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

Windows Server 2003, Windows Server 2008

5.1 Service Pack 2

✦ symantec™

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: 5.1.SP2.0

Document version: 5.1.SP2.0.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

For information about Symantec's support offerings, you can visit our Web site 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

Documentation feedback

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:

sfha_docs@symantec.com

Support agreement resources

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

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

Contents

Introducing the Veritas agent for IBM Metro Mirror

This chapter includes the following topics:

- About the agent for IBM Metro Mirror
- Supported software for IBM Metro Mirror
- Typical IBM Metro Mirror in a VCS cluster
- IBM MetroMirror agent functions

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 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 supports Metro Mirror (i.e. synchronous replication) as well as Global Mirror (i.e. asynchronous replication).

Note: On Windows, replication LUNs and FlashSnap LUNs must not be visible to the host at the same time.

Supported software for IBM Metro Mirror

The IBM Metro Mirror agent supports Storage Foundation and High Availability Solutions 5.0 and 5.1 for Windows.

The agent supports version 5.4.0.656 or later of IBM DSCLI.

Typical IBM Metro 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
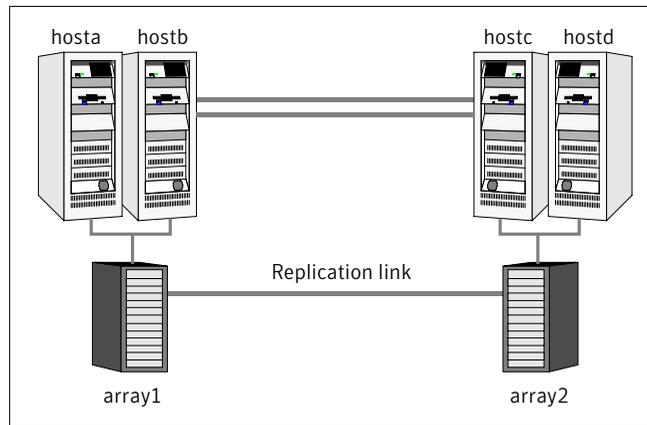
Clustering in a Metro Mirror environment typically consists of the following hardware infrastructure:

■ The primary array (array1) has one or more primary hosts. A Fibre Channel or SCSI directly attaches these hosts to the IBM DS8000 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 a IBM DS8000 array that contains MetroMirror/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*.

> **Note:** On Windows, you must not include the flashcopy devices in the volume group or connect to the host.

- 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; this network heartbeating could be LLT or TCP/IP.

  See "About cluster heartbeats" on page 20.

- 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.

IBM MetroMirror agent functions

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 functions:

online	If the state of all local devices is read-write enabled i.e. "FULL DUPLEX" or "SUSPENDED", the agent creates a lock file on the local host. The lock file indicates that the resource is online.
	If the local devices are target devices with "TARGET FULL DUPLEX" state, the agent runs the failoverpprc command to make the volumes writable. This operation makes the devices writable for the application. After successful execution of this command, the agent creates lock file on the local host.
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 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 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 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 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 IBM Metro Mirror
- Installing the agent for Metro Mirror
- Removing the agent for Metro Mirror

Before you install the agent for IBM Metro Mirror

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.

Installing the agent for Metro Mirror

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.

To install the VCS agent for

1   Log on to any node in the cluster.

    Ensure that the logged on user has the domain administrative privileges.

2   Download the complete agent pack tarball from FileConnect site:

    https://fileconnect.symantec.com/

    Alternatively,

    Download the individual agent tarball from the Symantec Veritas Operations
    Services (VOS) site:

    https://vos.symantec.com/home

3   Uncompress the file to a temporary location.

4   If you downloaded the complete Agent Pack tarball, navigate to the directory
    containing the package for the platform running in your environment.

Windows 2008 x86	`cd1\windows\w2k8x86\vcs\` `replication\metromirror_agent\vcs_version\` `version_agent\pkgs`
Windows 2008 x64	`cd1\windows\w2k8x64\vcs\` `replication\metromirror_agent\vcs_version\` `version_agent\pkgs`
Windows 2008 IA64	`cd1\windows\w2k8IA64\vcs\` `replication\metromirror_agent\vcs_version\` `version_agent\pkgs`
Windows 2003 x64	`cd1\windows\w2k3x64\vcs\` `replication\metromirror_agent\vcs_version\` `version_agent\pkgs`
Windows 2003 x86	`cd1\windows\w2k3x86\vcs\` `replication\metromirror_agent\vcs_version\` `version_agent\pkgs`
Windows 2003 IA64	`cd1\windows\w2k3IA64\vcs\` `replication\metromirror_agent\vcs_version\` `version_agent\pkgs`

5   Double-click **vrtsvcsagentname.msi.**

    Follow the instructions that the install program provides, to complete the
    installation of Veritas Cluster Server agent.

If you installed the Metro Mirror when you installed Veritas Storage Foundation and High Availability for Windows, follow these instructions to install the agent.

This removes the existing Metro Mirror agent. You can now follow the procedures to install the new agent from the agent pack CD.

Removing the agent for Metro Mirror

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

To remove the agent Metro Mirror

1 Open the Windows Control Panel and click **Add or Remove Programs.**

2 Select Veritas Cluster Server Enterprise Agent for IBM Metro Mirror or VRTSvcsi.

3 Click the **Remove** button.

4 The installer guides though the uninstallation procedure.

5 Complete the uninstallation.

Note: For Win IA64 and Win x64 architectures, you must manually delete the agent directory if it is not removed after the uninstallation.

Configuring the agent for IBM Metro Mirror

This chapter includes the following topics:

-
-
-

Configuration concepts for the MetroMirror agent

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

Resource type definition for the MetroMirror 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 = "C:\Program_Files\ibm\dscli"
    str HMC1
    str HMC2
    str User
    str PasswdFile
    str LocalStorageImageID
    str RemoteStorageImageID
```

```
                 str VolIds{}
                 temp str VCSResLock
        )
```

Attribute definitions for the MetroMirror 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: C:\Program Files\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.
	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
DSMon	Checks the state of the replicated volumes as part of monitor function.
	Possible values are as follows:
	Default is 0
	1 when the resource is supposed to be online and lock file exists.
	2 when the resource is supposed to be offline and lock file is removed.
	3 = always
	Type-dimension: scalar-integer
AutoFailBack	Executes failbackpprc 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.
	Type-dimension: scalar-boolean
	Default is 1

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

Before you configure the agent for IBM Metro Mirror

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 MetroMirror agent" on page 17.

- Verify that you have installed the agent on all systems in the cluster.

- Verify the hardware setup for the agent.

- 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 20.

- Set up system zones in replicated data clusters.
  See "About configuring system zones in replicated data clusters" on page 20.

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

Use the SystemZones attribute to create these zones.

Figure 3-1   Example system zone configuration
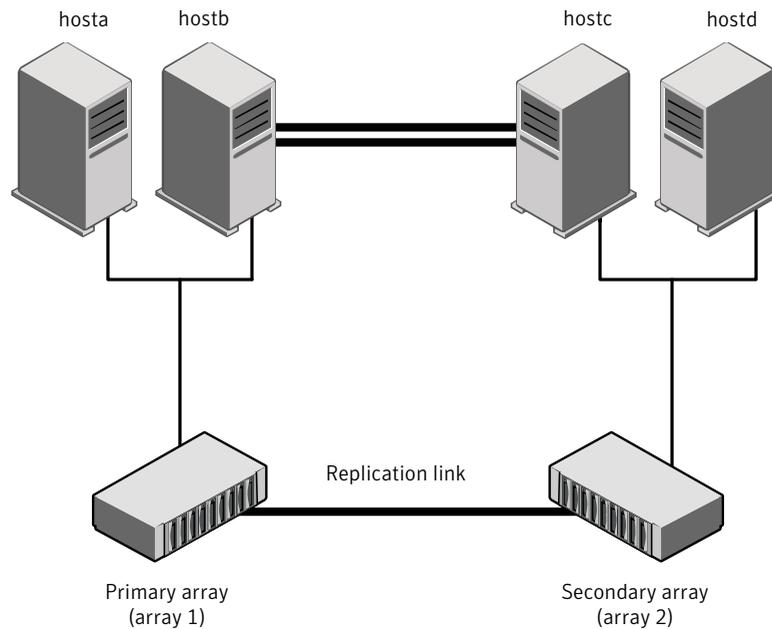
Modify the SystemZones attribute using the following command:

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

The variable grpname represents the service group in the cluster.

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

Configuring the agent for IBM Metro Mirror

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

■ Converting their devices to Metro Mirror devices

■ Synchronizing the devices

■ Adding the IBM Metro Mirror agent to the service group

Configure IBM DS8000 volumes as resources of type Metro Mirror.

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

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

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 (Metro Mirror) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

   <systemdrive>\Program Files\Veritas\cluster server\conf\Sample_Metro Mirror\Metro MirrorTypes.cf

3   Click **Import**.

4   Save the configuration.

5   Add a resource of type Metro Mirror at the bottom of the service group.

6   Configure the attributes of the Metro Mirror resource.

7   If the service group is not configured as a global service group, configure the service group using the Global Group Configuration Wizard.

   See the *Veritas Cluster Server Administartor'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 (Metro Mirror) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

```
Program Files\Veritas\Cluster Server\conf\config\Metro
MirrorTypes.cf.
```

3   Click **Import**.

4   Save the configuration.

5   In each service group that uses replicated data, add a resource of type Metro Mirror at the bottom of the service group.

6   Configure the attributes of the Metro Mirror 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.

Managing and testing clustering support for IBM Metro Mirror

This chapter includes the following topics:

- Typical test setup for the IBM Metro Mirror agent

- Testing service group migration

- Testing host failure

- Performing a disaster test

- Performing the failback test

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.

- 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
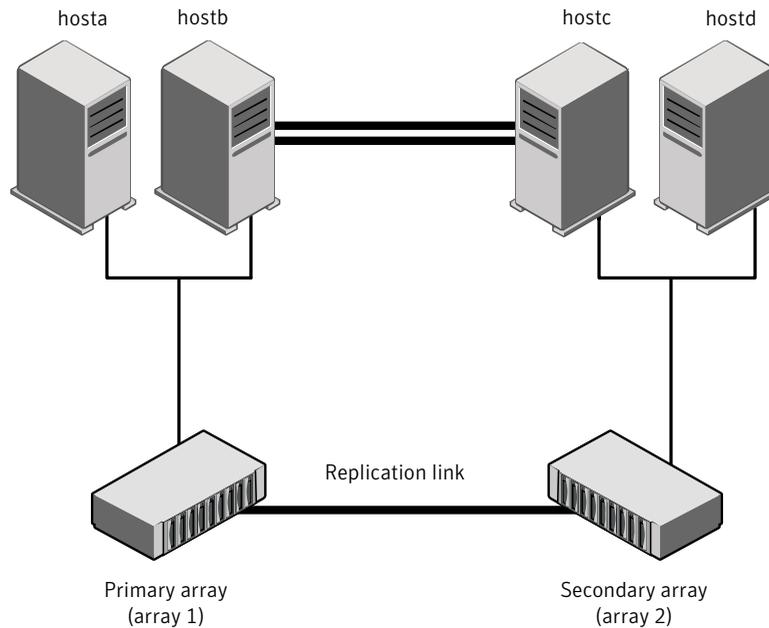
Testing service group migration

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

To perform the service group migration test

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

Migrate the service group to a host 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 MetroMirror: The service group comes online on hostb and local volumes remain in the FULL DUPLEX 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.

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.

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 MetroMirror: The logical drives transition their role from secondary to primary 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 DS8000 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 MetroMirror: 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.

3   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   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   Migrate the application back to the original primary site.

Index

V