Cluster Server Agent for IBM DS4K RemoteMirror Installation and Configuration Guide

Linux, Solaris

5.0

VERITAS™

Cluster Server Agent for IBM DS4K RemoteMirror 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

Document version: 5.0 Rev 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 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

Introducing the agent for IBM DS4K RemoteMirror

This chapter includes the following topics:

About the agent for IBM DS4K RemoteMirror

The Cluster Server agent for IBM DS4K RemoteMirror provides support for application failover and recovery. The agent provides this support in environments that use DS4000/5000 MetroMirror to manage replication relationships that are defined inside the IBM DS4000/5000 arrays.

The agent manages all the remote pairs or replication relationships created between the logical drives of two IBM DS4000/5000 storage arrays.

The agent monitors and manages the state of replicated logical drives within IBM DS4000/5000 arrays that are attached to VCS nodes. The agent ensures that the system that has the DS4KRemoteMirror resource online also has safe and exclusive access to the configured logical drives.

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 (i.e. synchronous 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 DS4K RemoteMirror supports, see the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

Supported hardware for DS4KRemoteMirror

The agent supports DS4KRemoteMirror on all microcode levels on all IBM DS4000/5000 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 DS4K RemoteMirror setup in a VCS cluster

Figure 1-1 displays a typical cluster setup in a DS4KRemoteMirror environment.

Figure 1-1   Typical clustering setup for the agent
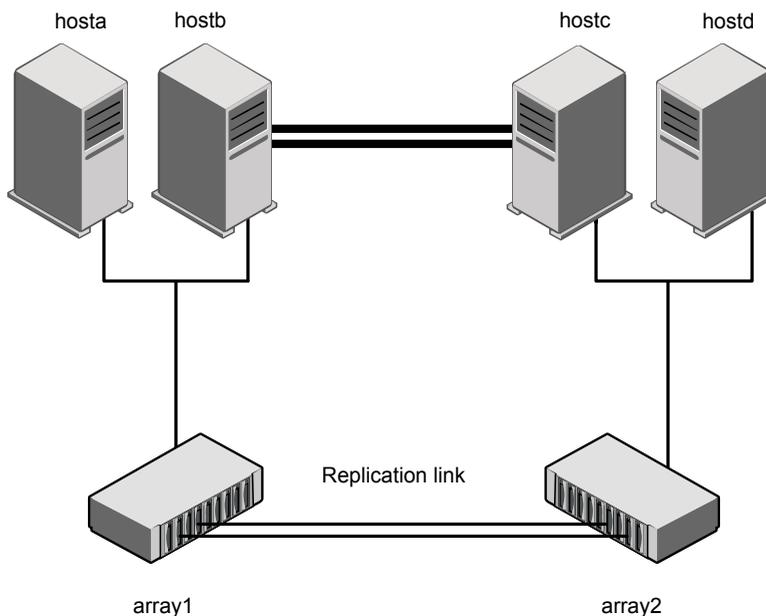
Clustering in a DS4KRemoteMirror environment typically consists of the following
hardware infrastructure:

- The primary array (array1) has one or more primary hosts. A Fibre Channel or
  SCSI directly attaches these hosts to the IBM DS4000/5000 array that contains
  the Metro Mirror logical drives.

- The secondary array (array2) has one or more secondary hosts. A Fibre Channel
  or SCSI directly attaches these hosts to a IBM DS4000/5000 array that contains
  MetroMirror target logical drives. The target logical drives are paired with the
  primary logical drives 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.

- SMClient must be installed on all the cluster nodes.

- 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 DS4000/5000 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 DS4KRemoteMirror only in a global cluster environment and not in a replicated data cluster environment.

IBM DS4K RemoteMirror agent functions

The Cluster Server agent for IBM Metro Mirror monitors and manages the state of replication relationships of a list of logical drives within DS4000 arrays that are attached to VCS nodes.

The agent performs the following functions:

Table 1-1   Agent functions

Function	Description
online	Ensures that the role of all configured logical drives are primary.
	If the name of the logical drives are identical, this operation determines the ID of the logical drive in order to differentiate between the primary and secondary logical drives.
	Determines the role and replication state of all logical drives and calculates the effective role and replication state.
	Role reversal of the logical drive occurs based on whether the replication state is sychronized and the value of the SplitTakeover attribute.
	If the value of the SplitTakeover attribute is set to 0, VCS waits for the administrator to intervene to failover to secondary. If the value of the SplitTakeover attribute is set to 1, VCS waits for the administrator to intervene to failover to secondary.
	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.
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.

Table 1-1   Agent functions *(continued)*

Function	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. There is no detailed monitoring.
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.
info	Modify or add the resource information of the resource for DS4KRemoteMirror for attribute ReplicationStatus with effective replication state.
actions/RMStatus	Retrieves the mapping and the state of each configured logical drive. This is a purely informational action entry point with no operational impact. It indicates the effective replication state in the engine log.
actions/PreSwitch	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 `hagrp -switch` command. For this, the PreSwitch attribute must be set to 1. The option `-nopre` indicates that the VCS engine must switch the servicegroup regardless of the value of the PreSwitch service group attribute.
	This operation exits with 1 if the effective replication state is not in synchronized state, else with 0.
	If running the PreSwitch action fails, the failover should not occur. This minimizes the application downtime and data loss.

Installing and removing the agent for IBM DS4K RemoteMirror

This chapter includes the following topics:

- Before you install the agent for IBM DS4K RemoteMirror

- Installing the agent for IBM DS4K RemoteMirror

- Removing the agent for IBM DS4K RemoteMirror

Before you install the agent for IBM DS4K RemoteMirror

Before you install the Cluster Server agent for IBM DS4K RemoteMirror, 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*.

Prerequisites for using the IBM DS4K RemoteMirror agent

Following are the prerequisites for starting a MetroMirror service prior to using the IBM DS4K RemoteMirror agent:

- Establish a fiber channel path between the logical subsystems used for the replication.

- Create two mirror repository logical drives, one for each controller in the storage subsystem when you activate the Enhanced Remote Mirroring premium feature on the storage subsystem.

- Add the hostname, user, and password to the storage subsystem.

- A mirror pair (synchronous replication) relationship must be created between each source and target logical drives and activated for the Enhanced Remote Mirroring feature.

Installing the agent for IBM DS4K RemoteMirror

You must install the IBM DS4K RemoteMirror 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.

    Linux   `cd1/linux/generic/vcs/replication/ds4kremotemirror_agent/`
             `agent_version/rpms/`

    Solaris `cd1/solaris/dist_arch/vcs/replication/ds4kremotemirror_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.

Linux	`# rpm -ihv \`
	`VRTSvcsi4-`*AgentVersion*`-Linux_GENERIC.noarch.rpm`
Solaris	`# pkgadd -d . VRTSvcsi4`

Removing the agent for IBM DS4K RemoteMirror

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:

Linux	`# rpm -e VRTSvcsi4`
Solaris	`# pkgrm VRTSvcsi4`

Configuring the agent for IBM DS4K RemoteMirror

This chapter includes the following topics:

- Configuration concepts for the IBM DS4K RemoteMirror

- Before you configure the agent for IBM DS4K RemoteMirror

- Configuring the agent for IBM DS4K RemoteMirror

Configuration concepts for the IBM DS4K RemoteMirror

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 DS4KRemoteMirror agent

Review the description of the agent attributes.

Required attributes

You must assign values to required attributes.

Table 3-1   Required attributes

Attribute	Description
SMCliHome	Base directory where the SMCli binary is installed.
	Default is: /opt/IBM_DS4000/client.
	Type-dimension: string-scalar
SplitTakeover	Indicates whether VCS should failover to secondary node automatically or wait for the administartor to intervene during a link failure or an unsynchornized replication state.
	If set to 0, VCS will wait for the administartor to intervene.
	If set to 1, VCS will failover to the secondary node.
	Type dimension: integer-scaler
Mode	Used at the time of failover to decide which commands to use to failover to the other site. The values for this attribute can be asynchronous or synchronous.
	Metro Mirror supports the synchronous mode and Global Mirror supports the asynchronous mode. Only the MetroMirror synchronous mode is supported.
	Type-dimension: string-scalar

Table 3-1   Required attributes *(continued)*

Attribute	Description
LocalStorageName	List of IP address or hostname of local storage subsystem or controller.
	The first accessible IP address is used in the SMCLI.
	Type-dimension: string-scalar
LogicalDrives	List of primary logical drives on the locally attached array used for the mirror pair.
	Type-dimension: string-scalar

Internal attributes

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

Table 3-2   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

Sample configuration for the IBM DS4K RemoteMirror agent

Figure 3-1 shows the dependency graph for a VCS service group with a resource of type DS4KRemoteMirror.

Figure 3-1   Sample configuration for the DS4KRemoteMirroragent
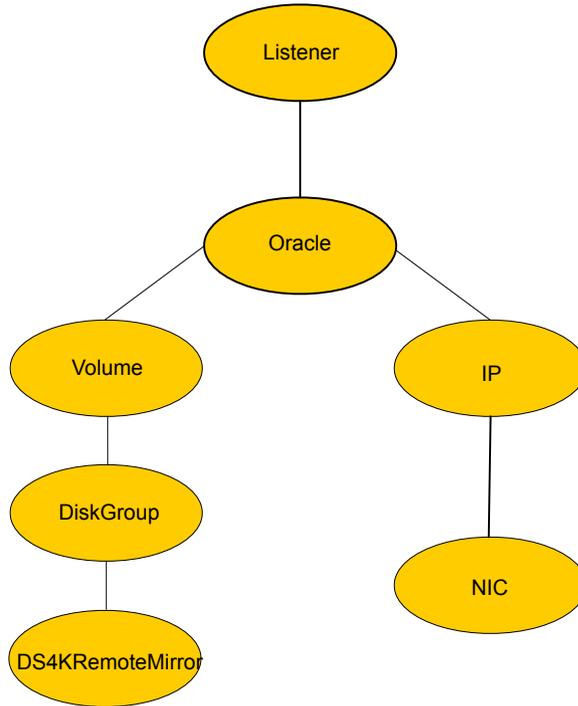
The DiskGroup resource depends on the DS4KRemoteMirror resource.

You can configure a resource of type DS4kRemoteMirror as follows in main.cf:

```
DS4KRemoteMirror ora_ds4k (
        SplitTakeover = 0
        Mode = sync
        LocalStorageName = { "10.182.1.188"}
        LogicalDrives = { PrimaryOraDrive1, PrimaryOraDrive2 }
        )
```

This resource manages the following objects:

- A group of two logical drives: PrimaryOraDrive1 and PrimaryOraDrive2 that are used by the locally connected DS4K storage with IP "10.182.1.188".

- The mode of replication is synchronous.

Before you configure the agent for IBM DS4K RemoteMirror

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 DS4K RemoteMirror setup in a VCS cluster" on page 9.

- Make sure that DS4KRemoteMirror 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 SMCLI password file. Use the `managepwd` SMCLI command to do so.

- Reboot the node after the SMCLI software is installed on that node. The SMCLI installation sets some system environment variables that don't take effect until after a reboot. If these environment variables are not set, the DS4KRemoteMirror 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 DS4KRemoteMirror 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.

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

Figure 3-2   Example system zone configuration
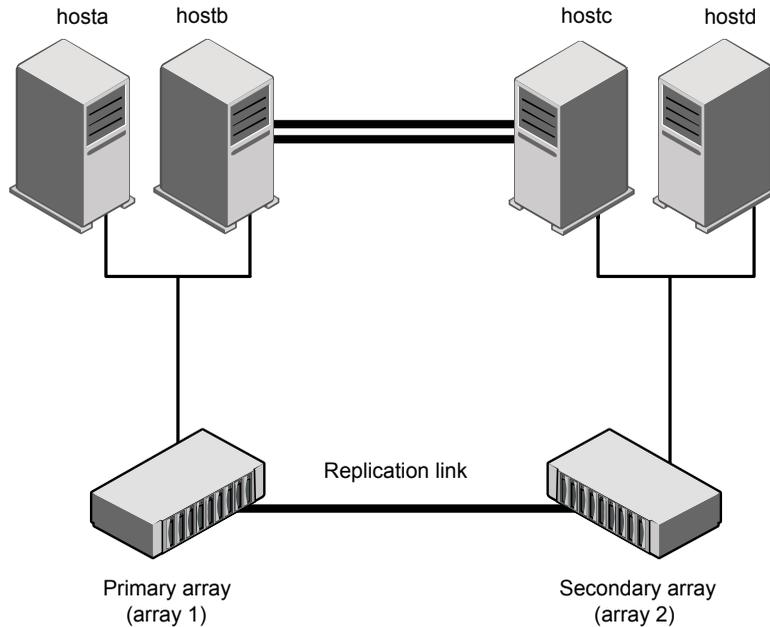
About preventing split-brain

Split-brain occurs when all heartbeat links between the primary and secondary hosts are cut. In this situation, each side mistakenly assumes that the other side is down. You can minimize the effects of split-brain by ensuring that the cluster heartbeat links pass through a similar physical infrastructure as the replication links. When you ensure that both pass through the same infrastructure, if one breaks, so does the other.

Sometimes you cannot place the heartbeats alongside the replication links. In this situation, a possibility exists that the cluster heartbeats are disabled, but the replication link is not. A failover transitions the original primary to secondary and secondary to primary. In this case, the application faults because its underlying volumes become write-disabled, causing the service group to fault. VCS tries to fail it over to another host, causing the same consequence in the reverse direction. This phenomenon continues until the group comes online on the final node. You can avoid this situation by setting up your infrastructure such that loss of heartbeat links also mean the loss of replication links.

Configuring the agent for IBM DS4K RemoteMirror

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

- Converting their devices to DS4KRemoteMirror devices

- Synchronizing the devices

- Adding the IBM DS4K RemoteMirror agent to the service group

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

Note: You must not change the replication state of devices from primary to secondary and from secondary to primary, outside of a VCS setup. The agent for IBM DS4K RemoteMirror 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 (DS4KRemoteMirror) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types**, and select:

   /etc/VRTSvcs/conf/DS4KRemoteMirrorTypes.cf

3 Click **Import**.

4 Save the configuration.

5 Add a resource of type DS4KRemoteMirror at the bottom of the service group.

6 Configure the attributes of the DS4KRemoteMirror 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 (DS4KRemoteMirror) is not added to your configuration, add it. From the Cluster Explorer **File** menu, choose **Import Types** and select:

   /etc/VRTSvcs/conf/DS4KRemoteMirrorTypes.cf

3. Click **Import**.

4. Save the configuration.

5. In each service group that uses replicated data, add a resource of type DS4KRemoteMirror at the bottom of the service group.

6. Configure the attributes of the DS4KRemoteMirror resource.

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 DS4K RemoteMirror

This chapter includes the following topics:

- Typical test setup for the IBM DS4K RemoteMirror agent

- Testing service group migration

- Testing host failure

- Performing a disaster test

- Performing the failback test

Typical test setup for the IBM DS4K RemoteMirror agent

A typical test environment includes the following characteristics:

- Two hosts (hosta and hostb) are attached to the primary IBM DS4000/5000 array.

- Two hosts (hostc and hostd) are attached to the secondary IBM DS4000/5000 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
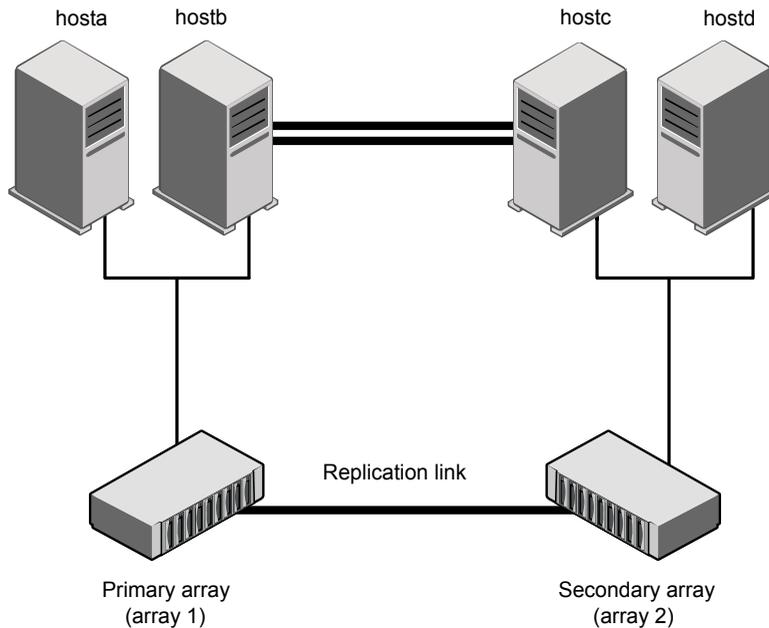
Testing service group migration

Verify 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.

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 primary 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 primary state from the secondary 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 logical drives are in primary role.

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.

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 DS4000/5000 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 secondary 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 primary state.

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: Automatically resynchronize the volumes using the failback action. After the resynchronization completes, the state of the original target volumes changes to primary. The state of the original source volumes changes to secondary.

4   Migrate the application back to the original primary site.

Index