Veritas™ Cluster Server Agent for Oracle Data Guard Installation and Configuration Guide

AIX, HP-UX, Linux, Solaris

5.0

June 2008

symantec™

Veritas Cluster Server Agent for Oracle Data Guard Installation and Configuration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Agent version: 5.0.03.0

Document version: 5.0.03.0.0

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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/techsupp/

Contacting Technical Support

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

http://www.symantec.com/business/support/assistance_care.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/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.

Contents

Chapter 1

Introducing the Veritas agent for Oracle Data Guard

This chapter includes the following topics:

About the agent for Oracle Data Guard

The Veritas agent for Oracle Data Guard provides failover support and recovery in an environment that uses the Oracle Data Guard. Oracle Data Guard replicates data between Oracle databases.

The agent monitors and manages the state of replicated Oracle 10g database that runs on VCS nodes. The Data Guard resource is online on the system with the primary database server. The agent makes sure that Oracle Data Guard replicates the database information from the primary database server to the standby database server.

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

The Veritas agent for Oracle Data Guard Broker manages the replication in Oracle 10g R2 databases in parallel applications such as Veritas Storage Foundation for Oracle RAC. This agent uses the Oracle Data Guard Broker to manage the database replication in a parallel application environment. The Data Guard Broker agent

simplifies the RAC database switch over or fail over using the Data Guard command-line interface DGMGRL.

You can use the Data Guard Broker agent in global clusters that run SF Oracle RAC.

Note: The Data Guard agent and the Data Guard Broker agent do not support replicated data clusters.

See the following Technical Support TechNote for the latest updates or software issues for this agent:

http://seer.entsupport.symantec.com/docs/282004.htm

What's new in this release

The Veritas agent for Oracle Data Guard includes the following new or enhanced features:

- The Veritas agent for Oracle Data Guard Broker that is packaged with the Data Guard agent supports Veritas Storage Foundation for Oracle RAC in this release.

Supported software and hardware

The agent for Oracle Data Guard supports the following software versions:

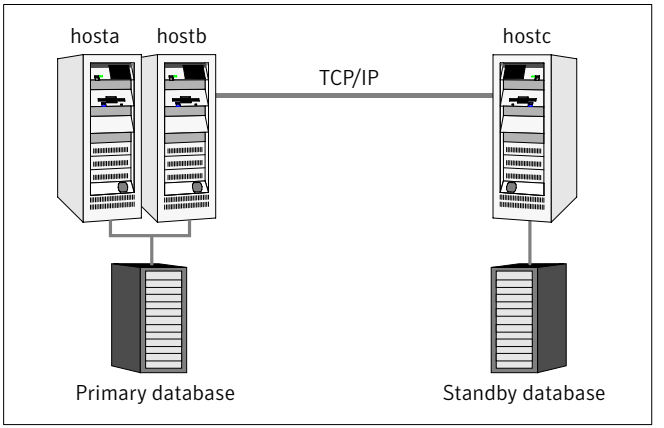
Veritas Cluster Server	■ VCS 5.0 and 5.0 MP1 on AIX ■ VCS 5.0 and 5.0 MP1 on HP-UX 11i v2 ■ VCS 5.0 and 5.0 MP1 on Red Hat Enterprise Linux ■ VCS 5.0 and 5.0 MP1 on SUSE Linux Enterprise Server ■ VCS 5.0 and 5.0 MP1 on Solaris SPARC See *Veritas Cluster Server Release Notes* for more details on the supported architectures and the operating system versions.

Veritas SF for Oracle RAC	SF Oracle RAC 5.0 MP1 on the following operating systems: ■ AIX ■ HP-UX 11i v2 ■ Red Hat Enterprise Linux ■ SUSE Linux Enterprise Server ■ Solaris SPARC ■ Solaris x64 See *Veritas Storage Foundation for Oracle RAC Release Notes* for more details on the supported architectures and the operating system versions.
Oracle	Oracle Data Guard agent supports the following Oracle versions: ■ Oracle 10g R1 ■ Oracle 10g R2 **Note:** The Data Guard agent supports only a single standby database instance per configured primary database. The Data Guard Broker agent supports Oracle 10g R2. You must use the Data Guard Broker agent in a parallel environment. For parallel application setup that uses Oracle RAC database, Oracle Data Guard Broker must be configured on the primary and the standby sites.

Typical Oracle Data Guard setup in a VCS cluster

Figure 1-1 displays a typical cluster setup in a Data Guard environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a Data Guard environment typically consists of the following hardware infrastructure:

- The primary database instance (db1) sends redo data across a TCP/IP link to a standby database instance (db2). A local cluster protects the primary database and makes it highly available.
- The standby database instance applies the redo information to a physical copy of the primary database.
- The primary and standby sites must be connected through a single TCP/IP network connection. This link can be shared with VCS global clusters for heartbeat communication.
- 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 31.

Agent functions for the Data Guard agent

The Oracle Data Guard agent monitors and manages the state of replicated Oracle database that runs on VCS nodes. Agent functions bring resources online, take them offline, and perform different monitoring actions. Agent functions are also known as entry points.

The agent also supports DataGuard role transition.

See "About DataGuard role transition" on page 15.

online	Creates a lock file on the local host to indicate that the resource is online. Depending on the role of the database, the agent performs actions to make the database accessible. See "About the Oracle DataGuard agent's online function" on page 14.
offline	Removes the lock file on the local node. Because a switch of the replication direction, promoting the standby and demoting the primary is executed on the target node. Oracle reconfiguration is not done as part of offline. In case of a complete shutdown, an Oracle resource is responsible to close the database.
monitor	Verifies that the lock file exists. ■ If the lock file does not exist, the monitor entry point reports the status of the resource as offline. ■ If the lock file exists, the agent checks if the role of the database is still PRIMARY and the open mode is WRITE.
open	Creates a lock file in the local agent directory if the role of the database is PRIMARY and the open mode is WRITE.
clean	Removes the lock file for the following resource states: ■ OFFLINE TIMEOUT ■ OFFLINE INEFFECTIVE ■ ONLINE TIMEOUT ■ UNEXPECTED OFFLINE ■ MONITOR HUNG
info	Reports the state and the role of the database.
start_stb_curlog.sql	Custom startup script for the VCS agent for Oracle. See "About the custom startup script for the Oracle agent" on page 14.
actions/DGStatus	Reports the current state and role of the database in real time.
actions/DGDemotePri	Demotes an active PRIMARY to STANDBY database. The agent calls this action as part of the online entry point from a STANDBY database server, when the database role is switched to PRIMARY. The active STANDBY database node drives a DataGuard database server role transition.

About the Oracle DataGuard agent's online function

The agent determines the role of the database and the type of open mode using the SQL commands:

```
DATABASE_ROLE from V$DATABASE
OPEN_MODE from V$DATABASE
```

If the role of the replicated database is PRIMARY and the open mode is MOUNT, the agent makes the database accessible for clients as follows:

- Alters the database to open mode READ WRITE.
- Creates a lock file on the local host to indicate that the resource is online.

If the role of the database is PHYSICAL STANDBY, the agent assumes a site fault and reconfigures the database as follows:

- The agent first tries to demote a primary database instance by executing the action `DGDemotePri` inside the remote cluster.
- Then, the agent changes the mode of the local database from PHYSICAL STANDBY to PRIMARY.
  The agent stops the reception of redo log information using the SQL command:

  ```
  ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL
  ```

  The agent changes the role of the database using the SQL command:

  ```
  ALTER DATABASE COMMIT TO SWITCHOVER TO PRIMARY
  ```

- The agent then restarts the local database instance to make the changes effective and creates a lock file in the local agent home directory.

About the custom startup script for the Oracle agent

The Oracle Data Guard agent uses a custom startup script start_stb_curlog.sql to start the Oracle agent. The Oracle database instance start has to be implemented by using a VCS resource of type Oracle with the attribute StartUpOpt set to CUSTOM. The necessary file start_custom_<InstID>.sql can then be implemented as a symbolic link to the start_stb_curlog.sql file.

Depending on the database role, the agent does the following actions:

- If the database role is PRIMARY, the agent mounts the database.
- If the database role is PHYSICAL STANDBY, the agent opens the database in mode READ ONLY. Then, the agent executes the following SQL command to start the replication reception:

```
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING
CURRENT LOGFILE DISCONNECT FROM SESSION
```

About DataGuard role transition

You can switch the service group in which the DataGuard resource resides using the `hagrp -switch` command.

If the agent is OFFLINE on the original primary, the agent removes the lock file.

If the agent is ONLINE on the former standby, the agent executes the following actions:

- Execute action DGDemotePri on the original primary.
- Alter database role from standby to primary.
- Restart Oracle instance on the standby.

Agent functions for the Data Guard Broker agent

The Oracle Data Guard Broker agent monitors and manages the state of replicated Oracle RAC database that runs on SF Oracle RAC nodes. Agent functions bring resources online, take them offline, and perform different monitoring actions. Agent functions are also known as entry points.

online	Creates a lock file on the local host to indicate that the resource is online. Depending on the role of the database, the agent performs actions to make the database accessible using the `dgmgrl switchover | failover` command.
offline	Removes the lock file on the local node. Because a switch of the replication direction, promoting the standby and demoting the primary is executed on the target node. Oracle reconfiguration is not done as part of offline. In case of a complete shutdown, an Oracle resource is responsible to close the database.

monitor	Verifies that the lock file exists. ■ If the lock file does not exist, the monitor entry point reports the status of the resource as offline. ■ If the lock file exists, the agent checks the role of the database using `dgmgrl show database` command and reports the status of the resource as online if the the local database server is PRIMARY.
open	Creates a lock file in the local agent directory if the `dgmgrl show database` command reports the role of the database as PRIMARY.
clean	Removes the lock file for the following resource states: ■ OFFLINE TIMEOUT ■ OFFLINE INEFFECTIVE ■ ONLINE TIMEOUT ■ UNEXPECTED OFFLINE ■ MONITOR HUNG
actions/DGStatus	Returns the output from the `dgmgrl show database` command.
actions/ActRemote	Freezes or flushes a dependent child group which contains a resource of type Oracle for the same Sid. In the SF Oracle RAC global cluster environment, the Data Guard Broker starts or stops the database instances outside of the agent framework. As a precaution, the Data Guard Broker agent temporarily freezes any child group on which the service group with the Broker resource depends. Thus the agent avoids VCS to report an unexpected offline. The Oracle Data Guard Broker may restart the instances after a considerable time after the failover is complete. So, the cluster administrator must manually unfreeze any child service group after the Broker completes the replication switchover ot failover.

The online function always creates an online lock file to enable database monitoring. The agent then determines the state of the database using the `dgmgrl` command option `show database`.

If the database is already started as PRIMARY, the agent creates the online lock file and exits.

If the database role is STANDBY, the online script assumes that a switch of direction or failover of the replication link is requested. The agent does the following:

- On the node where the Oracle database instance is reported as “standby apply,” the agent initiates a promotion from standby to primary using the Data Guard Broker `dgmgrl` command line interface.
- On the nodes where the database instances are in standby mode, the agent loops and monitors the role of the local instance. The Broker command that is run on the apply instance also takes care of the promotion of all the standby instances. As soon as the agent finds the role as PRIMARY, the agent terminates.
- On the apply instance, the online script requests a `dgmgrl failover` if the agent finds the remote cluster state as FAULTED. In any other case, the script assumes that the primary database instance is still active at the remote site, and requests a local database promotion using `dgmgrl switchover`.

The Oracle Data Guard Broker shuts down all other standby instances and all primary instances except one. The Broker restarts all the instances after the failover or switchover transition is complete. As a precaution, the online script requests a temporary freeze for any child service group which contains a resource of type Oracle with the same Sid attribute value. Thus the agent prohibits any VCS interaction with the resources that the Oracle Broker manipulates as part of a switchover or failover.

The online script monitors the output of the `dgmgrl` command and restarts instances if the Broker requests after reconfiguration of the database profiles. For any database shutdown or startup command, the script uses the `dgmgrl` CLI, so you must configure the Oracle Net to support a database start if the Broker is not active.

See Oracle Data Guard Broker documentation.

The Oracle Data Guard Broker agent relies on the Data Guard Broker command interface to achieve a standby to primary promotion. The agent does not use any other Oracle interfaces like sqlplus or CRS.

Chapter 2

Installing and removing the agent for Oracle Data Guard

This chapter includes the following topics:

Before you install the agent for Data Guard

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 Oracle Data Guard setup in a VCS cluster" on page 11.

Installing the agent for Data Guard

You must install the Oracle Data Guard agent on each node in the cluster. In global cluster environments, install the agent on each node in each cluster.

These instructions assume that you have already installed VCS or SF for Oracle RAC.

Note: The VRTScsodg package contains both the Oracle Data Guard agent and the Oracle Data Guard Broker agent.

To install the agent on AIX systems

1. Determine the device access name of the disc drive.

   ```
   # cd /dev
   # lsdev -C -c cdrom
   ```

   The output resembles:

   ```
   cd0 Available 10-60-00-4,0 16 Bit SCSI Multimedia CD-ROM Drive
   ```

   In this example, the CD device access name is cd0.

2. Insert the disc into the system's drive.

3. Mount the disc.

   ```
   # mkdir -p /cdrom
   # mount -V cdrfs -o ro /dev/cd0 /cdrom
   ```

4. Navigate to the location of the agent packages:

   ```
   # cd /cdrom/aix/replication/dataguard_agent/version/pkgs
   ```

   The variable *version* represents the version of the agent.

5. Add the filesets for the software.

   ```
   # installp -ac -d VRTScsodg.rte.bff VRTScsodg
   ```

To install the agent on HP-UX systems

1. Insert the disc into the system's drive.

2. Create a mount point directory. For example, /cdrom. The directory must have read-write permissions.

3. Determine the block device file for the disc drive.

   ```
   # ioscan -fnC disk
   ```

   For example, the listing may indicate the block device is /dev/dsk/c1t2d0.

4. Start the Portable File System (PFS).

   ```
   # nohup pfs_mountd &
   # nohup pfsd &
   ```

5 Mount the disc.

```
# /usr/sbin/pfs_mount -t rrip /dev/dsk/c#t#d# /cdrom
```

The variable */c#t#d#* represents the location of the drive.

6 Install the agent software. Type one of the following commands depending on the operating system on the node.

HP-UX (PA)

```
# swinstall -s /cdrom/hpux/replication\
/dataguard_agent/version/PA/depot VRTScsodg
```

HP-UX (IA)

```
# swinstall -s /cdrom/hpux/replication\
/dataguard_agent/version/IA/depot VRTScsodg
```

The variable *version* represents the version of the agent.

To install the agent on Linux systems

1 Log in as superuser.

2 Insert the disc into the system's drive.

3 Mount the disc, if the disc does not automatically mount.

```
# mount -o ro /dev/cdrom /mnt/cdrom
```

4 Navigate to the /mnt directory.

```
# cd /mnt/cdrom
```

5 Navigate to the location of the agent package.

```
# cd linux/linux/replication/dataguard_agent/version/rpms/
```

The variable *version* represents the version of the agent.

6 Install the agent software:

```
# rpm -ivh agentrpm
```

The variable *agentrpm* represents the agent package in the rpms directory.

To install the agent on Solaris systems

1 Insert the disc into the system's drive.

```
# cd /cdrom/cdrom0
```

2 Navigate to the location of the agent package.

```
# cd solaris/platform/replication/dataguard_agent
/version/pkgs/
```

The following are the *platform* values:

- x64
- sparc

The variable *version* represents the version of the agent.

3 Install the agent binaries.

```
pkgadd -d . VRTScsodg
```

Removing the agent for Data Guard

Before you attempt to remove the agent, make sure the application service group is not online. You must remove the agent from each node in the cluster.

Note: This procedure removes both the Oracle Data Guard agent and the Oracle Data Guard Broker agent.

To remove the agent from an AIX cluster

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

```
# installp -u VRTScsodg.rte
```

To remove the agent from an HP-UX cluster

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

```
# swremove VRTScsodg
```

To remove the agent from a Linux cluster

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

```
# rpm -e VRTScsodg
```

To remove the agent from a Solaris cluster

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

```
# pkgrm VRTScsodg
```

Chapter 3

Configuring the agent for Oracle Data Guard

This chapter includes the following topics:

Configuration concepts for the Oracle Data Guard agent

Review the resource type definition and the attribute definitions for the agents for Oracle Data Guard. The resource type for both the Oracle Data Guard agent and the Oracle Data Guard Broker agent is defined in the OraDGTypes.cf file.

Resource type and attribute definitions for the Data Guard agent

The resource type definition defines the agent in VCS.

Resource type definition for the Data Guard agent on AIX, HP-UX, and Linux is as follows:

```
type OraDG (
    static keylist SupportedActions = { DGStatus, DGDemotePri }
    static int OnlineRetryLimit = 1
    static int OnlineTimeout = 1200
    static int RestartLimit = 1
    static str ArgList[] = { LinkRes, AgentDebug, Encoding }
    str LinkRes
```

```
    boolean AgentDebug = 0
    str Encoding
    )
```

Resource type definition for the Data Guard agent on Solaris is as follows:

```
type OraDG (
    static str ContainerType = Zone
    static keylist SupportedActions = { DGStatus, DGDemotePri }
    static int OnlineRetryLimit = 1
    static int OnlineTimeout = 1200
    static int RestartLimit = 1
    static str ArgList[] = { LinkRes, AgentDebug, Encoding }
    str ContainerName
    str LinkRes
    boolean AgentDebug = 0
    str Encoding
    )
```

Review the description of the agent attributes. You must assign values to the required attributes.

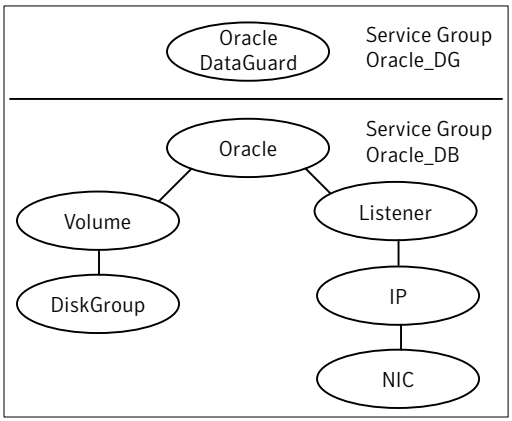
LinkRes	Required attribute Name of the Oracle resource that manages the replicated database instance. Type-dimension: string-scalar
AgentDebug	Optional attribute Logs additional debug messages when this flag is set. Type-dimension: string-scalar Default = 0
Encoding	Optional attribute Specifies the operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. For example, if Oracle output is in “JAPANESE_JAPAN.JA16EUC,” then “eucJP” is the Solaris value for Encoding. Refer to the Oracle and Solaris documentation for respective encoding values. Type-dimension: integer-scalar The default is ““.

Sample configuration for the Data Guard agent

Figure 3-1 shows a sample dependency graph.

VCS service group has a resource of type Data Guard. A second service group contains all necessary resources to control the database instance. The Oracle_DG group depends on the Oracle_DB group, which is an online local soft group dependency.

Figure 3-1 Dependency graph



You can configure a resource of type OraDG in the main.cf file:

```
OraDG oradg_SID1 (
    LinkRes = "ora_SID1"
    )
```

Note the following variations to a standard Oracle database cluster configuration:

- The Oracle resource depends on the Listener resource. The listener process must be already active when the database instance is started because the Data Guard TCP/IP replication links use the Oracle Net Services.
- The IP and NIC resource in the database service group are optional. These resources are only necessary if a cluster on its own protects the primary database. For wide area or site failover, you can implement a transparent network client reconnect.

  To implement a transparent network client reconnect, do one of the following:

  - Use a DNS agent as part of the Data Guard service group
  - Create an alternate Oracle Net Service entries on client machines

- The Oracle resource undergoes and offline-online cycle when promoting a Data Guard standby server to become a primary database. The service group dependency must be soft.

Resource type and attribute definitions for the Data Guard Broker agent

The resource type definition defines the agent in VCS.

Resource type definition for the Data Guard Broker agent on AIX, HP-UX, and Linux is as follows:

```
type OraDGBroker (
    static keylist SupportedActions = { ActRemote }
    static int OnlineRetryLimit = 1
    static int OnlineTimeout = 1800
    static int RestartLimit = 1
    static str ArgList[] = { Sid, Owner, Home, AgentDebug, Encoding }
    str Sid
    str Owner
    str Home
    boolean AgentDebug = 0
    str Encoding
    )
```

Resource type definition for the Data Guard Broker agent on Solaris is as follows:

```
type OraDGBroker (
    static str ContainerType = Zone
    static keylist SupportedActions = { ActRemote }
    static int OnlineRetryLimit = 1
    static int OnlineTimeout = 1800
    static int RestartLimit = 1
    static str ArgList[] = { Sid, Owner, Home, AgentDebug, Encoding }
    str Sid
    str Owner
    str Home
    boolean AgentDebug = 0
    str Encoding
    str ContainerName
    )
```

Review the description of the agent attributes. You must assign values to the required attributes.

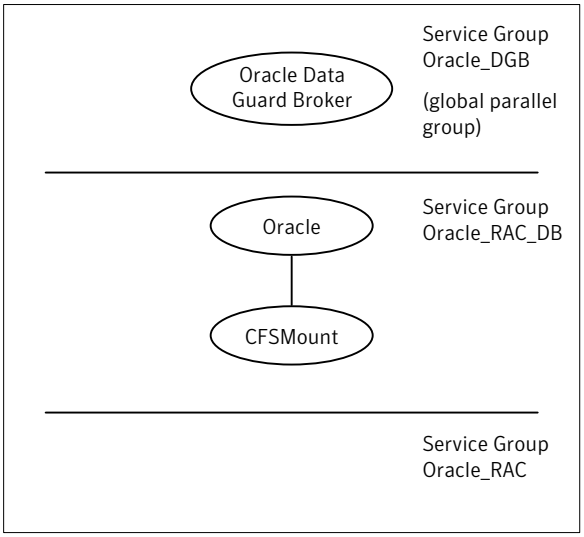
Sid	Required attribute The Oracle instance identifier. Type-dimension: string-scalar
Owner	Required attribute The operating system user who is the owner of the Oracle executables. Type-dimension: string-scalar
Home	Required attribute Location of $ORACLE_HOME where the Oracle binaries are installed. Type-dimension: string-scalar
AgentDebug	Optional attribute Logs additional debug messages when this flag is set. Type-dimension: string-scalar Default = 0
Encoding	Optional attribute Specifies the operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. For example, if Oracle output is in “JAPANESE_JAPAN.JA16EUC,” then “eucJP” is the Solaris value for Encoding. Refer to the Oracle and Solaris documentation for respective encoding values. Type-dimension: integer-scalar The default is ““.

Sample configuration for the Data Guard Broker agent

Figure 3-2 shows a sample dependency graph.

In an SF Oracle RAC environment, VCS service group has a resource of type Data Guard Broker. A second service group contains all necessary resources to control the database instance. The Oracle_DGB group depends on the Oracle_DB group, which is an online local soft group dependency.

Figure 3-2 Dependency graph



You can configure a resource of type OraDGBroker in the main.cf file:

```
OraDGBroker Oracle_DBG (
    Sid@node1 = "DBRAC1"
    Sid@node2 = "DBRAC2"
    User = "oracle"
    Home = "/opt/app/oracle/product/10.2.0/db_1"
    )
```

Note the following variations to a standard Oracle database cluster configuration:

- The Oracle resource or Oracle_RAC_DB service group is optional. The Oracle Data Guard Broker uses it's own interface to the database server. The Broker may run in an Oracle Cluster Ready Service (CRS) environment without any assistance from VCS.
- If you have implemented an Oracle resource, the Oracle resource must use StartUpOpt = SRVCTLSTART. You must configure the Oracle CRS to start the database into "mount" mode.
  See the Oracle Data Guard Broker documentation for Oracle 10g R2.
- You must configure the Oracle network listener to be under the control of the Oracle CRS.

Before you configure the agent for Data Guard

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 Oracle Data Guard agent" on page 25.
- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical Oracle Data Guard setup in a VCS cluster" on page 11.
- Make sure that the cluster has an effective heartbeat mechanism in place.
  See "About cluster heartbeats" on page 31.
- 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*.

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 preventing split-brain

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

Configuring the agent for Data Guard

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

- Changing the database startup profile by adding alternate log destination and creating the necessary Oracle net service entries.
- Creating a second complete database copy on the standby server.
- Adding a new service group with at least the Oracle Data Guard agent. The new service group becomes the parent of the existing Oracle database group.

See the Oracle Data Guard documentation for details on how to configure an Oracle database for Data Guard replication.

On Solaris, the Oracle Data Guard agent is zone-aware. You can configure the agent in local zone or global zone.

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

   /etc/VRTSvcs/conf/OraDGTypes.cf.
3. Click **Import**.
4. Save the configuration.
5. Add a new group with at least one resource of type OraDG for VCS or of type OraDGBroker for SFRAC.
6. Configure the attributes of the OraDG or the OraDGBroker resource that you added.
7. Create an online local soft group dependency between the new OraDG or the OraDGBroker group and the existing Oracle database group.
8. Configure the OraDG or the OraDGBroker service group using the Global Group Configuration Wizard as a global group. See the *Veritas Cluster Server User's Guide* for more information.

9 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.

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

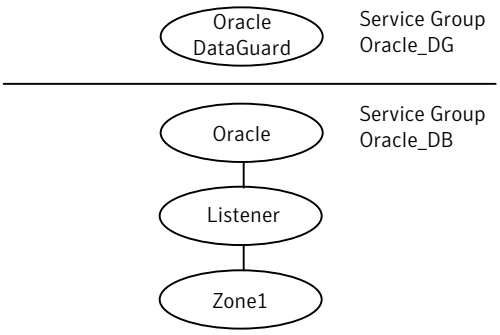
Configuring the agent for Solaris non-global zones

For non-global zone environments (local zones), you need to add a Zone resource and set up the ContainerName attribute. You must set the ContainerName attribute for the OraDG resource. You must also add a Solaris Zone resource under the Listener resource. The Listener and Oracle resources are executed in the non-global zone and you need to set their ContainerName attribute too.

Note: SF Oracle RAC does not support local zones. So, do not configure the Data Guard Broker agent for SF Oracle RAC in local zones.

Figure 3-3 illustrates the dependency tree.

Figure 3-3 Dependency tree



Prepare the configuration with the `hazonesetup` command. This updates the Administrators attribute of the group that operates the Zone, Listener, and the Oracle resource. You need to set the same Administrators attribute for the failover group with OraDG resource manually.

See the *Veritas Cluster Server User's Guide* for more information on using Solaris zones.

Chapter 4

Managing and testing clustering support for Oracle Data Guard

This chapter includes the following topics:

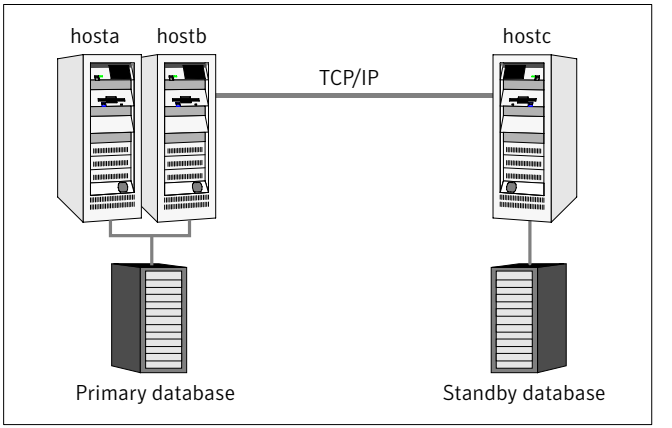
Typical test setup for the Oracle Data Guard agent

A typical test environment includes the following characteristics:

- Two hosts (hosta and hostb) are attached to a shared storage enclosure.
- Another host (hostc) is attached to another local storage device.
- The application runs on hosta, which has access to the shared storage device.
- A single heartbeat over a shared network connects the two sites. The two clusters are connected as VCS global clusters.

Figure 4-1 depicts a typical test environment.

Figure 4-1 Typical test setup



Testing service group migration

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

To perform the service group migration test

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

   Migrate the service group to a host that is attached to the shared storage device.

   Click **Switch To**, and click the system that is attached to the same storage device (hostb) from the menu.

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

   Migrate the service group to a host that attached to a different storage device.

3. Click **Switch To**, and click the system that is attached to the another storage device (hostc) from the menu.

4. 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.

5. Click **Switch To**, and click the system on which the group was initially online (hosta).

Testing host failure

In this scenario, the host where the application runs is lost. Eventually all the hosts in the cluster are lost.

To perform the host failure test

1. Halt or shut down the host where the application runs (hosta).
2. Halt or shut down hostb.

   In a global cluster, a cluster down alert appears and gives you the opportunity to fail over the service group manually.
3. Switch the service group to its original host when VCS starts.

   You can switch the service group only after some Oracle Data Guard reconfiguration. Convert the former primary database on the faulted host to a standby database.

   Refer to the Oracle Data Guard documentation for specific instructions and information on role management.

   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).

Failure scenarios for Oracle Data Guard

Review the failure scenarios and agent behavior in response to failure.

All host or all application failure

If all hosts on the primary side are disabled or if the application cannot start successfully on any primary host, the service group fails over.

In global cluster environments, failover requires user confirmation by default. Multiple service groups can fail over in parallel.

Replication link failure

Data Guard detects link failures, monitors the archive logs created on the active primary. When the standby server reconnects to the primary database server, the

Data Guard resynchronizes the standby database with all the archive logs. The agent resynchronizes the archive logs since the time of the link failure.

The standby database may not contain the most recent data in the following conditions:

- A failover is initiated due to a disaster at the primary site, and
- A synchronization was in progress

However the agent is able to execute a role transition from standby to primary. The database contents at the standby site are always consistent.

After recovery of the replication link, the two replicated databases can be logically inconsistent. The database transactions can result in inconsistency in the following conditions:

- The transactions are committed on the original primary after the link failure, and
- The transactions are never replicated to the standby at the time of takeover on the original primary after the link failure

You can get both sites back into a consistent state only if Oracle flash recovery was enabled at both primary and standby database servers. Otherwise, a restart from the last consistent backup can be necessary.

Split-brain in a Data Guard environment

When split-brain occurs in a replicated database cluster, VCS assumes a total disaster because the primary database is unreachable. VCS attempts to start the application. Once the heartbeats are restored, VCS stops the applications on one side and restarts the VCS engine (HAD). This action eliminates concurrency violation of the same group being online at two places simultaneously.

You must resynchronize the databases manually either by using flashback information or the archive logs. Similar to a replication link failure, a complete restart from a backup copy might be necessary.

In a global cluster, you can confirm the failure before failing over the service groups. You can check with the site administrator to identify the cause of the failure. However, when the heartbeat is restored, VCS does not stop HAD at either site. VCS forces you to choose which group to take offline. You must resynchronize the data manually.

Index

S

T

U