membership. Storage Foundation for Oracle RAC is supported with metro_mirror only in a global cluster environment and not in a replicated data cluster environment.

IBM Metro Mirror agent functions

The Cluster Server agent for IBM Metro Mirror monitors and manages the state of replicated DS6000 or DS8000 devices that are attached to VCS nodes.

The agent performs the following functions:

Table 1-1 Agent functions

Function	Description
online	<p>If the state of all local devices is read-write enabled that is "FULL DUPLEX" or "SUSPENDED", the agent creates a lock file on the local host. The lock file indicates that the resource is online.</p> <p>If the local devices are target devices with the "TARGET FULL DUPLEX" state, the agent runs the <code>failoverpprc</code> command to make the volumes writable. This operation makes the devices writable for the application. After successful execution of this command, the agent creates a lock file on the local host. If the AutoFailback attribute is set to 1, the agent executes the <code>failback</code> command to reverse the direction of replication.</p>
offline	Removes the lock file from the host. The agent does not run any Metro Mirror commands because taking the resource offline is not indicative of the intention to give up the devices.
monitor	Verifies that the lock file exists. If the lock file exists, the monitor function reports the status of the resource as online. If the lock file does not exist, the monitor function reports the status of the resource as offline.
open	<p>Removes the lock file on the host where the function is called. This operation prevents potential concurrency violation if the service group fails over to another node.</p> <p>Note that the agent does not remove the lock file if the agent was started after running the <code>hastop -force</code> command.</p>

Table 1-1 Agent functions (*continued*)

Function	Description
clean	<p>Determines if it is safe to fault the resource if the online function fails or times out.</p> <p>The agent checks if a management operation was in progress when the online thread timed out. If the operation was killed, the devices are left in an unusable state.</p>
actions/failback	<p>Performs a failback from the original secondary side to merge any changed tracks from the original secondary to the original primary.</p>
actions/PreSwitch	<p>Ensures that the remote site cluster can come online during a planned failover within a GCO configuration. The VCS engine on the remote cluster invokes the PreSwitch action on all the resources of the remote site during a planned failover using the <code>hagrp -switch</code> command. For this, the PreSwitch attribute must be set to 1. The option <code>-nopre</code> indicates that the VCS engine must switch the servicegroup regardless of the value of the PreSwitch service group attribute.</p> <p>If running the PreSwitch action fails, the failover should not occur. This minimizes the application downtime and data loss.</p>

IBM Global Mirror agent functions

The Cluster Server agent for IBM Global Mirror monitors and manages the state of replicated DS6000 or DS8000 devices that are attached to VCS nodes.

The agent performs the following functions:

Table 1-2 Agent functions

Action	Description
online	<p>If the state of all local devices is read-write enabled that is the devices are in "Copy Pending" or "Suspended" state, the agent creates a lock file on the local host. The lock file indicates that the resource is online.</p> <p>If the original primary volumes are still accessible, the agent runs the <code>gmstop</code> command followed by the <code>failback</code> command to reverse the direction of replication. The agent then restarts the global session using the <code>gmstart</code> command.</p>
offline	<p>Removes the lock file from the host. Moreover, the agent stops the Global Mirror session to support a graceful redirection of the replication link.</p>

Table 1-2 Agent functions (*continued*)

Action	Description
monitor	Verifies that the lock file exists. If the lock file exists, the monitor function reports the status of the resource as online. If the lock file does not exist, the monitor function reports the status of the resource as offline.
open	Removes the lock file on the host where the function is called. This operation prevents potential concurrency violation if the service group fails over to another node. Note: The agent does not remove the lock file if the agent was started after running the <code>hastop -force</code> command.
clean	Determines if it is safe to fault the resource if the online function fails or times out. The agent checks if a management operation was in progress when the online thread timed out. If the operation was killed, the devices are left in an unusable state.
actions/ failback	Performs a <code>failback</code> from the original secondary side to merge any changed tracks from the original secondary to the original primary.
actions/GMStart	Performs a <code>gmstart</code> on the primary side to restart Global Mirror snapshots.
actions/GMStop	Performs a <code>gmstop</code> on the primary side to suppress Global Mirror snapshots.
actions/GMStatus	Reports the current state of the replicated global mirror volumes.
actions/PreSwitch	Reports the state of the replicated volumes to verify if a replication link redirection is possible without the risk of data loss.
action/GetCurrentRPO	Fetches the current point in time Recovery Point Objective (RPO). The agent performs this action function on the disaster recovery (DR) system where the <code>ComputedRSLA</code> attribute is set to 1. The RPO is computed in seconds. Note: The agent does not compute the RPO when the group is frozen. The agent does not store the computed RPO; make a note of the RPO for future reference.

Note: The agent uses the following internal action functions to compute the RPO: `StartRPOComputation`, `StopRPOComputation`, `StartWriter`, and `ReportRPOData`.

Installing and removing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

This chapter includes the following topics:

- [Before you install the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)
- [Installing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)
- [Upgrading the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)
- [Removing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)

Before you install the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

Before you install the Cluster Server agent for IBM DS6000/8000 Metro Mirror and Global Mirror, ensure that you install and configure the VCS on all nodes in the cluster.

Set up replication and the required hardware infrastructure. For information about setting up Oracle RAC environment, refer to the *Storage Foundation for Oracle RAC Configuration and Upgrade Guide*.

See [“Typical IBM DS6000/8000 Metro Mirror and Global Mirror in a VCS cluster”](#) on page 9.

Installing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

You must install the IBM DS6000/8000 Metro Mirror and Global Mirror agent on each node in the cluster. In global cluster environments, install the agent on each node in each cluster.

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

To install the agent in a VCS environment

- 1 Download the Agent Pack from the Symantec Operations Readiness Tools (SORT) site: <https://sort.symantec.com/agents>.

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

- 2 Uncompress the file to a temporary location, say /tmp.
- 3 If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

```
AIX      cdl/aix/vcs/replication/metro_mirror_agent/  
         agent_version/pkgs/
```

```
Linux    cdl/linux/generic/vcs/replication/metro_mirror_agent/  
         agent_version/rpms/
```

```
Solaris  cdl/solaris/dist_arch/vcs/replication/metro_mirror_agent/  
         agent_version/pkgs/
```

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

- 4 Log in as a superuser.
- 5 Install the package.

```
AIX      # installp -ac -d VRTSvcsi.rte.bff VRTSvcsi.rte
```

```
Linux    # rpm -ihv \  
         VRTSvcsi-AgentVersion-Linux_GENERIC.noarch.rpm
```

```
Solaris  # pkgadd -d . VRTSvcsi
```

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

Upgrading the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

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

To upgrade the agent software

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

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

- 2 Remove the agent from the node.

See [“Removing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror”](#) on page 17.

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

- 4 Install the current version of the agent.

See [“Installing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror”](#) on page 15.

- 5 Copy the file MetroMirrorTypes.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 If the agent types file was not added automatically on successful installation of the agent, add the agent types file.

```
# /etc/VRTSvcs/conf/sample_metromirror/addMetroMirrorType.sh
```

- 8 From a node in the cluster, edit your configuration file /etc/VRTSvcs/conf/config/main.cf.

Configure the new attributes, if applicable.

- 9 Verify the configuration by running the following command:

```
# hacf -verify config
```

- 10 Start VCS on local node first.

- 11 Start VCS on other nodes.

Removing the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

Before you attempt to remove the agent, make sure the application service group is not online.

You must remove the HTC agent from each node in the cluster.

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

```
AIX          # installp -u VRTSvcsi.rte
```

```
Linux        # rpm -e VRTSvcsi
```

```
Solaris      # pkgrm VRTSvcsi
```

Configuring the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

This chapter includes the following topics:

- [Configuration concepts for the Metro Mirror agent](#)
- [Configuration concepts for the IBM Global Mirror agent](#)
- [Before you configure the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)
- [Configuring the agent for IBM DS6000/8000 Metro Mirror and Global Mirror](#)

Configuration concepts for the Metro Mirror agent

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

Resource type definition for the Metro Mirror agent

The Metro Mirror resource type represents the IBM Metro Mirror agent in VCS.

```
type MetroMirror (  
    static keylist SupportedActions = { MMStatus, failback, PreSwitch }  
    static int MonitorInterval = 300  
    static int ActionTimeout = 150  
    static int NumThreads = 1  
    static int OpenTimeout = 180  
    static str AgentDirectory = "/opt/VRTSvcs/bin/MetroMirror"  
    static str ArgList[] = { DSCliHome, HMC1, HMC2, User, PasswdFile,
```

```

LocalStorageImageID, RemoteStorageImageID, VolIds, DSMon, AutoFailback,
EnableResetReserve }
str DSCliHome = "/opt/ibm/dscli"
str HMC1
str HMC2
str User = admin
str PasswdFile = "~/dscli/security.dat"
str LocalStorageImageID
str RemoteStorageImageID
str VolIds[]
int DSMon = 0
boolean AutoFailback = 1
boolean EnableResetReserve = 0
temp str VCSResLock
    )

```

Attribute definitions for the Metro Mirror agent

Review the description of the agent attributes.

Required attributes

You must assign values to required attributes.

Table 3-1 Required attributes

Attribute	Description
DSCliHome	Path to the DS8000 command line interface. Type-Dimension: string-scalar Default: /opt/ibm/dscli.
HMC1	IP address or host name of the primary management console. Type-Dimension: string-scalar
User	User name for issuing DSCLI commands from the command line. This is an optional attribute. Type-Dimension: string-scalar Default: admin.

Table 3-1 Required attributes (*continued*)

Attribute	Description
PasswdFile	Specifies the password file that contains your password. See the <code>managepwfile</code> DSCSI command for information on how to generate a password file. This is an optional attribute. Default: <code>~/dscli/security.dat</code> Type-Dimension: string-scalar
LocalStorageImageID	The image ID of the local storage, which consists of manufacturer, type and serial number. For example, <code>IBM.2107-75FA120</code> Type-Dimension: string-scalar
RemoteStorageImageID	The image ID of the remote storage, which consists of manufacturer, type and serial number. For example, <code>IBM.3108-75GB248</code> Type-Dimension: string-scalar
VolIds	IDs of local DS8000 Metro Mirror volumes that the agent manages. Type-Dimension: string-keylist

Optional attributes

Configuring these attributes is optional.

Table 3-2 Optional attributes

Attribute	Description
HMC2	IP address or host name of the secondary management console. Type-Dimension: string-scalar

Table 3-2 Optional attributes (*continued*)

Attribute	Description
DSMon	<p>Checks the state of the replicated volumes as part of monitor function.</p> <p>Type-Dimension: scalar-integer</p> <p>Possible values are as follows:</p> <p>0: Default</p> <p>1: When the resource is supposed to be online and lock file exists.</p> <p>2: When the resource is supposed to be offline and lock file is removed.</p> <p>3: Always</p>
AutoFailBack	<p>Executes failback as part of the online function to reactivate the replication link. This potentially overwrites data at the former primary site if the replication link was down during the failover. Therefore, AutoFailBack can be suppressed by setting this attribute to 0. In this case, the replication has to be restarted by using the failback action.</p> <p>Type-Dimension: scalar-boolean</p> <p>Default: 1</p>
EnableResetReserve	<p>This attribute is used to specify the relationship between a remote mirror and copy. This relationship is established when the volume on the secondary logical subsystem is reserved by another host. Set this attribute when the volume on the secondary logical subsystem is reserved.</p> <p>Type-dimension: scalar-boolean</p> <p>Default: 0</p>

Internal attributes

These attributes are for internal use only. Do not modify their values.

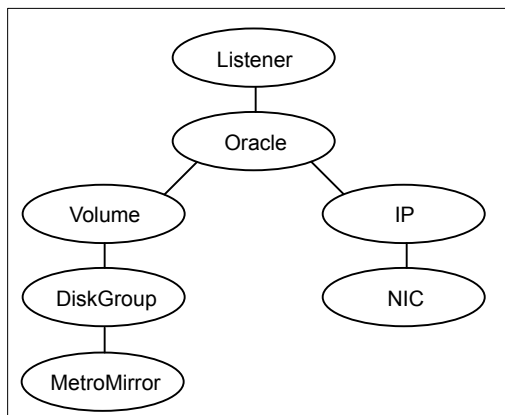
Table 3-3 Internal attribute

Attribute	Description
VCSResLock	<p>The agent uses the VCSResLock attribute to guarantee serialized management in case of a parallel application.</p> <p>Type-Dimension: temporary string-scalar</p>

Sample configuration for the Metro Mirror agent

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

Figure 3-1 Sample configuration for the metro_mirroragent



The DiskGroup resource depends on the MetroMirror resource.

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

```

MetroMirror ora_mmir (
    DSCliHome = "/opt/ibm/dscli"
    HMC1 = "ds8000c.example.com"
    User = admin
    PasswdFile = "/opt/ibm/dscli/ds_pwfile"
    LocalStorageImageID = "IBM.2107-75FA120"
    RemoteStorageImageID = "IBM.2107-75FA150"
    VolIds = { 1260, 1261 }
)
  
```

This resource manages the following objects:

- A group of two Metro Mirror volumes: 1260 and 1261 on the local array with the storage image ID IBM.2107-75FA120.
- The HMC ds800c.example.com manages the local array.
- The Metro Mirror target volumes are on the remote array with the storage image ID IBM.2107-75FA150.
- The password file, created using the `managepwfile` DSCLI command, is located at the following path:
 /opt/ibm/dscli/ds_pwfile

Configuration concepts for the IBM Global Mirror agent

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

Resource type definition for the Global Mirror agent

The IBM Global Mirror agent is represented by the GlobalMirror resource type in VCS.

```
type GlobalMirror (
    static keylist RegList = { ComputeDRSLA }
    static keylist SupportedActions = {GMStatus, failback, PreSwitch,
    GMStart, GMStop, ReportRPOData, StartWriter, GetCurrentRPO,
    StartRPOComputation, StopRPOComputation }
    static int MonitorInterval = 300
    static int NumThreads = 1
    static int OpenTimeout = 180
    static str AgentDirectory = "/opt/VRTSvcs/bin/GlobalMirror"
    static str ArgList[] = { DSCliHome, HMC1, HMC2, User,
    PasswdFile, LocalStorageImageID, LocalLSS,
    RemoteStorageImageID, RemoteLSS, GMSession,
    VolIds, EnableResetReserve, DSMon, AutoFailback, ComputeDRSLA }
    str DSCliHome = "/opt/ibm/dscli"
    str HMC1
    str HMC2
    str User = admin
    str PasswdFile = "~/dscli/security.dat"
    str LocalStorageImageID
    str LocalLSS
    str RemoteStorageImageID
    str RemoteLSS
    str GMSession
    str VolIds[]
    boolean EnableResetReserve = 0
    int DSMon = 0
    boolean AutoFailback = 1
    int ComputeDRSLA
    temp boolean Tagging = 0
    temp str VCSResLock
)
```

Attribute definitions for the Global Mirror agent

Review the description of the agent attributes.

Required attributes

You must assign values to required attributes.

Table 3-4 Required attributes

Attribute	Description
DSCliHome	Path to the DS8000 command line interface. Type-Dimension: string-scalar Default: /opt/ibm/dscli.
HMC1	IP address or host name of the primary management console. Type-Dimension: string-scalar
User	User name for issuing DSCLI commands from the command line. Type-Dimension: string-scalar Default: admin.
PasswdFile	Specifies the password file that contains your password. See the <code>managepwfile</code> DSCLI command for information on how to generate a password file. Type-Dimension: string-scalar Default: ~/dscli/security.dat
LocalStorageImageID	The image ID of the local storage, which consists of manufacturer, type, and serial number. For example, IBM.2107-75FA120 Type-Dimension: string-scalar
LocalLSS	The logical subsystem ID where the local volumes reside. A two-digit hexadecimal number, for example, 0F. Type-Dimension: string-scalar
RemoteStorageImageID	The image ID of the remote storage, which consists of manufacturer, type, and serial number. For example, IBM.3108-75GB248 Type-Dimension: string-scalar

Table 3-4 Required attributes (continued)

Attribute	Description
RemotelSS	The logical subsystem ID where the remote volumes reside. A two-digit hexa-decimal number, for example 0F. Type-Dimension: string-scalar
GMSession	The Global Mirror master session ID. A two-digit hexa-decimal number, for example 0F. Type-Dimension: string-scalar
Vollds	IDs of local DS8000 Metro Mirror volumes that the agent manages. Type-Dimension: string-keylist

Optional attributes

Configuring these attributes is optional.

Table 3-5 Optional attributes

Attribute	Description
HMC2	IP address or host name of the secondary management console. Type-Dimension: string-scalar
ComputeDRSLA	Used to enable or disable Recovery Point Objective (RPO) computation. Set this attribute on any one node in the disaster recovery (DR) cluster. Setting this attribute to 1 starts the RPO computation process. Ensure that you reset this attribute to 0 after you use the GetCurrentRPO action function to check the RPO. Type-Dimension: integer-scalar Default: 0

Internal attributes

These attributes are for internal use only. Do not modify their values.

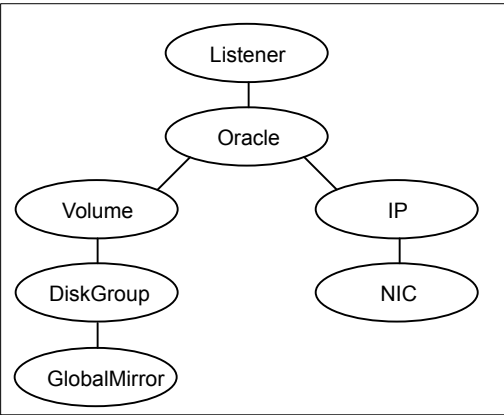
Table 3-6 Internal attributes

Attribute	Description
VCSResLock	The agent uses the VCSResLock attribute to guarantee serialized management in case of a parallel application. Type-Dimension: temporary string-scalar
Tagging	This internal attribute is used for maintaining the process of computing RPO.

Sample configuration for the Global Mirror agent

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

Figure 3-2 Sample configuration for the metro_mirroragent



The DiskGroup resource depends on the MetroMirror resource.

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

```

GlobalMirror ora_gmir (
    DSCliHome = "/opt/ibm/dscli"
    HMC1 = "ds8000c.example.com"
    User = admin
    PasswdFile = "/opt/ibm/dscli/ds_pwfile"
    LocalStorageImageID = "IBM.2107-75FA120"
    LocalLSS = "01"
    RemoteLSS = "00"
    GMSession = "1A"

```

```
RemoteStorageImageID = "IBM.2107-75FA150"
VolIds = { 1260, 1261 }
boolean EnableResetReserve = 0
)
```

This resource manages the following objects:

- A group of two Global Copy volumes: 1260 and 1261 on the local array with the storage image ID IBM.2107-75FA120 on logical subsystem 01.
- The HMC ds800c.example.com manages the local array.
- The Global Copy target volumes are on the remote array with the storage image ID IBM.2107-75FA150 on logical subsystem (LSS) 00.
- For the replication link, the Global Mirror master session with ID 1A is used.
- The password file, created using the `managepwfile` DSCLI command, is located at the following path:
`/opt/ibm/dscli/ds_pwfile`

Before you configure the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

Before you configure the agent, review the following information:

- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
 See [“Typical IBM DS6000/8000 Metro Mirror and Global Mirror in a VCS cluster”](#) on page 9.
- Make sure that Metro Mirror paths are configured in both directions between the source and the target LSS. Metro mirror role reversal fails if paths are not configured from the current target LSS to the current source LSS.
- Ensure that the replication paths are configured in both directions between the source and target LSS. GlobalMirror role reversal fails if paths are not configured from the current target LSS to the current source LSS.
- Make sure that the cluster has an effective heartbeat mechanism in place.
 See [“About cluster heartbeats”](#) on page 28.
- Set up system zones in replicated data clusters.
 See [“About configuring system zones in replicated data clusters”](#) on page 28.
- Generate the DSCLI password file. Use the `managepwfile` DSCLI command to do so.

- Reboot the node after the DSCLI software is installed on that node. The DSCLI installation sets some system environment variables that do not take effect until a reboot. If these environment variables are not set, the metro_mirror will not function properly.

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

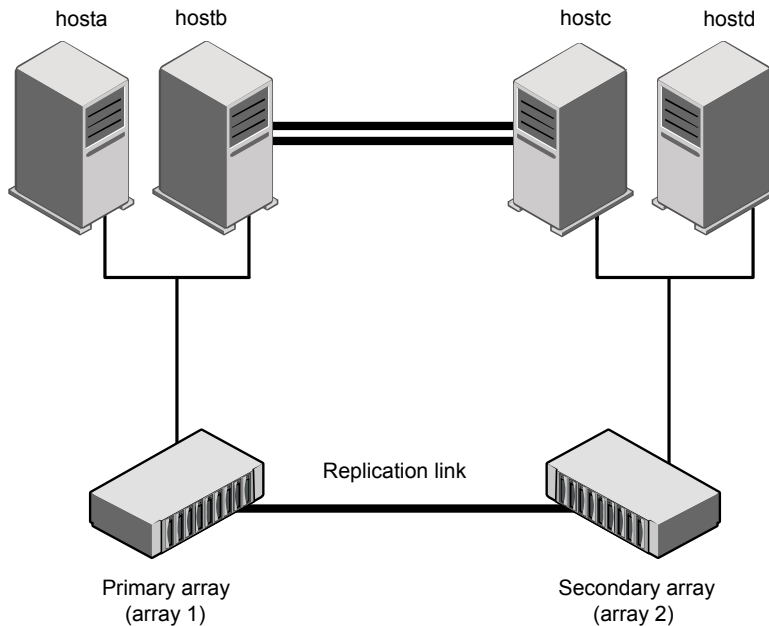
In a replicated data cluster, you can prevent unnecessary metro_mirror failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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

[Figure 3-3](#) 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 3-3 Example system zone configuration



This command creates two system zones: zone 0 with hosta and hostb, zone 1 with hostc and hostd.

Configuring the agent for IBM DS6000/8000 Metro Mirror and Global Mirror

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

- Converting their devices to metro_mirror devices
- Synchronizing the devices
- Adding the IBM DS6000/8000 Metro Mirror and Global Mirror agent to the service group

Configure IBM DS6000/8000 volumes as resources of type MetroMirror.

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

See [“Sample configuration for the Global Mirror agent”](#) on page 26.

Note: You must not change the replication state of devices from primary to secondary and from secondary to primary, outside of a VCS setup. The agent for IBM Metro Mirror and Global Mirror 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 If the agent resource type (MetroMirror) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types**, and select:
`/etc/VRTSvc/conf/MetroMirrorTypes.cf`
- 3 Click **Import**.
- 4 Save the configuration.
- 5 Add a resource of type MetroMirror at the bottom of the service group.
- 6 Configure the attributes of the MetroMirror resource.
- 7 If the service group is not configured as a global service group, configure the service group using the Global Group Configuration Wizard.
Refer to the *Cluster Server Administrator's Guide* for more information.
- 8 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.
- 9 Repeat step 5 through step 8 for each service group in each cluster that uses replicated data.

Configuring the agent manually in a replicated data cluster

Configuring the agent manually in a replicated data cluster involves the following tasks:

To configure the agent in a replicated data cluster

- 1 Start Cluster Manager and log on to the cluster.
- 2 If the agent resource type (MetroMirror) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:
`/etc/VRTSvc/conf/MetroMirrorTypes.cf`

- 3 Click **Import**.
- 4 Save the configuration.
- 5 In each service group that uses replicated data, add a resource of type MetroMirror at the bottom of the service group.
- 6 Configure the attributes of the MetroMirror resource.
- 7 Set the SystemZones attribute for the service group to reflect which hosts are attached to the same array.

Configuring the agent for IBM Global Mirror to compute RPO

In a global cluster environment, the agent for IBM Global Mirror can compute the recovery point objective (RPO), which is a disaster recovery (DR) SLA. In a DR configuration where data is replicated asynchronously to the DR site, the DR site data is not always as current as the primary site data.

RPO is the maximum acceptable amount of data loss in case of a disaster at the primary site. The agent computes RPO in terms of time, that is, in seconds.

Before you configure the agent to compute RPO, ensure the following:

- The service group containing the GlobalMirror resource and the VxVM DiskGroup resource are online at the production site.
- The DiskGroup resource is dependent on the GlobalMirror resource.

To configure the agent to compute the RPO:

- 1 In the DR cluster, on any one of the nodes where the service group is configured, run the following command to start the RPO computation:

```
hares -modify GlobalMirrorResourceName ComputeDRSLA 1 -sys
SystemName
```

- 2 Run the `GetCurrentRPO` action function on the same node in the DR cluster.

If the agent has completed computing the RPO, the agent reports the RPO. Note down this RPO for future reference.

If the RPO is not reported, it indicates that the agent needs more time to finish computing the RPO. Wait for some more time before you run the `GetCurrentRPO` action function again.

- 3 Run the following command to stop the RPO computation:

```
hares -modify GlobalMirrorResourceName ComputeDRSLA 0 -sys
SystemName
```

Managing and testing clustering support for IBM DS6000/8000 Metro Mirror and Global Mirror

This chapter includes the following topics:

- [Typical test setup for the IBM DS6000/8000 Metro Mirror and Global Mirror agent](#)
- [Testing service group migration](#)
- [Testing host failure](#)
- [Performing a disaster test](#)
- [Performing the failback test](#)

Typical test setup for the IBM DS6000/8000 Metro Mirror and Global Mirror agent

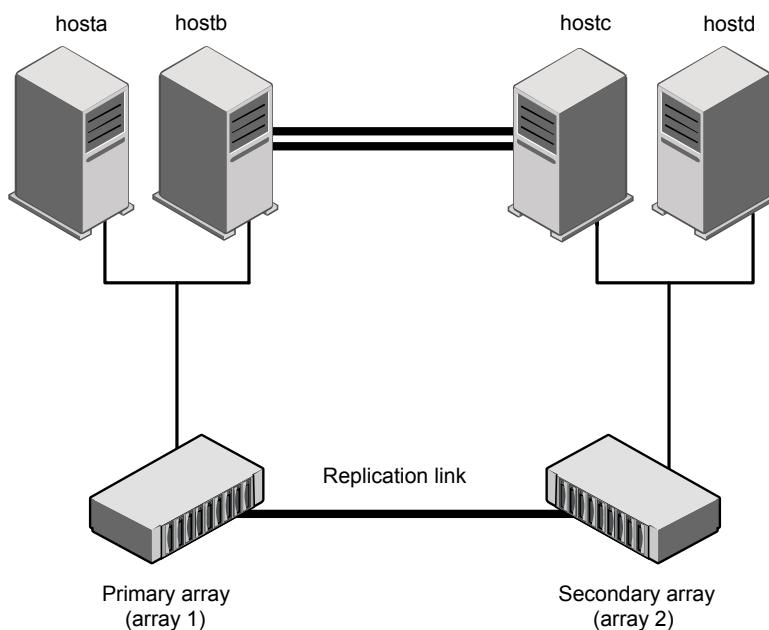
A typical test environment includes the following characteristics:

- Two hosts (hosta and hostb) are attached to the primary IBM DS6000/8000 array.
- Two hosts (hostc and hostd) are attached to the secondary IBM DS6000/8000 array.

- The application is running on hosta and volumes in the local array are read-write enabled, in the FULL DUPLEX (Metro Mirror) or COPY PENDING (Global Mirror) state.
- A replicated data cluster has two dedicated heartbeat links.
A global cluster has one network heartbeat.

Figure 4-1 depicts a typical test environment.

Figure 4-1 Typical test setup



Testing service group migration

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

To perform the service group migration test

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

Migrate the service group to a host that is attached to the same array.
- 2 Click **Switch To** and click the system that is attached to the same array (hostb) from the menu.

For Metro Mirror: The service group comes online on hostb and local volumes remain in the FULL DUPLEX state.

For Global Mirror: The service group comes online on hostb and local volumes remain in the FULL DUPLEX/COPY PENDING state.
- 3 In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group.

Migrate the service group to a host that is attached to a different array.
- 4 Click **Switch To**, and click the system that is attached to another array (hostc) from the menu.

For Metro Mirror: The service group comes online on hostc and the volumes there transition to the FULL DUPLEX state from the TARGET FULL DUPLEX state.

For Global Mirror: The service group comes online on hostc and the volumes there transition to the FULL DUPLEX/COPY PENDING state from the TARGET FULL DUPLEX/TARGET COPY PENDING state.
- 5 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.
- 6 Click **Switch To** and click the system on which the group was initially online (hosta).

The group comes online on hosta. The devices return to the original state in step 1.

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).
 For Metro Mirror: The service group fails over to hostb and devices are in the FULL DUPLEX state.
 For Global Mirror: The service group fails over to hostb and devices are in the FULL DUPLEX/COPY PENDING state.
- 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.
 In a global cluster, a cluster down alert appears and gives you the opportunity to fail over the service group manually.
 For Metro Mirror: The logical drives transition their role from secondary to primary and start on the target host.
 For Global Mirror: In both environments, the devices transition from the TARGET FULL DUPLEX/TARGET COPY PENDING to the FULL DUPLEX/COPY PENDING state and start on the target host.
- 3 Power on the two hosts that were shut down.
- 4 Switch the service group to its original host when VCS starts.
 Do the following:
 - In the **Service Groups** tab of the Cluster Explorer configuration tree, right-click the service group.
 - Click **Switch To** and click the system on which the service group was initially online (hosta).
 The service group comes online on hosta and devices swap roles again.

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 on the source side and shut down the source array.
If you cannot shut down the primary IBM DS6000/8000 arrays, disconnect the metro mirror paths and simultaneously shut down the hosts. This action mimics a disaster scenario from the point of view of the secondary site.
- 2 For Metro Mirror: In a replicated data cluster, the service group fails over to hostc or hostd if all volumes were originally in the TARGET FULL DUPLEX state and no copy or synchronization was in progress at the time of disaster.
For Global Mirror: In a replicated data cluster, the service group fails over to hostc or hostd if all volumes were originally in the TARGET FULL DUPLEX/TARGET COPY PENDING state.
- 3 In a global cluster, the administrator is notified of the failure. The administrator can then initiate the failover.
- 4 After the failover, the original target volumes go to the SUSPENDED state (Reason = "Host Source").

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 original primary hosts.
- 2 Take the service group offline using the following command:
If you run this test in a replicated data cluster, type the following command from any host:

```
hagrp -offline grpname -any
```

If you run the test in a global cluster, type the command from hostc or hostd.

- 3 For Metro Mirror: Manually resynchronize the volumes using the failback action. After the resynchronization completes, the state of the original target volumes changes to FULL DUPLEX (Reason = "-"). The state of the original source volumes changes to TARGET FULL DUPLEX (Reason = "-").

- 4 For Global Mirror: Manually resynchronize the volumes using the failback action and the StartGM action for Global Mirror. After the resynchronization completes, the state of the original target volumes changes to FULL DUPLEX/COPY PENDING (Reason = "-"). The state of the original source volumes changes to TARGET FULL DUPLEX/TARGET COPY PENDING (Reason = "-").
- 5 Migrate the application back to the original primary site.

Setting up a fire drill

This chapter includes the following topics:

- [About fire drills](#)
- [Fire drill configuration for Metro Mirror](#)
- [About the Metro MirrorSnap agent](#)
- [Before you configure the fire drill service group](#)
- [Configuring the fire drill service group](#)
- [Verifying a successful fire drill](#)
- [Sample configuration for a fire drill service group](#)

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 DS6000/8000 MetroMirror, the Metro MirrorSnap 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 is currently not supported for volumes replicated with Global Mirror.

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

The agent also supports fire drills for storage devices that are managed by native LVM on the AIX platform.

Fire drill configuration for Metro Mirror

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

VCS performs the following tasks for fire drill:

- Resynchronizes the persistent snapshot with target lun.
- Modifies the disk group name in the snapshot.
- Brings the fire drill service group online using the snapshot data.

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

About the Metro MirrorSnap agent

The Metro MirrorSnap agent is the fire drill agent for IBM DS6000/8000 MetroMirror.

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

Metro MirrorSnap agent functions

The Metro MirrorSnap agent performs the following functions:

Table 5-1 Agent functions

Function	Description
online	<ul style="list-style-type: none">■ Resynchronizes the persistent snapshot with target LUN.■ Modifies the disk group name in the snapshot.■ Creates a lock file to indicate that the resource is online.
offline	<ul style="list-style-type: none">■ Removes the lock file created by the online function.■ Optional: Refresh the snapshot from the replication target volumes at the end of the fire drill. Default is to keep the fire drill state on the snapshot volumes.

Table 5-1 Agent functions (*continued*)

Function	Description
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.

Resource type definition for the Metro MirrorSnap agent

Following is the resource type definition for the Metro MirrorSnap agent:

```
type MetroMirrorSnap (  
    static int MonitorInterval = 300  
    static int ActionTimeout = 150  
    static int NumThreads = 1  
    static int OpenTimeout = 180  
    static str AgentDirectory = "/opt/VRTSvcs/bin/MetroMirrorSnap"  
    static str ArgList[] = { TargetResName, OffRefresh }  
    str TargetResName  
    boolean OffRefresh = 0  
    temp str VCSResLock  
)
```

Attribute definitions for the Metro MirrorSnap agent

To customize the behavior of the Metro MirrorSnap agent, configure the following attributes:

Table 5-2 Agent attributes

Attribute	Description
TargetResName	<p>Name of the resource managing the LUNs that you want to take snapshot of. Set this attribute to the name of the MetroMirror 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>Name of the resource managing the LUNs that you want to take snapshot of. Set this attribute to the name of the MetroMirror resource if you want to take a snapshot of replicated data.</p> <p>Type-Dimension: string-scalar</p>
SnapshotName	
OffRefresh	<p>Specifies whether the snapshot volumes refresh as part of the offline process or they retain the last state after completing the fire drill.</p> <p>Default: 0</p> <p>The snapshot volumes keep the last state and do not refresh.</p>

Before you configure the fire drill service group

Before you configure the fire drill service group, ensure that the following pre-requisites are met:

- Make sure the application service group is configured with a MetroMirror resource.
- Make sure the infrastructure to take snapshots is properly configured between the source and target arrays.
- Make sure FlashCopy for MetroMirror is installed and configured at the target array.
- Make sure you create persistent snapshots with 'change recording' enabled.

- You must use Veritas Volume Manager or AIX LVM to import and deport the storage.
- When you resynchronize the snapshot with the target-LUN on secondary site, make sure you have persistent snapshot attached to the target LUN.
- When you take snapshots of non-replicated devices, create a IBM DS6000/8000 device group with the same name as the VxVM disk group. The device group must contain the same devices as in the VxVM disk group and have the same LUNs associated.
- Non-replicated volumes are no longer supported.
- For non-replicated devices:
 - You must use Veritas Volume Manager.
On HP-UX, you must use Veritas Volume Manager 5.0 MP1.

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 45.

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 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 toolbar.

Adding resources to the fire drill service group

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

To add resources to the service group

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

Configuring resources for fire drill service group

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

To configure the fire drill service group

- 1 In Cluster Explorer, click the **Service Group** tab in the left pane.
- 2 Click the fire drill service group in the left pane and click the **Resources** tab in the right pane.
- 3 Right-click the MetroMirror resource and click **Delete**.
- 4 Add a resource of type Metro MirrorSnap and configure its attributes.
- 5 Right-click the resource to be edited and click **View > Properties View**. If a resource to be edited does not appear in the pane, click **Show All Attributes**.
- 6 Edit attributes to reflect the configuration at the remote site. For example, change the Mount resources so that they point to the volumes that are used in the fire drill service group.

Enabling the FireDrill attribute

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

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

To enable the FireDrill attribute

- 1 In Cluster Explorer, click the **Types** tab in the left pane, right-click the type to be edited, and click **View > Properties View**.
- 2 Click **Show All Attributes**.
- 3 Double-click **FireDrill**.
- 4 In the **Edit Attribute** dialog box, enable **FireDrill** as required, and click **OK**.
- 5 Repeat the process of enabling the FireDrill attribute for all required resource types.

Verifying a successful fire drill

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

To verify a successful fire drill

- 1** Bring the fire drill service group online on a node at the secondary site that does not have the application running.

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

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

Sample configuration for a fire drill service group

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

You can configure a resource of type Metro MirrorSnap in the main.cf file as follows:

```
MetroMirrorSnap oradg_fd {  
    TargetResName = "oradf_rdf"  
}
```

Index

A

attribute definitions 19, 24

C

cluster
 heartbeats 28

D

disaster test 35
DSCliHome attribute 19, 24

F

failback test 36
fire drill
 about 38
 configuration wizard 41
 Metro MirrorSnap agent 39
 running 44
 service group for 41

H

HMC1 attribute 19, 24
HMC2 attribute 20, 25

I

IBM Metro Mirror agent
 attribute definitions 19, 24
IBM Metro Mirror agent attributes
 DSCliHome 19, 24
 HMC1 19, 24
 HMC2 20, 25
 LocalStorageImageID 19, 24
 PasswdFile 19, 24
 RemoteStorageImageID 19, 24
 User 19, 24
 VCSResLock 21, 25
 VolIds 19, 24
installing the agent
 AIX systems 15

installing the agent (*continued*)
 Linux systems 15
 Solaris systems 15

L

LocalStorageImageID attribute 19, 24

M

Metro MirrorSnap agent
 about 39
 attribute definitions 40
 operations 39
 type definition 40
migrating service group 33

P

PasswdFile attribute 19, 24

R

Recovery Point Objective (RPO)
 Configuring RPO computation support 31
RemoteStorageImageID attribute 19, 24
resource type definition
 Metro MirrorSnap agent 40

S

sample configuration 22, 26
service group
 migrating 33

T

testing
 disaster 35
 failback 36
type definition
 Metro MirrorSnap agent 40

U

- uninstalling the agent
 - AIX systems 17
 - Linux systems 17
 - Solaris systems 17
- User attribute 19, 24

V

- VCSResLock attribute 21, 25
- Vollds attribute 19, 24