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

Windows Server 2003, Windows Server 2008

5.1

April 2008

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

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder.

Windows is a registered trademark of Microsoft Corporation.

Technical support

For technical assistance, visit

http://www.symantec.com/business/support/index.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 1 Introducing the Veritas agent for IBM Metro Mirror 7

About the agent for IBM Metro Mirror 7
Supported software and hardware 7
Typical IBM Metro Mirror setup in a VCS cluster 8
IBM Metro Mirror agent operations 9

Chapter 2 Installing and removing the agent for IBM Metro Mirror 11

Before you install the agent for MetroMirror 11
Installing the agent for MetroMirror 11
Removing the agent for MetroMirror 12

Chapter 3 Configuring the agent for IBM Metro Mirror 15

Configuration concepts for the Metro Mirror agent 15
Resource type definition for the Metro Mirror agent 15
Attribute definitions for the Metro Mirror agent 16
Sample configuration for the Metro Mirror agent 17
Before you configure the agent for MetroMirror 18
About cluster heartbeats 19
About configuring system zones in replicated data clusters 19
Configuring the agent for MetroMirror 20
Configuring the agent manually in a global cluster 20
Configuring the agent manually in a replicated data cluster 21

Chapter 4 Managing and testing clustering support for IBM Metro Mirror 23

Typical test setup for the IBM Metro Mirror agent 23
Testing service group migration 24
Testing host failure 25
Performing a disaster test 25
Performing the failback test 26

Index 27

Chapter 1

Introducing the Veritas agent for IBM Metro Mirror

This chapter includes the following topics:

- About the agent for IBM Metro Mirror
- Supported software and hardware
- Typical IBM Metro Mirror setup in a VCS cluster
- IBM Metro Mirror agent operations

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

Supported software and hardware

The IBM MetroMirror agent supports SFW HA 5.1.

The agent supports all versions of IBM DSCLI.

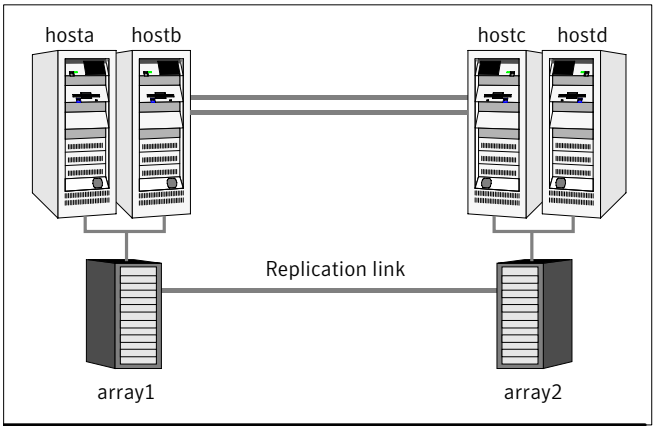
The agent supports MetroMirror on all microcode levels on all IBM DS8000 arrays.

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

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 19.

- 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, all hosts that are attached to the same array must be part of the same GAB membership.

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.

Chapter 2

Installing and removing the agent for IBM Metro Mirror

This chapter includes the following topics:

- Before you install the agent for MetroMirror
- Installing the agent for MetroMirror
- Removing the agent for MetroMirror

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 8.

Installing the agent for MetroMirror

If you did not install the MetroMirror when you installed Veritas Storage Foundation for Windows High Availability (SFW HA), follow these instructions to install the agent.

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 SFWHA.

To install the agent for MetroMirror

1. Open the Windows Control Panel and click **Add or Remove Programs.**
2. Click the SFW HA Server Components entry and click **Change.**

3 On the installer screen, click **Add or Remove** and click **Next.**

4 In the Option Selection dialog box, select the agent and click **Next.**

5 The installer validates the system for installation.

If a system is rejected, the Comments column displays the cause of rejection. Highlight the system to view detailed information about the failure in the Details box. Resolve the error, highlight the node in the selected systems list, and click **Validate Again.**

After all the systems are accepted, click **Next.**

6 An informational message appears if you selected the DMP option. Review the information and click **OK** to continue.

7 Review the summary of your selections and click **Next.**

8 Click **Update** to start the installation.

9 The installer displays the status of installation. After the installation is complete, review the installation report and click **Next.**

10 Click **Finish.**

Removing the agent for MetroMirror

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 MetroMirror

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

2 Click the VSFW HA Server Components entry and click **Remove.**

3 Review the Welcome page and click **Next.**

4 In the Option Selection dialog box, select the MetroMirror agent and click **Next.**

5 The installer validates the system for uninstallation.

If a system is rejected, the Comments column displays the cause of rejection. Highlight the system to view detailed information about the failure in the Details box. Resolve the error, highlight the node in the selected systems list, and click **Validate Again.**

After all the systems are accepted, click **Next.**

6 Review the summary of your selections and click **Uninstall.**

7 The installer displays the status of uninstallation.

8 After the uninstallation is complete, review the report and click **Next.**

9 Click **Finish.**

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

Chapter 3

Configuring the agent for IBM Metro Mirror

This chapter includes the following topics:

- Configuration concepts for the Metro Mirror agent
- Before you configure the agent for MetroMirror
- Configuring the agent for MetroMirror

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 = "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 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: 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

Internal attributes

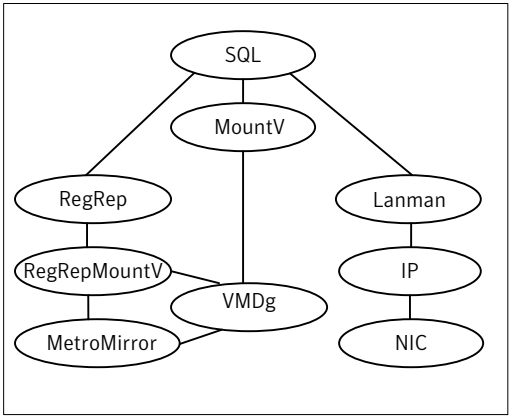
These attributes are for internal use only. Do not modify their values.

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 MetroMirror agent



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 = "C:\Program Files\ibm\dscli"
    HMC1 = "ds8000c.example.com"
    User = admin
    PasswdFile = "C:\Program Files\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:
  C:\Program Files\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 15.
- 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 8.
- 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 19.
- Set up system zones in replicated data clusters.
  See "About configuring system zones in replicated data clusters" on page 19.

- 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

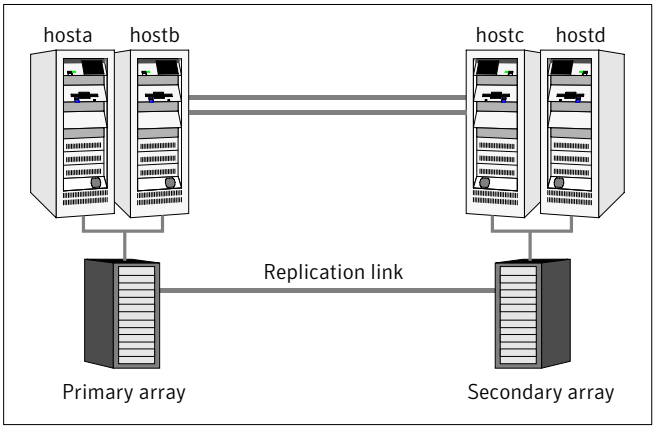
In a replicated data cluster, you can prevent unnecessary MetroMirror failover or failback by creating system zones. VCS attempts to fail over applications within the same system zone before failing them over across system zones.

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



Modify the SystemZones attribute using the following command:

```
C:\> 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 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.

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

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:

   Program Files\Veritas\Cluster Server\conf\config\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:

   ```
   Program Files\Veritas\Cluster
   Server\conf\config\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
- Testing service group migration
- Testing host failure
- Performing a disaster test
- Performing the failback test

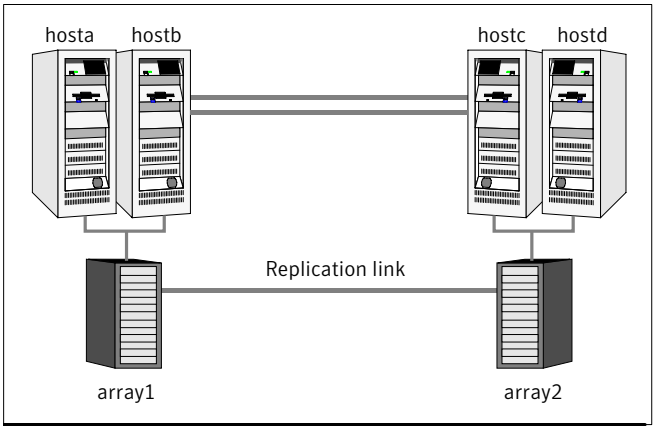
Typical test setup for the IBM Metro Mirror agent

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.
- 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. The test scenario is similar in both cases.

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.

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.

Index

A
action entry point 9
attribute definitions 16

C
clean entry point 9
cluster
    heartbeats 19

D
disaster test 25
DSCliHome attribute 16

E
entry points
    action 9
    clean 9
    monitor 9
    offline 9
    online 9
    open 9

F
failback test 26

H
HMC1 attribute 16
HMC2 attribute 17

I
IBM Metro Mirror agent
    attribute definitions 16
IBM Metro Mirror agent attributes
    DSCliHome 16
    HMC1 16
    HMC2 17
    LocalStorageImageID 16
    PasswdFile 16
    RemoteStorageImageID 16
IBM Metro Mirror agent attributes *(continued)*
    User 16
    VCSResLock 17
    VolIds 16
installing the agent
    Windows systems 11

L
LocalStorageImageID attribute 16

M
migrating service group 24
monitor entry point 9

O
offline entry point 9
online entry point 9
open entry point 9

P
PasswdFile attribute 16

R
RemoteStorageImageID attribute 16

S
sample configuration 17
service group
    migrating 24

T
testing
    disaster 25
    failback 26

U
uninstalling the agent
    Windows systems 12

User attribute 16

V

VCSResLock attribute 17
VolIds attribute 16