Veritas™ Cluster Server One Agent for EMC SRDF Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris, ESX, Windows Server 2003/2008

5.0 Service Pack 1

March 2010

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: 5.0SP1.0

Document version: 5.0SP1.0.0

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 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/business/support/index.jsp

Contacting Technical Support

Customers with a current maintenance 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 non-technical support Web page at the following URL:

customercare.symantec.com

Customer service

Customer Care information is available at the following URL:

www.symantec.com/customercare

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

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

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	customercare_apac@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.

Contents

Chapter 1

Introducing the Veritas Cluster Server One Agent for EMC SRDF

This chapter includes the following topics:

About the agent for EMC SRDF

The Veritas agent for EMC SRDF provides support for application failover and recovery. The agent provides this support in environments that use SRDF to replicate data between EMC Symmetrix arrays.

The agent monitors and manages the state of replicated EMC Symmetrix devices that are attached to VCS One client systems. The agent ensures that the system that has the SRDF resource online also has safe and exclusive access to the configured devices.

You can use the agent in global clusters that run VCS One.

The agent supports SRDF device groups and consistency groups in sync and async modes. The agent also supports dynamic SRDF (role swap).

Note: The agent does not support semi-synchronous and Adaptive Copy.

What's new in this release

The VCSOne agent for EMC SRDF includes the following new or enhanced features:

- The agent for SRDF is supported on ESX 3.5/4.0/4i.
- The agent for SRDFprovides support for Windows Server 2003 and 2008.

Supported software for EMC SRDF

The agent for EMC SRDF supports the following software versions:

Veritas Cluster Server One	■ VCS One 5.0 SP1on AIX ■ VCS One 5.0 SP1 on HP-UX 11i v2 ■ VCS One 5.0 SP1 on Red Hat Enterprise Linux ■ VCS One 5.0 SP1on SUSE Linux Enterprise Server ■ VCS One 5.0 SP1 on Solaris SPARC ■ VCS One 5.0 SP1 on Solaris x64 (OPTERON) ■ VCS One 5.0 SP1 on ESX 3.5/4.0/4i ■ VCS One 5.0 SP1 on Windows Server 2003, 2008. See the product's Release Notes for more details on the supported architectures and the operating system versions.

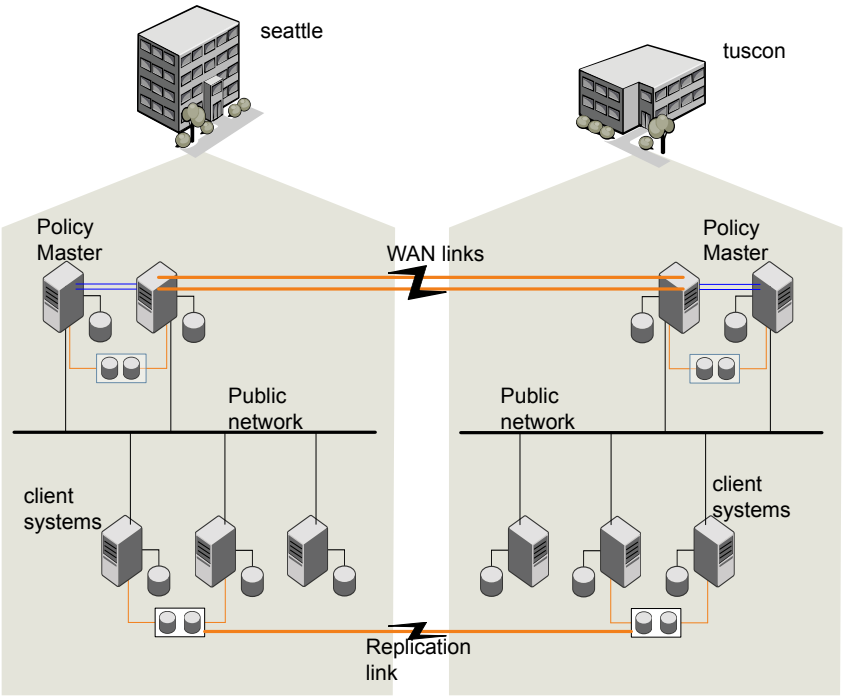
Supported hardware for EMC SRDF

The SRDF agent supports Solutions Enabler (SE) 6.4 or later and corresponding array microcode levels. Please refer to the EMC hardware compatibility list for specific information.

Typical EMC SRDF setup in a VCS One cluster

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

Figure 1-1 Typical clustering setup for the agent



VCS One clusters using SRDF for replication uses the following hardware infrastructure:

- The primary array has one or more R1 devices. A Fibre Channel or SCSI directly attaches these devices to the EMC Symmetrix array that contains the SRDF R1 devices.
- The secondary array has one or more R2 devices. A Fibre Channel or SCSI directly attaches these devices to a EMC Symmetrix array that contains the SRDF R2 devices. The R2 devices are paired with the R1 devices in the R1 array. The R2 devices and arrays must be at a significant distance to survive a disaster that may occur at the R1 side.

EMC SRDF agent functions

The VCS One agent for SRDF monitors and manages the state of replicated Symmetrix devices that are attached to VCS One client systems.

The agent performs the following functions:

online	If the state of all local devices is read-write enabled (RW), the agent creates a lock file on the local host. The lock file indicates that the resource is online. If one or more devices are in the write-disabled (WD) state, the agent runs a `symrdf` command to enable read-write access to the devices. See "About the EMC SRDF agent's online function" on page 12.
offline	Removes the lock file on the local host. The agent does not run any SRDF 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	The lock file is not removed in all cases. If the devices are capable of dynamic swap, a "swapfile" is created. The presence or absence of this file is used to determine the commands that must be run during the online function. If an online lock file exists, but no parent (i.e. resource or service group) is online, then the lock file is deleted.
clean	Determines if it is safe to fault the resource if the online entry point fails or times out.
info	Reports the device state to the VCS One interface. This entry point can be used to verify the device state and to monitor dirty track trends.
action/update	Performs a `symrdf update` from the R2 side to merge any dirty tracks from the R2 to the R1.

About the EMC SRDF agent's online function

If the state of all local devices is read-write enabled (RW), the agent creates a lock file on the local host to indicate that the resource is online.

If one or more devices are in the write-disabled (WD) state, the agent runs a `symrdf` command to enable read-write access to the devices.

Depending on SRDF/S and SRDF/A, the states can be different as follows:

- For R2 devices in the SYNCHRONIZED or CONSISTENT state, the agent runs the `symrdf failover` command to make the devices writable.

- For R1 devices in the FAILED OVER or R1 UPDATED state, the agent runs the `symrdf failback` command to make the devices writable.
- For all devices in the PARTITIONED state, the agent runs the `symrdf` command to make the devices writable.
  The agent runs the command only if the AutoTakeover attribute is set to 1 and if there are no dirty tracks on the local device. Dirty tracks indicate that an out-of-order synchronization was in progress when the devices became partitioned, rendering them inconsistent and unusable. If dirty tracks exist, the online entry point faults on timeout.
- For R1 devices in the UPDINPROG state, the agent runs a `symrdf` command only after the devices transition to the R1 UPDATED state.
- For R2 devices in the SYNCINPROG state, the agent runs a `symrdf` command only after the devices transition to the SYNCHRONIZED or CONSISTENT state.

The agent does not run any command if there is not enough time remaining for the entry point to complete the command.

See "Setting the OnlineTimeout attribute for the SRDF resource" on page 26.

About dynamic swap support for the EMC SRDF agent

The agent supports the SRDF/S and SRDF/A dynamic swap capability. The agent performs a role swap for the healthy arrays that are configured for dynamic swap when a service group fails over between the arrays. If one array is down, a unilateral read-write enable occurs. The agent fails over the device groups that are not configured for dynamic swap using the following command: `symrdf failover`. The command enables read-write on the R2 device.

The agent checks the following criteria before determining if a swap occurs:

- All devices in the device group are configured as dynamic devices.
- Dynamic RDF is configured on the local Symmetrix array.
- The microcode is level 5567 or later.

The commands for online are different for SRDF/S dynamic swap and SRDF/A dynamic swap as follows:

- For SRDF/S, for R2 devices in the SYNCHRONIZED state, the agent runs the `symrdf failover -establish` command.
- For SRDF/A, for R2 devices in the CONSISTENT state, the agent runs the `symrdf -force failover` command. If consistency is enabled, the agent runs the `symrdf disable` command. The agent then issues the `symrdf swap`

command to do the role-swap and the `establish` command to re-establish the replication, and re-enables the consistency.

Dynamic swap does not affect the ability to perform fire drills.

Chapter 2

Installing and removing the agent for EMC SRDF

This chapter includes the following topics:

Installing the Veritas Cluster Server One agent for SRDF

You must install the agent for SRDF on all the client systems of the VCS One cluster that will host the SRDF service group. You can install the agent for SRDF using the installagpack program or using the command line interface (CLI).

The installation of the agent packs involves the following phases:

Installing the agent packages	See "Installing the agent packages using the installer" on page 16.
Adding the agent resource type definitions	See "Adding the agent resource type definitions" on page 17.

Note: The installagpack program supports only the -addtypes, -rmtypes, -responsefile, and -rsh options. Symantec recommends that you do not use any of the other options from the `installagpack` command help output.

Installing the agent packages using the installer

You can install the agent packages on one or more client systems of a specific platform type.

Perform the following steps to install the agent packages using the installer

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.
2. Depending on the platform type, navigate to the directory containing the agent installer:

AIX	`cd1/aix/vcsone/`*`vcsone_version`*
HP-UX	`cd1/hpux/hpux`*`os_version`*`/vcsone/`*`vcsone_version`* Where *os_version* is the HP-UX version.
Linux	`cd1/linux/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`cd1/solaris/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where, *dist_arch* is 'sol_sparc' or 'sol_x64'.

3. Enter the following command to start the agent pack installation:

   ```
   # ./installagpack [-rsh]
   ```

   You can use the `-rsh` option if rsh and rcp are used for communication between systems instead of the default ssh and scp. This option requires that systems be preconfigured such that the `rsh` commands between systems execute without prompting for passwords or confirmations.
4. Enter the name of the client systems where you want to install the agents.
5. Choose whether to install all the agents or any specific agent. Follow the installer prompt to specify your option.
6. Review the output as the installation program installs the agent packages.

   You can view installation logs in the /var/VRTS/install/logs directory.

Installing the agent package using the CLI

You can install the desired agent package using the CLI, on one or more client systems of a specific platform type.

Perform the following steps to install the agent packages using CLI

1 Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.

2 Depending on the platform type, navigate to the directory containing the agent installer:

AIX	# **cd1/aix/vcsone/vcsone_version/pkgs**
HP-UX	# **cd1/hpux/hpux*os_version*/vcsone/vcsone_version/depot**
Linux	# **cd1/linux/*dist_arch*/vcsone/vcsone_version/rpms** Where, *dist* is the Linux distribution and *arch* is the architecture
Solaris	# **cd1/solaris/*dist_arch*/vcsone/vcsone_version/pkgs** Where *dist_arch* is 'sol_sparc' or 'sol_x64'

3 Type the following command on each client system to install the agent. Answer the prompt accordingly:

AIX	# **installp -ac -d . VRTScse.rte**
HP-UX	# **swinstall -s `pwd` VRTScse**
Linux	# **rpm -ivh VRTScse_rpm_filename**
Solaris	# **pkgadd -d . VRTScse**

Adding the agent resource type definitions

You must add the agent resource type definitions to the Policy Master database configuration. You can perform this task from any client system in the VCS One cluster.

Note: You must add the agent resource type definitions only one time per platform type.

To add the agent resource types to the policy master database configuration

1. Set up RSH or SSH communications between the client system and the policy master system.

   For information on configuring SSH for remote communication, refer to the *Veritas Cluster Server One Installation Guide*.

2. Make sure that the PM daemon is running.

   ```
   # /opt/VRTSvcsone/bin/haclus -display
   ```

   The output should show ClusterState is RUNNING.

3. If you have just installed the agents on VCS One client systems and still have the VCS One Agent Pack software disc mounted, skip to step 6.

4. Mount the VCS One Agent Pack software disc.

5. Depending on the platform type, navigate to the directory containing the agent installer:

AIX	`cd1/aix/vcsone/`*`vcsone_version`*
HP-UX	`cd1/hpux/hpux`*`os_version`*`/vcsone/`*`vcsone_version`* Where *os_version* is the HP-UX version.
Linux	`cd1/linux/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	`cd1/solaris/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist_arch* is the sol_sparc or sol_x64.

6. Enter the command to start the agent pack installer for adding resource types to the Policy Master configuration database. Use the `-addtypes` option:

   ```
   # ./installagpack -addtypes
   ```

7. When the installer prompts, enter the virtual IP address of the Policy Master.

8. Review the output as the installer verifies communication with the Policy Master system.

9 Choose whether to add the type definitions for all the agents or for specific agents. Follow the installer prompts to add the type definitions.

10 Review the output as the installer adds the agent types to the PM database configuration and copies the appropriates types.xml files to the PM system.

You can view installation logs in the /var/VRTS/install/logs directory.

Removing the Veritas Cluster Server One agent for SRDF

Removing the agent package involves removing the agent files from each client system where it was installed.

You can remove the packages using the agent pack installer or the command line.

See "Removing the agent packages using the installer" on page 19.

See "Removing the agent package using CLI" on page 20.

After removing the agent packages you can remove the agent type definition from the Policy Master system.

See "Removing the agent type definition from the Policy Master system" on page 21.

Removing the agent packages using the installer

You can remove all the agent packages or the desired agent package using the uninstallagpack program.

Note: The uninstallagpack program supports only the -responsefile and -rsh options. Symantec recommends that you do not use any of the other options from the `uninstallagpack` command help output.

To remove the agent packages from the client systems

1 Freeze the service groups that hosts the application, on the system from which you want to remove the agent package.

```
# hagrp -freeze <groupname>
```

2 Stop the agent on all client systems before you remove the agent package from the system.

```
# haagent -stop -notransition <AgentName> -sys <system_name>
```

3 Ensure that the agent operations are stopped on all the cluster systems.

```
# haagent -display <AgentName>
```

4 Mount the VCS One Agent Pack software disc on the client system where you plan to run the uninstallagpack program.

5 Depending on the platform type, navigate to the directory containing the agent uninstaller:

AIX	**cd1/aix/vcsone/*vcsone_version***
HP-UX	**cd1/hpux/hpux*os_version*/vcsone/*vcsone_version***
	Where *os_version* is the HP-UX version.
Linux	**cd1/linux/*dist_arch*/vcsone/*vcsone_version***
	Where *dist* is the Linux distribution and *arch* is the architecture.
Solaris	**cd1/solaris/*dist_arch*/vcsone/*vcsone_version***
	Where *dist_arch* is the sol_sparc or sol_x64.

6 Start the uninstallagpack program.

```
# ./uninstallagpack [-rsh]
```

7 Enter the name of the client systems on which you want to uninstall the agent pack. The names must be separated by spaces.

8 Choose whether to remove all the agent packages or a specific agent package. Follow the installer prompt to remove the agent package.

9 Review the output as the program verifies the agent pack that you installed and removes the agent packages.

You can view logs in the /var/VRTS/install/logs directory.

Removing the agent package using CLI

You can remove a desired agent package using the CLI.

Note: You must remove this agent package from each client system in the cluster.

To remove the agent for SRDF from a client system

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

AIX	# **installp -u VRTScse**
HP-UX	# **swremove VRTScse**
Linux	# **rpm -e VRTScse**
Solaris	# **pkgrm VRTScse**

Removing the agent type definition from the Policy Master system

After you remove the agent packages, you can remove the agent type definitions for all the agents for specific agents from the Policy Master system.

To remove the agent type definition from the Policy Master system

1. Navigate to the following directory on the client system.

   # **cd /opt/VRTS/install**

2. Run the following command to remove the agent type definition from the Policy Master system:

   # **./installagpack -rmtypes**

3. When the installer prompts, enter the virtual IP address of the Policy Master.
4. Choose whether to remove the type definitions for all the agents or for specific agents. Follow the installer prompts to remove the type definitions.

   You can view logs in the /var/VRTS/install/logs directory.

Chapter 3

Configuring the agent for EMC SRDF

This chapter includes the following topics:

Configuration concepts for the EMC SRDF agent

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

Resource type definition for the EMC SRDF agent

The resource type represents the VCS One configuration of the agent and specifies how the agent is defined in the configuration file main.xml. For more information, refer to the sample SRDFTypes.platform.xml files in the `/etc/VRTSagents/ha/conf/SRDF` directory on the primary client system.

Attribute	Default value
SymHome	/usr/symcli
GrpName	<No default value>
DevFOTime	2
AutoTakeover	0
SplitTakeover	0

Attribute	Default value
Mode	<No default value>
IsCompositeGroup	0
SwapRoles	1

Attribute definitions for the SRDF agent

Review the description of the agent attributes.

Required attributes

You must assign values to required attributes.

GrpName
: Name of the Symmetrix device group or composite group that the agent manages. Specify the name of a device group or composite group.

  Note: If this is a composite group, ensure that you set the value of IsCompositeGroup to 1.

  Type-dimension: string-scalar

Optional attributes

Configuring these attributes is optional.

SwapRoles
: This attribute only applies to dynamic devices. Specifies whether the roles of the dynamic devices must be swapped at the time of failover or not. If set to 1, the RDF1 dynamic devices are made RDF2, and vice-versa. If set to 0, the roles remain the same.

  Type-dimension: integer-scaler

  Default: 1

IsCompositeGroup
: Specifies whether the SRDF group is a composite group or not. If set to 0, VCS One treats it as device group. If set to 1, VCS One treats it as composite group.

  Type-dimension: integer-scaler

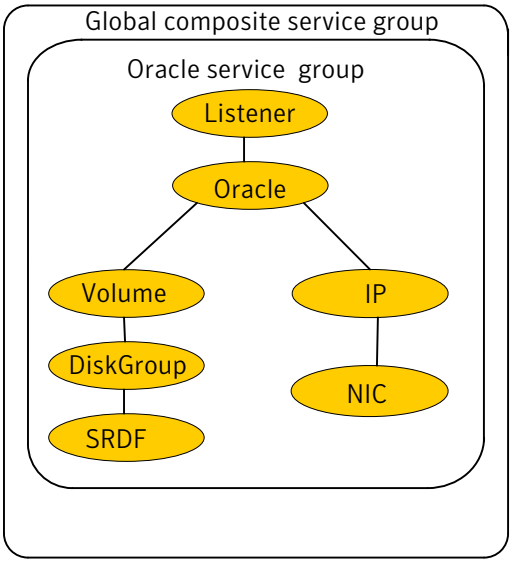
  Default: 0

SymHome	Path to the bin directory that contains the Symmetrix command line interface. Type-dimension: string-scalar Default is /usr/symcli. Default is C:\Program Files\EMC\SMYCLI\bin.
DevFOTime	Average time in seconds that is required for each device or composite group to fail over. This value helps the agent to determine whether it has adequate time for the online operation after waiting for other device or composite groups to fail over. If the online operation cannot be completed in the remaining time, the failover does not proceed. Type-dimension: integer-scalar Default is 2 seconds per device.
AutoTakeover	A flag that determines whether the agent performs a `symrdf rw_enable` operation on the partitioned devices at the secondary site. Type-dimension: integer-scalar Default is 0.
SplitTakeover	A flag that determines whether the agent permits a failover to R2 devices in the Split state. The value 0 indicates that the agent does not permit a failover to R2 devices in the Split state. The value 1 indicates that the agent permits a failover to R2 devices in the Split state if the devices are read-write enabled. The attribute has no effect on failing over to a host attached to R1 devices. Set the attribute to 0 to minimize the risk of data loss on a failover to devices that may not be in synch. Type-dimension: integer-scalar Default is 0.
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. If the value is not specified, the agent assumes that the mode is Synchronous. If the devices are setup to replicate in the Asynchronous mode, you must set Mode to Asynchronous.

Sample configuration for the SRDF agent

Figure 3-1 shows a dependency graph of a VCS One global composite service group that has a resource of type SRDF.

Figure 3-1 VCS One global composite service group with resource type SRDF



Setting the OnlineTimeout attribute for the SRDF resource

Set the OnlineTimeout attribute for the SRDF resource so that its entry points do not time out, or they automatically restart if they timed out.

To set the OnlineTimeout attribute

1 For each SRDF resource in the configuration, use the following formula to calculate an appropriate value for the OnlineTimeout attribute:

$$\text{OnlineTimeout} = \sum_{1}^{n_{devicegroups}} ((n_{devices} \times d_{failovertime}) + \varepsilon)$$

- $n_{devices}$ represents the number of devices in a device group.
- $d_{failovertime}$ represents the time taken to failover a device.

- $n_{devicegroups}$ represents the total number of device groups that might fail over simultaneously.
- The epsilon is for the command instantiation overhead. You can set it to any value based on your setup

To set the Online Timeout attribute for a single device group (typically the case for SRDF), multiply the number of devices in the device group with the time taken to failover a device (default = 2 seconds) and add it to the value of epsilon.

For example: if you have a single device group that consists of 5 devices and the time taken to failover a single device is 50 seconds, set the OnlineTimeout attribute to [(5*50)+ 10] seconds. The value of the epsilon here is equal to 10 seconds. Thus, the OnlineTimeout attribute is equal to 260 seconds.

To set the Online Timeout attribute for multiple device groups (currently not supported by SRDF), calculate the OnlineTimeout attribute for all device groups and set the OnlineTimeout attribute to at least the amount of time the largest device group takes to fail over.

2 If the resulting value seems excessive, divide it by two for every increment in the value of the RestartLimit attribute.

Before you configure the agent for EMC SRDF

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 EMC SRDF agent" on page 23.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical EMC SRDF setup in a VCS One cluster" on page 10.
- Verify that the clustering infrastructure is in place.
  - If you plan to configure the agent in a global cluster, make sure the global composite service group for the application is configured.
    For more information, see the *Veritas Cluster Server One User's Guide*.

Configuring the agent for EMC SRDF

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

- Converting their devices to SRDF devices

- Synchronizing the devices
- Adding the EMC SRDF agent to the service group

Note: You must not change the replication state of a cluster from primary to secondary and viceversa, outside of a VCS One setup. The agent for EMC SRDF fails to detect a change in the replication state if the role reversal is done externally.

Chapter 4

Managing and testing clustering support for EMC SRDF

This chapter includes the following topics:

Failure scenarios in global clusters

Table 4-1 lists the failure scenarios in a global cluster configuration and describes the behavior of VCS One and the agent in response to the failure.

See the *Veritas Cluster Server One User's Guide* for more information on the DR configurations and the global composite service group attributes.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for EMC SRDF

Failure	Description and VCS One response

Application failure	Application cannot start successfully on any client system at the primary site.
	VCS One response at the secondary site:
	■ Causes global composite service group at the primary site to fault and triggers a BPA event.
	■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site.
	Agent response:
	■ Write enables the devices at the secondary site.
	■ For dynamic RDF devices, the agent does the following if the value of the SwapRoles attribute of the SRDF resource is 1:
	  ■ Swaps the R1/R2 personality of each device in the device group or the consistency group.
	  ■ Restarts replication from R1 devices on the secondary site to the R2 devices at the primary site.
	See "Performing failback after a client system failure or an application failure" on page 35.

Client system failure	All client systems at the primary site fail.
	VCS One response at the secondary site:
	■ Triggers a BPA event.
	■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site.
	Agent response:
	■ Write enables the devices at the secondary site.
	■ For dynamic RDF devices, the agent does the following if the value of the SwapRoles attribute of the SRDF resource is 1:
	  ■ Swaps the R1/R2 personality of each device in the device group or the consistency group.
	  ■ Restarts replication from R1 devices on the secondary site to the R2 devices at the primary site.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for EMC SRDF *(continued)*

Failure	Description and VCS One response
Site failure	All PMs, client systems, and their storage at the primary site fail. A site failure renders the devices on the array at the secondary site in the PARTITIONED state. VCS One response at the secondary site: ■ Triggers a BPA event. ■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site. Agent response: The agent does the following on the secondary site in case of a manual failover based on the value of the AutoTakeover attribute of the SRDF resource: ■ 1—If invalid tracks do not exist, the agent issues the `symrdf failover` command to make the SRDF devices write-enabled. ■ 0—The agent faults the SRDF resource. See "Performing failback after a site failure" on page 36.
Replication link failure	Replication link between the arrays at the two sites fails. A replication link failure renders the SRDF devices in the PARTITIONED state. When the link is restored, the SRDF devices attain the SUSPENDED state. VCS One response: No action. Agent response: No action. The VCS agent for EMC SRDF does not monitor the replication link status and cannot detect link failures. After the link is restored, you must resynchronize the SRDF devices. To resynchronize the SRDF devices after the link is restored: ■ Before you resync the R2 device, you must split off the BCV device from the R2 device at the secondary site. ■ You must initiate resync of R2 device using the `symrdf resume` command. ■ After R1 and R2 devices are in sync, reestablish the mirror relationship between the BCV and R2 devices. If you initiate a failover to the secondary site when resync is in progress, the online function of the EMC SRDF agent waits for the resync to complete and then initiates a takeover of the R2 devices. **Note:** If you did not configure BCV devices and if disaster occurs when resync is in progress, then the data at the secondary site becomes inconsistent. Symantec recommends configuring BCV devices at both the sites. See "Typical EMC SRDF setup in a VCS One cluster" on page 10.

Table 4-1 Failure scenarios in a global cluster configuration with VCS One agent for EMC SRDF *(continued)*

Failure	Description and VCS One response
Network failure	The network connectivity and the replication link between the sites fail. VCS One response: ■ VCS One at each site concludes that the remote cluster has faulted. ■ The global cluster failover in VCS One is manual. No action. ■ You must confirm the cause of network failure from the cluster administrator at each site and fix the issue. To resynchronize the data after the network link is restored: ■ Take the global composite service group offline at both the sites. ■ Manually resync the data. Depending on the site whose data you want to retain use the `symrdf establish` or the `symrdf restore` commands. ■ Bring the global composite service group online on on one of the sites. Agent response: Similar to the site failure
Storage failure	The array at the primary site fails. A storage failure at the primary site renders the devices on the array at the secondary site in the PARTITIONED state. VCS One response at the secondary site: ■ Causes the global composite service group at the primary site to fault and triggers a BPA event. ■ The global cluster failover in VCS One is manual. You must bring the global composite service group online at the secondary site. Agent response: The agent does the following on the secondary site in case of a manual failover based on the value of the AutoTakeover attribute of the SRDF resource: ■ 1—If invalid tracks do not exist, the agent issues the `symrdf failover` command to make the SRDF devices write-enabled. ■ 0—The agent faults the SRDF resource.

Testing the global composite service group migration

After you configure the VCS One agent for EMC SRDF, verify that the global composite service group can migrate to hosts across the sites. Depending on your DR configuration, perform one of the following procedures.

To test the global composite service group migration in global cluster setup

1 Fail over the global composite service group from the primary site to the secondary site.

Perform the following steps:

- Switch the global composite service group from the primary site to the secondary site.

  ```
  hacsg -switch <global_csg> -clus <secondary_clusname>
  ```

  VCS One brings the global composite service group online at the secondary site.

- Verify that the SRDF devices at the secondary site are write-enabled, and the device state is as follows:

For static RDF	FAILED OVER state
For dynamic RDF	The value of the SRDF resource attribute SwapRoles determines the device state: ■ 0—FAILED OVER state ■ 1—SYNCHRONIZED or CONSISTENT state

2 Fail back the global composite service group from the secondary site to the primary site.

  Perform the following steps:

  - Switch the global composite service group from the secondary site to the primary site.

    ```
    hacsg -switch <global_csg> -clus <primary_clusname>
    ```

    VCS One brings the global composite service group online at the primary site.

  - Verify that the SRDF devices at the primary site are write-enabled and the device state is SYNCHRONIZED or CONSISTENT.

Testing disaster recovery after site failure

Review the details on site failure and how VCS One and the agent for EMC SRDF behave in response to the failure.

See "Failure scenarios in global clusters" on page 29.

Depending on the DR configuration, perform one of the following procedures to test the disaster recovery in the event of site failure.

To test disaster recovery for site failure in global cluster setup

1 Halt all client systems and the arrays at the primary site.

If you cannot halt the array at the primary site, then disable the replication link between the two arrays.

You must bring the global composite service group online at the secondary site. Run the following command:

```
hacsg -online -force global_csg
```

2 Verify that the SRDF devices at the secondary site are write-enabled and are in PARTITIONED state.

3 Verify that the global composite service group is online at the secondary site.

```
hacsg -state global_csg
```

Testing disaster recovery after client system failure

Review the details on client system failure and how VCS One and the agent for EMC SRDF behave in response to the failure.

See "Failure scenarios in global clusters" on page 29.

Depending on the DR configuration, perform one of the following procedures to test how VCS One recovers after all client systems at the primary site fail.

To test disaster recovery for client system failure in global cluster setup

1 Halt the client system at the primary site.

You must bring the global composite service group online at the secondary site. Run the following command:

```
hacsg -online -force global_csg
```

2 Verify that the SRDF devices at the secondary site are write-enabled, and the device state is as follows:

For static RDF FAILED OVER state

For dynamic RDF — The value of the SRDF resource attribute SwapRoles determines the device state:

- 0—FAILED OVER state
- 1—SYNCHRONIZED or CONSISTENT state

3 Verify that the global composite service group is online at the secondary site.

```
hacsg -state global_csg
```

Performing failback after a client system failure or an application failure

Review the details on client system failure and application failure and how VCS One and the agent for EMC SRDF behave in response to these failures.

See "Failure scenarios in global clusters" on page 29.

After the client systems at the primary site are restarted, you can perform a failback of the global composite service group to the primary site. Depending on your DR configuration, perform one of the following procedures.

To perform failback after a client system failure or an application failure in global cluster

1 Switch the global composite service group from the secondary site to the primary site.

```
hacsg -switch <global_csg> -clus <remote_clusname>
```

VCS One brings the global composite service group online at the primary site.

The VCS agent for EMC SRDF does the following based on whether the RDF pairs are static or dynamic:

For dynamic RDF — Based on the value of the SwapRoles attribute of the SRDF resource:

- 1—Write enables the devices at the primary site, swaps the R1/R2 personality of each device in the device group or the consistency group, and restarts replication from R1 devices on the primary site to the R2 devices at the secondary site.
- 0—Issues the `symrdf failback` command to resync the R1 devices and to write enable the R1 devices at the primary site.

For static RDF	Issues the `symrdf failback` command to resync the R1 devices and to write enable the R1 devices at the primary site.

2 Verify that the SRDF devices at the primary site are write-enabled and the device state is SYNCHRONIZED or CONSISTENT.

Performing failback after a site failure

After a site failure at the primary site, the hosts and the storage at the primary site are down. VCS One brings the global composite service group online at the secondary site and the EMC SRDF agent write enables the R2 devices.

The device state is PARTITIONED.

Review the details on site failure and how VCS One and the agent for EMC SRDF behave in response to the failure.

See "Failure scenarios in global clusters" on page 29.

When the hosts and the storage at the primary site are restarted and the replication link is restored, the SRDF devices attain SPLIT state at both the sites. The devices are write-enabled at both sites. You can now perform a failback of the global composite service group to the primary site.

To perform failback after a site failure in global cluster

1 Take the global composite service group offline at the secondary site. At the secondary site, run the following command:

```
hacsg -offline global_csg
```

2 Resync the devices using the `symrdf restore` command.

The `symrdf restore` command write disables the devices at both the R1 and R2 sites.

After the resync is complete, the device state is CONSISTENT or SYNCHRONIZED at both the sites. The devices are write-enabled at the primary site and write-disabled at the secondary site.

3 Bring the global composite service group online at the primary site. Run the following command:

```
hacsg -online global_csg
```

This again swaps the role of R1 and R2.

Index