Veritas™ Cluster Server Agent for IBM Metro Mirror Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

5.0

December 2007

Veritas Cluster Server Agent for IBM Metro 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: 5.0.01.1

Legal Notice

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.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Third-party legal notices

Technical support

For technical assistance, visit

http://www.symantec.com/business/support/assistance_care.jsp

and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Chapter 5 Setting up a fire drill

Index

Chapter 1

Introducing the Veritas agent for IBM Metro Mirror

This chapter includes the following topics:

About the agent for IBM Metro Mirror

The Veritas agent for IBM Metro Mirror provides support for application failover and recovery. The agent provides this support in environments that use MetroMirror 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 MetroMirror resource online also has safe and exclusive access to the configured devices.

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

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

The agent supports Metro Mirror (i.e. synchronous replication) only; the agent does not support Global Copy nor Global Mirror (i.e. asynchronous replication).

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

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

What's new in this release

The Veritas Cluster Server for IBM Metro Mirror includes the following new or enhanced features:

- The MetroMirror agent supports Solaris 2.10 on x64 platforms.

Supported software and hardware

The agent for IBM Metro Mirror 5.0.01.1 supports the following software versions:

Veritas Cluster Server	■ VCS 5.0 ■ VCS 5.0 MP1
Veritas SF for Oracle RAC	■ SF Oracle RAC 5.0 ■ SF Oracle RAC 5.0 MP1
Veritas Volume Manager	■ VxVM 5.0 ■ 5.0MP1 RP2 installed on AIX systems ■ VxVM 5.0 MP1 On HP-UX, Symantec recommends using VxVM 5.0 MP1.
Operating systems	The agent supports the following operating systems: ■ AIX 5.2 and 5.3 on pSeries ■ HP-UX 11i v2 on PI ■ Linux on x86, Intel Xeon, AMD Opteron ■ Red Hat Enterprise Linux 4 Update3 ■ SUSE Linux Enterprise Server 9 with SP3 ■ Solaris 2.8, 2.9, and 2.10 on SPARC Solaris 2.10 on x64 platform See the product's Release Notes for more details on the supported architectures and the operating systems.

The agent supports all versions of IBM DSCLI.

The agent supports MetroMirror on all microcode levels on all IBM DS8000 arrays.

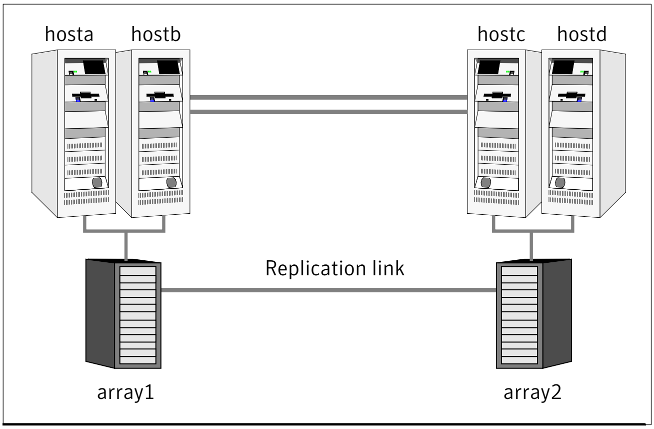
This support only exists if the host, the HBA, and the array combination is in IBM's hardware compatibility list.

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

Typical IBM Metro Mirror setup in a VCS cluster

Figure 1-1 displays a typical cluster setup in a MetroMirror environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a MetroMirror 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 DS8000 array that contains the MetroMirror primary devices.
- The secondary array (array2) has one or more secondary hosts. A Fibre Channel or SCSI directly attaches these hosts to a IBM DS8000 array that contains the MetroMirror secondary devices. The secondary devices are paired with the primary devices in the primary array. The secondary hosts and arrays must be at a significant distance to survive a disaster that may occur at the primary side.
- Network heartbeating between the two data centers to determine their health; this network heartbeating could be LLT or TCP/IP.
  See "About cluster heartbeats" on page 23.
- In a replicated data cluster environment, all hosts are part of the same cluster. You must connect them with the dual and dedicated networks that support LLT.
- In a global cluster environment, you must attach all hosts in a cluster to the same IBM DS8000 array.
- In parallel applications like Veritas Storage Foundation for Oracle RAC, all hosts that are attached to the same array must be part of the same GAB

membership. Veritas Storage Foundation for Oracle RAC is supported with MetroMirror only in a global cluster environment and not in a replicated data cluster environment.

IBM Metro Mirror agent operations

The Veritas 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 operations:

online

If the state of all local devices is read-write enabled, the agent creates a lock file on the local host. The lock file indicates that the resource is online. This operation makes the devices writable for the application.

If all local devices are in the WRITE-DISABLED state, the agent runs a `failoverpprc` command to enable read-write access to the devices.

For target volumes in the TARGET FULL DUPLEX state, the agent runs the `failoverpprc` command to make the volumes writable.

If the original primary volumes are still accessible, the agent runs the `failbackpprc` command to reverse the direction of replication.

offline

Removes the lock file from the host. The agent does not run any MetroMirror 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 entry point reports the status of the resource as online. If the lock file does not exist, the monitor entry point reports the status of the resource as offline.

open

Removes the lock file on the host where the entry point is called. This operation prevents potential concurrency violation if the service group fails over to another node.

Note that the agent does not remove the lock file if the agent was started after running the `hastop -force` command.

clean

Determines if it is safe to fault the resource if the online entry point 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.

action	Performs a failbackpprc from the original secondary side to merge any changed tracks from the original secondary to the original primary.

Installing and removing the agent for IBM Metro Mirror

This chapter includes the following topics:

Before you install the agent for MetroMirror

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

Set up replication and the required hardware infrastructure.

See "Typical IBM Metro Mirror setup in a VCS cluster" on page 9.

Installing the agent for MetroMirror

You must install the IBM Metro 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.

To install the agent on AIX systems

1 Determine the device access name of the disc drive.

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

The output resembles:

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

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

2 Insert the disc into the system's drive.

3 Mount the disc.

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

4 Navigate to the location of the agent packages:

```
# cd /cdrom/aix/replication/metro_mirror_agent/version/pkgs
```

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

5 Add the filesets for the software.

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

To install the agent on HP-UX systems

1 Insert the disc into the system's drive.

2 Create a mount point directory. For example, /cdrom. The directory must have read-write permissions.

3 Determine the block device file for the disc drive.

```
# ioscan -fnC disk
```

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

4 Start the Portable File System (PFS).

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

5. Mount the disc.

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

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

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

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

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

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

To install the agent on Linux systems

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

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

4. Navigate to the /mnt directory.

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

5. Navigate to the location of the agent package.

   ```
   # cd linux/linux/platform/replication/metro_mirror_agent
   /version/rpms/
   ```

   The variable `platform` represents the Linux distribution and architecture.

   The following are the platform values:

   - redhatlinux, redhatlinuxX86_64
   - suselinux, suselinuxX86_64

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

6 Install the agent software:

```
# rpm -ivh agentrpm
```

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

To install the agent on Solaris systems

1 Insert the disc into the system's drive.

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

2 Navigate to the location of the agent package.

```
# cd solaris/sparc/platform/replication/metro_mirror_agent
/version/rpms/
```

The variable *platform* represents the Solaris distribution and architecture.

The following are the platform values:

- x64
- sparc

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

3 Install the agent binaries.

```
pkgadd -d . VRTSvcsi
```

Upgrading the agent for MetroMirror

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 MetroMirror" 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 MetroMirror" on page 13.

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

   Configure the new attributes, if applicable.

8. Verify the configuration

   ```
   # hacf -verify config
   ```

9. Start VCS on local node first.

10. Start VCS on other nodes.

Removing the agent for MetroMirror

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

To remove the agent from an AIX cluster

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

  ```
  # installp -u VRTSvcsi
  ```

To remove the agent from an HP-UX cluster

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

  ```
  # swremove VRTSvcsi
  ```

To remove the agent from a Linux cluster

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

  ```
  # rpm -e VRTSvcsi
  ```

To remove the agent from a Solaris cluster

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

  ```
  # pkgrm VRTSvcsi
  ```

Chapter 3

Configuring the agent for IBM Metro Mirror

This chapter includes the following topics:

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

```
type MetroMirror (
    static keylist SupportedActions = {failback}
    static int MonitorInterval = 300
    static int NumThreads = 1
    static str ArgList[] = { DSCliHome, HMC1, HMC2, User,
        PasswdFile, LocalStorageImageID,
        RemoteStorageImageID, VolIds }
    str DSCliHome = "/opt/ibm/dscli"
    str HMC1
    str HMC2
    str User
    str PasswdFile
    str LocalStorageImageID
```

```
        str RemoteStorageImageID
        str VolIds{}
        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.

DSCliHome

Path to the DS8000 command line interface.

Type-dimension: string-scalar

Default is: /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.

Default is: admin.

Type-dimension: string-scalar

PasswdFile

Specifies the password file that contains your password. See the `managepwfile` DSCLI command for information on how to generate a password file. This is an optional attribute.

Default is: ~/dscli/security.dat

Type-dimension: string-scalar

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

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

VolIds

IDs of local DS8000 MetroMirror volumes that the agent manages.

Type-dimension: string-keylist

Optional attributes

Configuring these attributes is optional.

HMC2

IP address or host name of the secondary management console.

Type-dimension: string-scalar

Internal attributes

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

VCSResLock

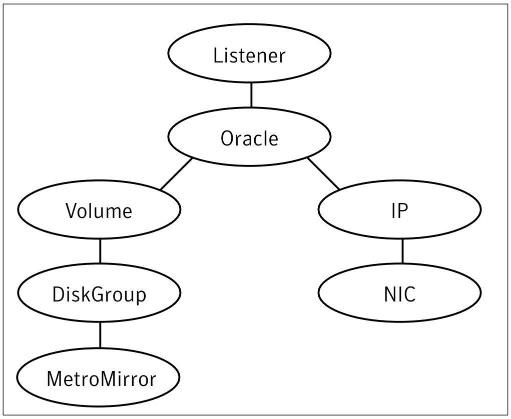
The agent uses the VCSResLock attribute to guarantee serialized management in case of a parallel application.

Type-dimension: temporary string-scalar

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 MetroMirroragent



The DiskGroup resource depends on the MetroMirror resource.

You can configure a resource of type Metro Mirror 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 MetroMirror 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 MetroMirror 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

Before you configure the agent for MetroMirror

Before you configure the agent, review the following information:

- Review the configuration concepts, which describe the agent's type definition and attributes.
  See "Configuration concepts for the Metro Mirror agent" on page 19.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical IBM Metro Mirror setup 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.
- Make sure that the cluster has an effective heartbeat mechanism in place.
  See "About cluster heartbeats" on page 23.
- Set up system zones in replicated data clusters.
  See "About configuring system zones in replicated data clusters" on page 23.

- 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 don't take effect until after a reboot. If these environment variables are not set, the MetroMirror 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

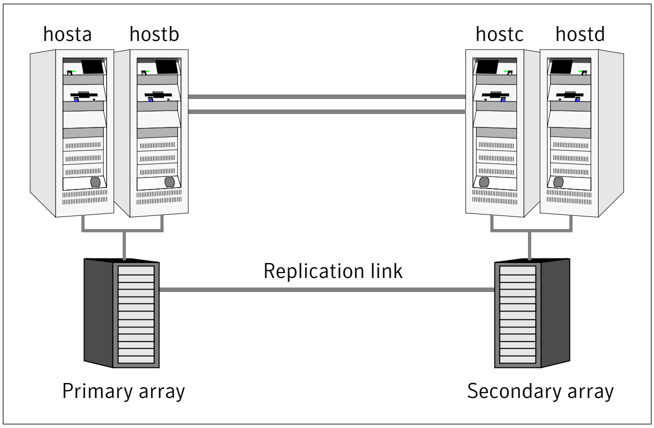
In a replicated data cluster, you can prevent unnecessary MetroMirror failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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



Configuring the agent for MetroMirror

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

- Converting their devices to MetroMirror devices
- Synchronizing the devices
- Adding the IBM Metro Mirror agent to the service group

Configure IBM DS8000 volumes as resources of type MetroMirror.

Configuring the agent manually in a global cluster

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

To configure the agent in a global cluster

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

   /etc/VRTSvcs/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 group, configure the service group using the Global Group Configuration Wizard.

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

8 To configure the agent to manage the volumes that Veritas Storage Foundation for Oracle RAC uses:

- Configure the SupportedActions attribute for the CVMVolDg resource
- Add the following keys to the list: import, deport.

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

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

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

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/VRTSvcs/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. Note that some attributes must be localized to reflect values for the hosts that are attached to different arrays.

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

Chapter 4

Managing and testing clustering support for IBM Metro Mirror

This chapter includes the following topics:

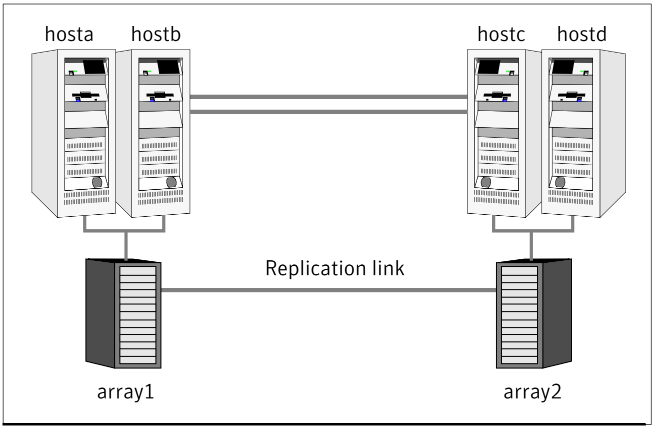
Typical test setup for the IBM Metro Mirror agent

A typical test environment includes the following characteristics:

- Two hosts (hosta and hostb) are attached to the primary IBM DS8000array.
- Two hosts (hostc and hostd) are attached to the secondary IBM DS8000 array.
- The application runs on hosta and volumes in the local array are read-write enabled in the FULL DUPLEX state.

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. Migrate the service group to a host that is attached to the same array.

   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 that is attached to the same array (hostb) from the menu.
     The service group comes online on hostb and local volumes remain in the FULL DUPLEX state.

2. Migrate the service group to a host that is attached to a different array.

   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 that is attached to the another array (hostc) from the menu.
     The service group comes online on hostc and the volumes there transition to the FULL DUPLEX state from the TARGET FULL DUPLEX state.

3. Migrate the service group back to its original host.

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 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).

The service group fails over to hostb and devices are in the FULL DUPLEX state.

2 Halt or shut down hostb.

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

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

The devices transition from the TARGET FULL DUPLEX to the FULL DUPLEX state and start on the target host.

3 Reboot 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 can not shut down the primary DS8000, 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 side.

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.

In a global cluster, the administrator is notified of the failure. The administrator can then initiate the failover.

2 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.

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 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 Migrate the application back to the original primary side.

Chapter 5

Setting up a fire drill

This chapter includes the following topics:

About fire drills

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

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

In clusters employing IBM Metro Mirror, the MetroMirrorSnap resource manages the replication relationship during a fire drill.

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

The agent supports fire drills only for storage devices that are managed using Veritas Volume Manager 5.0, which is a component of Veritas Storage Foundation. On HP-UX, you must use Veritas Volume Manager 5.0 MP1.

Fire drill configurations

VCS supports the following fire drill configurations for the agent:

Gold

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

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

In the Gold configuration, VCS does the following:

- 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.

For Gold configurations, you must use Volume Manager to import and deport the storage.

Silver

VCS takes a snapshot, but does not run the fire drill on the snapshot data. VCS breaks replication and runs the fire drill on the replicated target device. If a disaster occurs while resynching data after running the fire drill, you must switch to the snapshot for recovery.

In the Silver configuration, VCS does the following:

- Resynchronizes the persistent snapshot with the target LUN.
- Suspends replication.
- Modifies the disk group name in the snapshot.
- 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.

Bronze

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

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

In the Bronze configuration, VCS does the following:

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

Note: If you use DS6000 arrays, you can run only the Gold configuration. If you use DS8000 arrays, you can run any fire drill configuration.

About the MetroMirrorSnap agent

The MetroMirrorSnap agent is the fire drill agent for IBM Metro Mirror technology. The agent manages the replication relationship between the source and target arrays when running a fire drill. Configure the MetroMirrorSnap resource in the fire drill service group, in place of the MetroMirror resource.

MetroMirrorSnap agent operations

The MetroMirrorSnap agent performs the following operations:

Online

Gold Configuration

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

Silver Configuration

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

Bronze Configuration

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

Offline

Gold Configuration

- Removes the lock file created by the online operation.

Silver Configuration

- Resumes replication between the source and the target arrays.
- Removes the lock file created by the online operation.

Bronze Configuration

- Resumes the replication between the source and the target arrays.
- Removes the lock file created by the Online operation.

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 operation.

Resource type definition for the MetroMirrorSnap agent

Following is the resource type definition for the MetroMirrorSnap agent:

```
type MetroMirrorSnap (
    static int MonitorInterval = 300
    static int NumThreads = 1
    static str ArgList[] = { TargetResName, MountSnapshot,
        UseSnapshot, RequireSnapshot }
    str TargetResName
    int MountSnapshot
    int UseSnapshot
    int RequireSnapshot
    temp str VCSResLock)
```

Attribute definitions for the MetroMirrorSnap agent

To customize the behavior of the MetroMirrorSnap 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 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.

For example, in a typical Oracle setup, you might replicate data files and redo logs, but you may choose to avoid replicating temporary tablespaces. The temporary tablespace must still exist at the DR site and may be part of its own disk group.

Type-dimension: string-scalar

UseSnapshot

Specifies whether the MetroMirrorSnap resource takes a local snapshot of the target array. Set this attribute to 1 for Gold and Silver configurations. For Bronze, set this attribute to 0.

Type-Dimension: integer-scalar

See “About the Snapshot attributes” on page 35.

RequireSnapshot

Specifies whether the MetroMirrorSnap resource must take a snapshot before coming online.

Set this attribute to 1 if you want the resource to come online only after it succeeds in taking a snapshot.

Set this attribute to 0 if you do want the resource to come online even if it fails to take a snapshot. Setting this attribute to 0 creates the Bronze configuration.

Type-Dimension: integer-scalar

Note: Set this attribute to 1 only if UseSnapshot is set to 1.

MountSnapshot

Specifies whether the resource uses the snapshot to bring the service group online. Set this attribute to 1 for Gold configuration. For Silver and Bronze configurations, set the attribute to 0.

Type-Dimension: integer-scalar

Note: Set this attribute to 1 only if UseSnapshot is set to 1.

VCSResLock

Do not modify. For internal use only.

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 MetroMirrorSnap resource replaces the MetroMirror resource.

The following configuration creates a Gold fire drill configuration, but allows VCS to run a Bronze fire drill if the snapshot does not complete successfully.

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

```
MetroMirrorSnap oradg_fd {
    TargetResName = "oradf_rdf"
    UseSnapshot = 1
    RequireSnapshot = 0
    MountSnapshot = 1
    }
```

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 MetroMirror resource.
- Make sure the infrastructure to take snapshots is properly configured between the source and target arrays.
- When you use the Gold or Silver configuration, make sure FlashCopy for MetroMirror is installed and configured at the target array.
- Make sure you create persistent snapshots.
- For the Gold configuration, you must use Veritas Volume Manager 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 DS8000 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.
- For non-replicated devices:
  - You must use Veritas Volume Manager.
    On HP-UX, you must use Veritas Volume Manager 5.0 MP1.
  - You must use the Gold configuration without the option to run in the Bronze mode. Set the RequireSnapshot attribute to 1.

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 35.

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

You can create the fire drill service group using the Cluster Manager (Java Console).

See “Creating the fire drill service group using Cluster Manager (Java Console)” on page 37.

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

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

To create the fire drill service group

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

To disable the AutoFailOver attribute

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

Adding resources to the fire drill service group

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

To add resources to the service group

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

Configuring resources for fire drill service group

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

To configure the fire drill service group

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

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

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

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

Enabling the FireDrill attribute

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

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

To enable the FireDrill attribute

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

2 Click **Show All Attributes**.

3 Double click **FireDrill**.

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

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

Verifying a successful fire drill

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

To verify a successful fire drill

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

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

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

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

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

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

Index