Veritas™ Cluster Server Agent for IBM MetroMirror Configuration Guide

ESX

5.1 MP2

July 2008

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.MP2

Document Version: 5.1.MP2.0

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

1

Introducing the VCS agent for IBM MetroMirror

This chapter includes the following topics:

About the agent for IBM MetroMirror

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

What's new in this release

The Veritas Cluster Server agent for IBM MetroMirror includes the following new or enhanced features:

- The Veritas agent for IBM MetroMirror supports replicated data clusters in this release.

Supported software and hardware

The IBM MetroMirror agent supports Veritas Cluster Server 5.1 MP2 for ESX.

The agent supports all versions of IBM DSCLI.

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

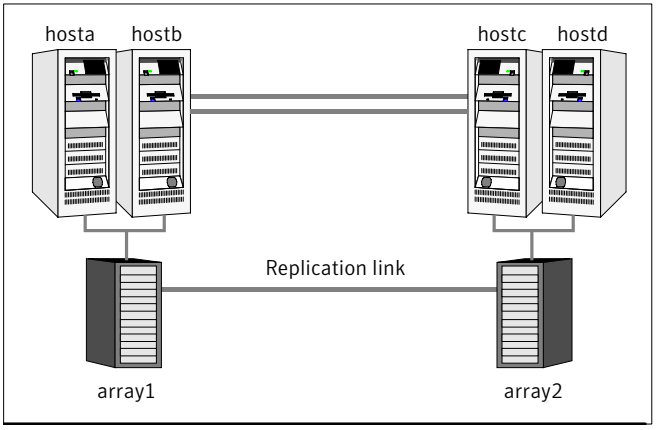
This support only exists if the host, the HBA, and the array combination is in IBM's hardware compatibility list.

Note: VMotion (i.e. the live migration of the virtual machine from the source ESX host to the target) is not supported across replicated system zones.

Typical IBM MetroMirror 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 17.
- 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, 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 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.
failbackpprc action	Performs a `failbackpprc` from the original secondary side to merge any changed tracks from the original secondary to the original primary.
MMStatus action	Retrieves the mapping and the state of the MetroMirror agent. This is a purely informational action entry point with no operational impact.

Additional considerations in an ESX environment

The agent performs the following actions before coming online:

- Changes the following ESX server settings:
  LVM.DisallowSnapshotLun=0.
  LVM.EnableResignature=0.
  Refer to the VMware documentation for more information on these settings.
- Rescans all Host Bus Adapters (HBA).

Chapter 2

Configuring the agent for IBM MetroMirror

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 = {MMStatus, 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 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: /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. 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

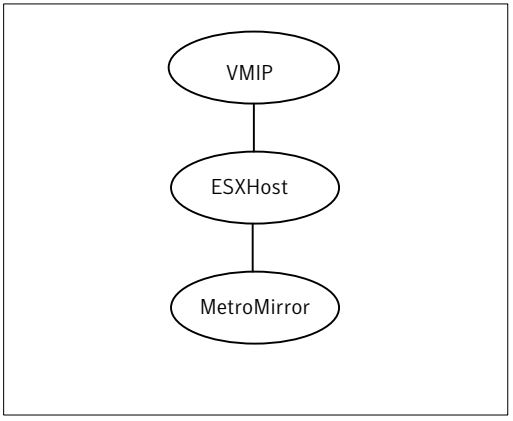
These attributes are for internal use only. Do not modify their values.

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 MetroMirror agent

Figure 2-1 shows the dependency graph for a VCS service group with a resource of type MetroMirror.

Figure 2-1 Sample configuration for the MetroMirror agent



The DiskGroup resource depends on the MetroMirror resource.

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

```
MetroMirror vmhost1 (
        DSCliHome = "/opt/ibm/dscli"
        HMC1 = "ds8000c.example.com"
        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:
  ~/dscli/security.dat

Before you configure the agent for MetroMirror

Before you configure the agent, review the following information:

- Verify that the clustering infrastructure is in place.
  If you plan to configure the agent in a global cluster, make sure the global service group for the application is configured.
  For more information, see the *Veritas Cluster Server User's Guide*.
- Review the configuration concepts, which describe the agent's type definition and attributes.
  See "Configuration concepts for the MetroMirror agent" on page 13.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical IBM MetroMirror setup in a VCS cluster" on page 10.
- Make sure that MetroMirror paths are configured in both directions between the source and the target LSS. MetroMirror 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 17.

- Set up system zones in replicated data clusters.
  See "About configuring system zones in replicated data clusters" on page 17.
- Generate the DSCLI password file. Use the `managepwfile` DSCLI command to do so.

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

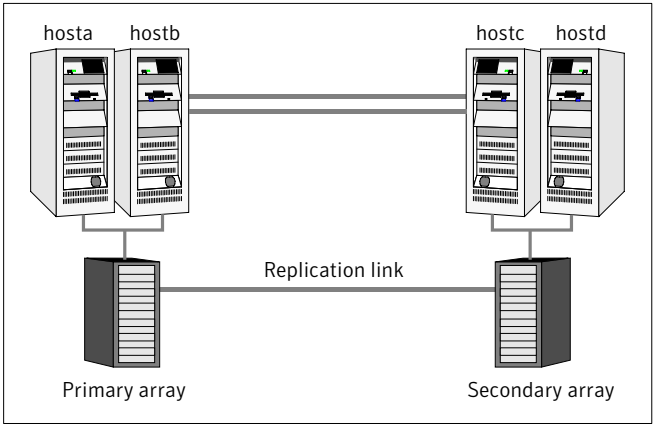
In a replicated data cluster, you can prevent unnecessary MetroMirror failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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

Figure 2-2 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 2-2 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 MetroMirror agent to the service group

Configure IBM DS8000 volumes as resources of type MetroMirror.

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

See "Sample configuration for the MetroMirror agent" on page 15.

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. 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.
9. Repeat step 5 through step 8 for each service group in each cluster that uses replicated data.

Configuring the agent manually in a replicated data cluster

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

To configure the agent in a replicated data cluster

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

   /etc/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 top 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.

3

Managing and testing clustering support for IBM MetroMirror

This chapter includes the following topics:

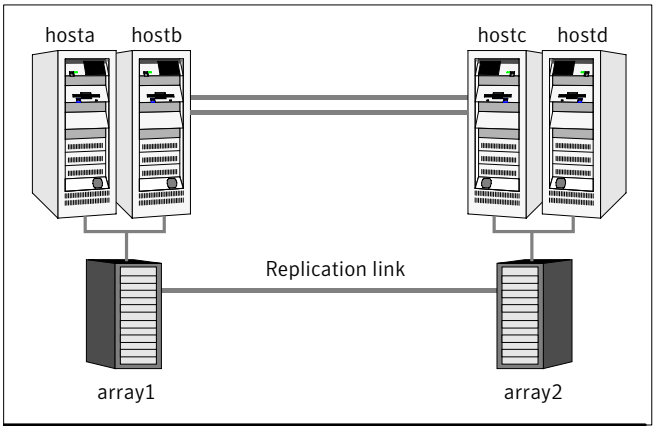
Typical test setup for the IBM MetroMirror agent

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.
- A replicated data cluster has two dedicated heartbeat links.
  A global cluster has one network heartbeat.

Figure 3-1 depicts a typical test environment.

Figure 3-1 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.

   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 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.

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).

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.

2. 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.

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. 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.

Rescanning Host Bus Adapters (HBAs) on VCS nodes

While executing rescan HBA operations on VCS nodes, use the following guidelines to make sure that the LVM settings conform to VCS requirements:

- Note the current values of the following LVM settings:
  DisallowSnapshotLun
  EnableResignature
- While rescanning snapshot LUNs for new datastores, set EnableResignature=1.
- If rescanning with DisallowSnapshotLun=0 and EnableResignature=0, make sure that snapshot LUNs that do not contain already resignatured datastores are not presented to the server.