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

AIX, HP-UX, Linux, Solaris

5.0

December 2011

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: 5.0.08.0

Document version: 5.0.08.0.1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/contact_techsupp_static.jsp

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support 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

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec Web site.

https://sort.symantec.com/documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Contents

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 databases that run 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 10gR2 and 11gR1 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.

The VCS agent for Data Guard does not support database environments under the control of Oracle Enterprise Manager.

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

Supported software for Oracle Data Guard

Table 1-1 lists the software versions that the agent for Data Guard supports.

Note: The agent for Data Guard supports all intermediate Maintenance Packs of the major VCS and SFRAC releases listed in Table 1-1

Table 1-1 Supported software for the Data Guard and OraDGSnap fire drill agent

Software	Version	AIX	HP-UX		Linux		Solaris	
			11iv2	11iv3	RHEL	SUSE	x64	SPARC
Veritas Cluster Server (VCS)	5.0	Yes	Yes	No	Yes	Yes	Yes	Yes
	5.1	Yes	No	Yes	Yes	Yes	Yes	Yes
	6.0	Yes	No	Yes	Yes	Yes	Yes	Yes
Veritas SF for Oracle RAC (SFRAC)	5.0	Yes	Yes	Yes	No	No	Yes	Yes
	5.1	No	No	No	No	No	No	Yes
Veritas Volume Manager (VxVM)	5.0	Yes	Yes	No	Yes	Yes	Yes	Yes
	5.1	Yes	No	Yes	Yes	Yes	Yes	Yes
	6.0	Yes	No	Yes	Yes	Yes	Yes	Yes

The Oracle Data Guard agent supports the following Oracle versions:

- Oracle 10gR1 and 10gR2 on AIX, HP-UX, Linux, and Solaris
- Oracle 11gR1and 11gR2 on HP-UX, Linux, and Solaris SPARC

Note: The Oracle Data Guard agent supports only a single standby database instance per configured primary database.

The Oracle Data Guard Broker agent supports the following Oracle versions:

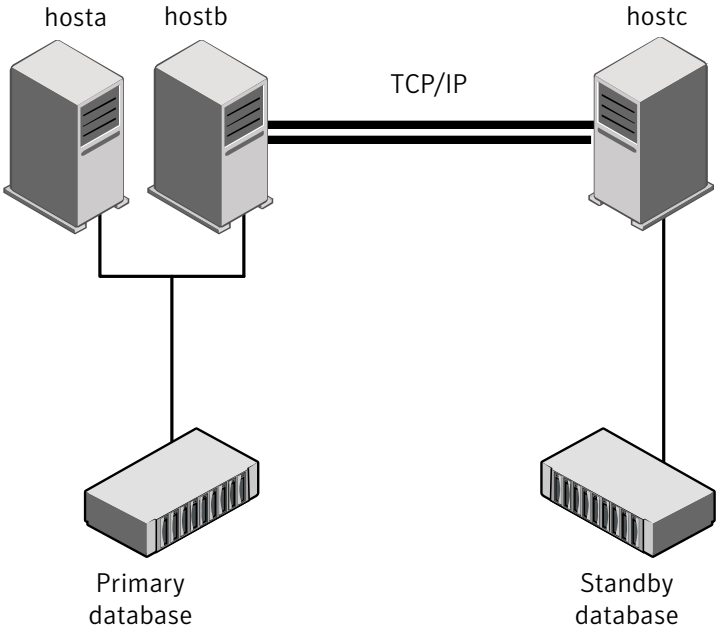
- Oracle 10gR2 on AIX, HP-UX, Linux, and Solaris
- Oracle 11gR1 and 11gR2 on Solaris SPARC

Note: 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 35.

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 16.

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 15.
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 15.
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.
actions/activateStandby	It enables the physical standby database to be opened in a read only mode with redo apply from a mounted state. It works only when the state of database is Mounted.
actions/deactivateStandby	Running this action entry point causes the physical standby database to be shutdown and then mounted with redo apply.
actions/flashbackRecover	It is used to convert a failed primary into a standby database using flashback database. After a failover occurs, the original primary database can no longer participate in the Data Guard configuration until it is repaired and established as a standby database in the new configuration. It works only when flashback is enabled at database level. This feature is enabled only when a new attribute Flashback is set to 1, otherwise by default it is 0, which means disabled.
actions/getremoteSCN	It is used only internally by flashbackRecover action entry point to get the SCN for STANDBY_BECAME_PRIMARY_SCN from new primary (remote node) using `SELECT TO_CHAR (STANDBY_BECAME_PRIMARY_SCN) FROM V$DATABASE`command.
actions/SnapshotOn	It converts the database to snapshot standby and opens the database for read and write operations. It is invoked internally while bringing the OraDGSnap resource online and should not be run manually.
actions/SnapshotOff	It converts snapshot standby database to physical standby. It is invoked internally while bringing the OraDGSnap resource to offline and should not be run manually.

Note: For activateStandby, deactivateStandby, flashbackRecover, SnapshotOn and SnapshotOff action entry points you need to increase the ActionTimeout and MonitorInterval to higher values for OraDG and OraDGSnap type before running. They are supported for Oracle 11gR2 and 11gR1 on Solaris SPARC and Linux.

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 mounts the database. 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 Oracle 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 Oracle 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 in a VCS environment

1. Download the Agent Pack from the Symantec Operations Readiness Tools (SORT) site: https://sort.symantec.com/agents.

   You can download the complete Agent Pack tarball or the individual agent tarball.

2. Uncompress the file to a temporary location, say /tmp.

3. If you downloaded the complete Agent Pack tarball, navigate to the directory containing the package for the platform running in your environment.

AIX	`cd1/aix/vcs/replication/Data Guard_agent/`*`agent_version`*`/pkgs/`
HP-UX (PA)	`cd1/hpux/generic/vcs/replication/Data Guard_agent/`*`agent_version`*`/PA/depot/`
HP-UX (IA)	`cd1/hpux/generic/vcs/replication/Data Guard_agent/`*`agent_version`*`/IA/depot`
Linux	`cd1/linux/generic/vcs/replication/Data Guard_agent/`*`agent_version`*`/rpms/`
Solaris	`cd1/solaris/dist_arch/vcs/replication/Data Guard_agent/`*`agent_version`*`/pkgs/`

   If you downloaded the individual agent tarball, navigate to the pkgs directory (for AIX, HP-UX, and Solaris), or rpms directory (for Linux).

4. Log in as superuser.

5. Install the package.

AIX	`# installp -ac -d VRTScsodg.rte.bff VRTScsodg.rte`
HP-UX (PA)	`# swinstall -s 'pwd' VRTScsodg`
Linux	`# rpm -ihv \` `VRTScsodg-`*`AgentVersion`*`-Linux_GENERIC.noarch.rpm`
Solaris	`# pkgadd -d . VRTScsodg`

Upgrading the Oracle Data Gaurd agent

Perform the following steps to upgrade the agent with minimal disruption, in a VCS environment

1. Persistently freeze the service groups that host the application.

   ```
   # hagrp -freeze group -persistent
   ```

2. Stop the cluster services forcibly.

   # hastop -all -force

3. Ensure that the agent operations are stopped on all the nodes.

   # ps -ef |grep OraDg

4. Uninstall the agent package from all the nodes.

   See "Removing the agent for Oracle Data Guard" on page 22.

5. Install the new agent on all the nodes.

   See "Installing the agent for Oracle Data Guard" on page 19.

6. Copy the new OraDGTypes.cf file from the agent's conf directory

VCS Version	Operating system	Agent types files
VCS 5.x	■ AIX ■ HP-UX ■ Linux	/etc/VRTSvcs/conf/OraDGTypes.cf
VCS 5.0	Solaris SPARC and x64	/etc/VRTSvcs/conf/OraDGTypes_50.cf
VCS 5.1	Solaris SPARC and x64	/etc/VRTSvcs/conf/OraDGTypes.cf

   to the VCS conf directory /etc/VRTSvcs/conf/config.

7. Check for the changes in the resource values required, if any, due to the new agent types file.

8. Start the cluster services.

   # hastart

9. Unfreeze the service groups once all the resources come to an online steady state.

   # hagrp -unfreeze *GroupName* -persistent

Removing the agent for Oracle 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.

To remove the agent, type the following command on each node. Answer prompts accordingly:

AIX	`# installp -u VRTScsodg.rte`
HP-UX	`# swremove VRTScsodg`
Linux	`# rpm -e VRTScsodg`
Solaris	`# pkgrm VRTScsodg`

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

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

```
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 Linux and HP-UX is as follows:

```
type OraDG (
static keylist SupportedActions = { DGStatus, DGDemotePri, activateStandby,
deactivateStandby, getremoteSCN, flashbackRecover, SnapshotOn, SnapshotOff  }
static int OnlineRetryLimit = 1
static int OnlineTimeout = 1200
static int RestartLimit = 1
static str ArgList[] = { LinkRes, AgentDebug, Encoding, Flashback }
str LinkRes
boolean AgentDebug = 0
boolean Flashback = 0
str Encoding
)
```

Resource type definition for the Data Guard agent on Solaris for VCS 5.0 or before:

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

Resource type definition for the Data Guard agent on Solaris for VCS 5.1 and later:

```
type OraDG (
static keylist SupportedActions = { DGStatus, DGDemotePri, activateStandby,
deactivateStandby, getremoteSCN, flashbackRecover, SnapshotOn, SnapshotOff }
static int OnlineRetryLimit = 1
static int OnlineTimeout = 1200
static int RestartLimit = 1
```

```
static str ArgList[] = { LinkRes, AgentDebug, Encoding, Flashback }
static int ContainerOpts{} = { RunInContainer=1, PassCInfo=0 }
str LinkRes
boolean AgentDebug = 0
boolean Flashback = 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 ““.
Flashback	Used to enable flashback recovery when failed primary comes up. It is used by flashbackRecover action entry point. The default value is 0.

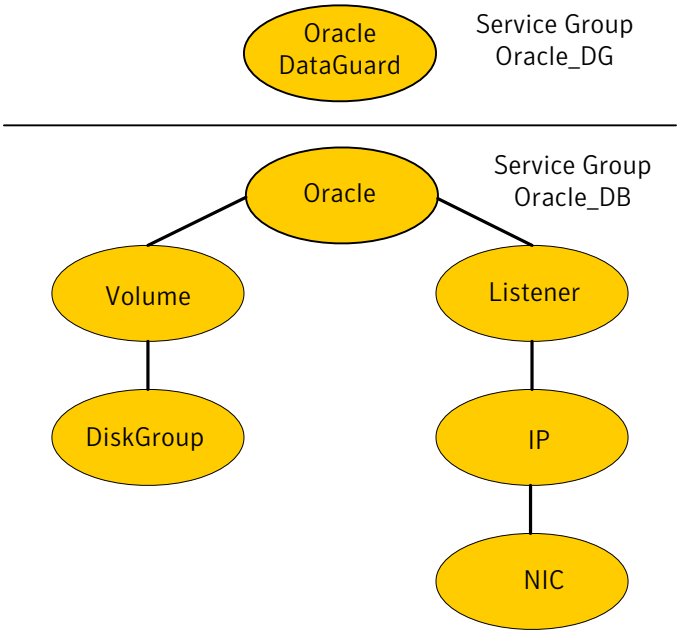
Sample configuration for the Data Guard agent

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:

```
group global_db_rep (
        SystemList = { primary-sys1 = 0, primary-sys2 = 1 }
        ClusterList = { dgclus1 = 0, dgclus2 = 1 }
                )

        OraDG dg_res (
                LinkRes = ora_db_prod
                Flashback = 1
                )

        requires group oradb_prod_SG online local soft



group oradb_prod_SG (
```

```
 SystemList = { primary-sys1 = 0, primary-sys2 = 1 }
 )

        IP lsnr_ip (
         Device = eth0
         Address = "10.209.71.181"
         NetMask = "255.255.252.0"
         )

 LVMLogicalVolume ora_vol (
         LogicalVolume = OraData
         VolumeGroup = VolGroup01
         )

 LVMVolumeGroup ora_grp (
         VolumeGroup = VolGroup01
         )
Mount ora_mnt (
         MountPoint = "/u01"
         BlockDevice = "/dev/mapper/VolGroup01-OraData"
         FSType = ext3
         FsckOpt = "-y"
         )

 NIC lsnr_nic (
         Device = eth0
         )

 Netlsnr ora_db_lsnr (
         Owner = oracle
         Home = "/u01/app/oracle/product/11.2.0/db_1"
         Listener = DGUARD
         )

 Oracle ora_db_prod (
         Sid = dguard
         Owner = oracle
         Home = "/u01/app/oracle/product/11.2.0/db_1"
         StartUpOpt = CUSTOM
         )

 lsnr_ip requires lsnr_nic
 ora_db_lsnr requires lsnr_ip
```

```
ora_db_prod requires ora_mnt
ora_vol requires ora_grp
ora_mnt requires ora_vol
ora_db_prod requires ora_db_lsnr
```

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 an offline-online cycle when promoting a Data Guard standby server to become a primary database. The service group dependency must be soft.
- The name of the Oracle DataGuard resource must be the same in each global cluster configuration. Otherwise, the DemotePri action entry point that is essential for a failover will not work.

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

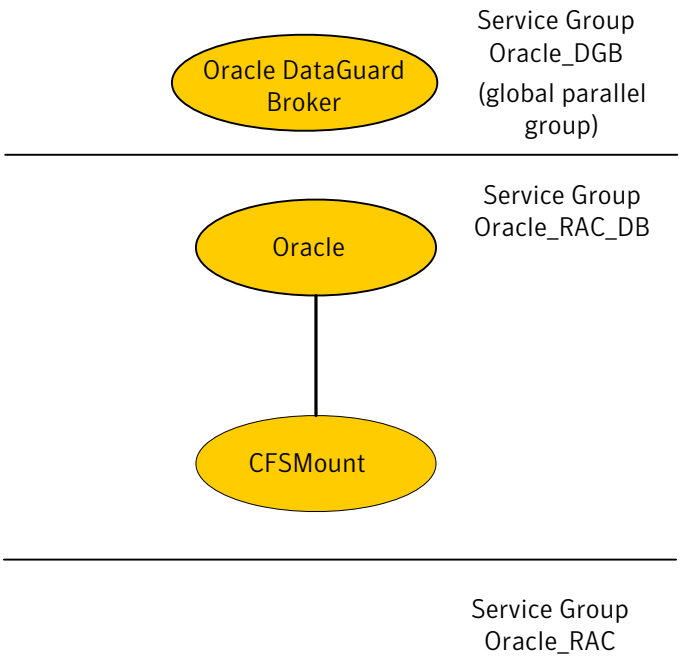
Encoding	Optional attribute Specifies the operating system encoding that corresponds to Oracle encoding for the displayed Oracle output. For example, if Oracle output is in “JAPANESE_JAPAN.JA16EUC,” then “eucJP” is the Solaris value for Encoding. Refer to the Oracle and Solaris documentation for respective 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.
- The name of the Oracle DataGuard Broker resource must be the same in each global cluster configuration. Otherwise, the DemotePri action entry point that is essential for a failover will not work.

Working of Active Physical Standby feature

The Active Data Guard Option available with Oracle Database 11g Enterprise Edition enables you to open a physical standby database for read-only access for reporting, for simple or complex queries, sorting, or Web-based access while Redo Apply continues to apply changes received from the production database. All queries reading from the physical standby database execute in real time, and return current results. With Active Dataguard, you can offload any operation that requires up-to-date, read-only access to the standby database. To support active standby in Oracle Dataguard agent, we have added two action entry points, activateStandby and deactivateStandby.

activateStandby - On physical standby, it mounts the database in Read-only with Redo apply using below SQL commands:

- `ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL`
- `ALTER DATABASE OPEN READ ONLY`

- `ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE DISCONNECT`

deactivateStandby - It works differently for different version of Oracle. For 11gR2, only oracle resource needs to offline and then online. But, for 11gR1 it needs to send requests to primary database to send redo log to standby as connection goes down after database offline, using `ALTER SYSTEM ARCHIVE LOG CURRENT`SQL command.

Working of Snapshot Standby Feature

The Snapshot Standby database feature available with Oracle Database 11g Enterprise Edition enables you to open a physical standby database for read-write access when a user requires an updateable snapshot of the physical standby database. A snapshot standby receives and archives redo data from a primary database but does not apply the redo data it receives. The redo data received from the primary database is applied once the snapshot standby database is converted back into a physical standby database, after discarding all local updates to the snapshot standby database. Queries executed on a Snapshot standby database will not provide current results to the user.

To support Snapshot standby in Oracle Dataguard agent, we have added two action entry points:

SnapshotOn - On physical standby, it converts the database to snapshot standby and opens the database for read-write.

- Run `ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL` to stop redo apply.
- Run `ALTER DATABASE CONVERT TO SNAPSHOT STANDBY` to convert the physical standby to snapshot standby database.
- Run `ALTER DATABASE OPEN` to open the database in read/write mode

SnapshotOff - It converts snapshot standby database to physical standby.

- Takes the database service group offline and then online to get the database in a MOUNTED state.
- Run `ALTER DATABASE CONVERT TO PHYSICAL STANDBY` to convert snapshot database to physical standby.
- Takes the database service group offline.
- Takes the database service group online.

Working of Flashback Recover feature

This feature is used to convert a failed primary into a standby database using flashback database. After a failover occurs, the original primary database can no longer participate in the Data Guard configuration until it is repaired and established as a standby database in the new configuration. To do this, you can use the flashbackRecover action entry point to recover the failed primary database to a point in time before the failover occurred, and then convert it into a physical standby database in the new configuration. A are completed, the Physical Standby database will become part of the Dataguard configuration and get in sync with the Primary database server. While executing the action entry point, it would check for the following conditions:

- Value of Flashback attribute of Dataguard resource is set to 1 or 0.
- Flashback is enabled at database level or not.
- Authority- If it is 1, then it would fail as it is running on new primary. Authority is 0, the action entry point would run on the failed primary.
- If failed primary and new primary database's role is PRIMARY, then it would proceed for flashback recovery.

Once the above conditions are met, it would continued as below:

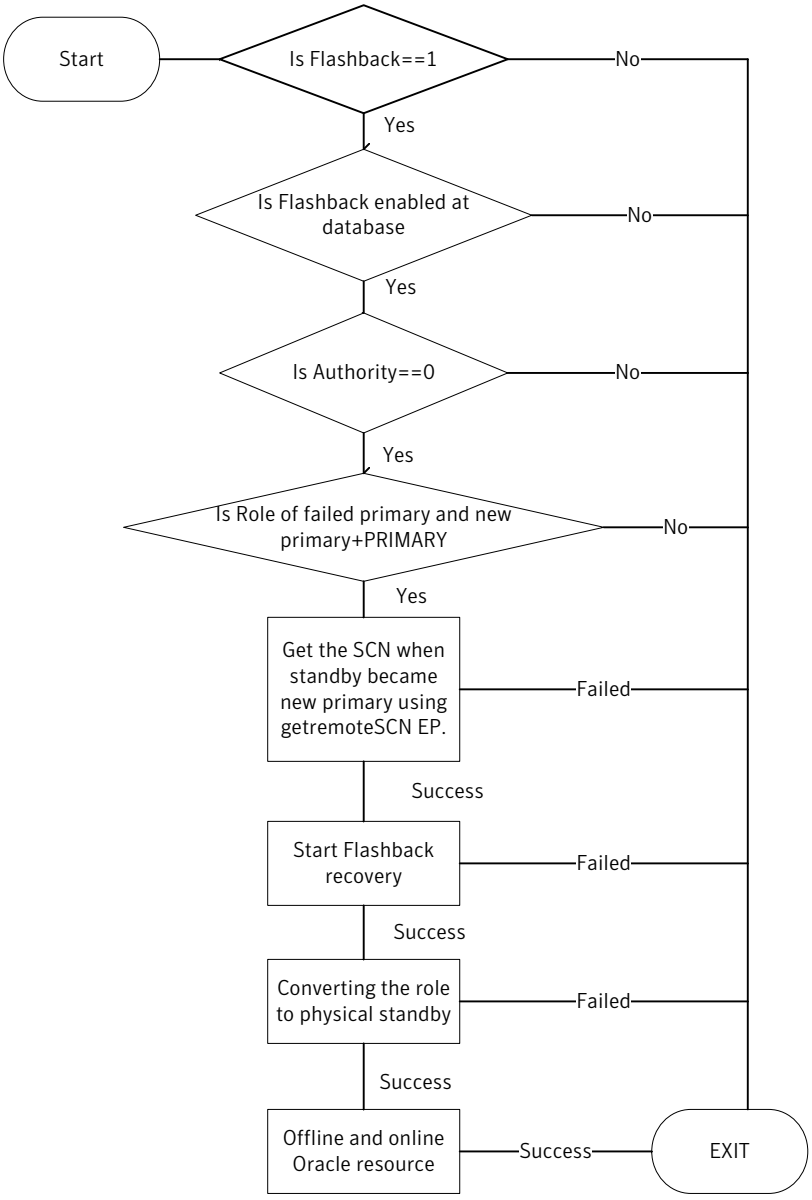
1. Determine the SCN at which the old standby database became the primary database, which is done using getremoteSCN action entry point.
2. Shutdown the old primary database (if necessary), mount it, and flash it back to the value for STANDBY_BECAME_PRIMARY_SCN that was determined in earlier step.
3. Converts the database to a Physical Standby using "ALTER DATABASE CONVERT TO PHYSICAL STANDBY" command and then offline and online oracle resource.

After the successful execution of the flashbackRecover action entry point on the failed primary, the new DATABASE_ROLE = PHYSICAL STANDBY and SWITCHOVER_STATUS = SWITCHOVER LATENT or SWITCHOVER PENDING or NOT ALLOWED.

Note: The user or DBA now needs to ensure that the Physical Standby Database receives and applies all the missing changes from the Primary database. Once the manual tasks by the user or DBA are completed, the Physical Standby database will become part of the Dataguard configuration and get in sync with the Primary database server. Do not run the Fire Drill in "ro" or "rw" configuration until the Standby database is brought in sync with the Primary database.

Flowchart for Flashback feature

Figure 3-3 Flowchart for Flashback feature



Before you configure the agent for Oracle 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 23.
- 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 35.
- 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 Oracle 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.

Note: Symantec recommends that you increase the values of the ActionTimeout, MonitorInterval, and OnlineTimeout attributes of the OraDG resource to suit your environment. Increasing the values of these attributes ensures that switchover and failover operations do not fail. The initial recommended value for ActionTimeout is 240, MonitorInterval is 480, and OnlineTimeout is 1200. This values may need to be fine-tuned to suit your environment.

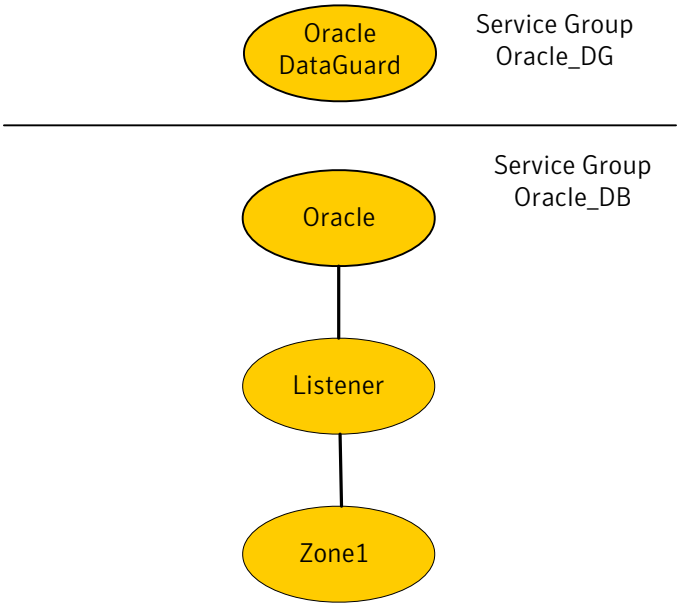
Configuring the agent for Solaris non-global zones

For non-global zone environments (local zones) running under VCS 5.0 or previous versions, 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. For non-global zone environments (local zones) running under VCS 5.1 or later versions, you need to add a Zone resource and set up the ContainerInfo attribute. You must set the ContainerInfo attribute for the OraDG service group . 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 the ContainerInfo attribute for the service group containing the oracle and zone resource too.

Note: Import relevant DataGuard types file before configuring the above attribute as mentioned in the Upgrade section. SF Oracle RAC does not support local zones. So do not configure the DataGuard Broker agent for SF Oracle RAC in local zones.

Figure 3-4 illustrates the dependency tree.

Figure 3-4 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.

For Oracle Data Guard to work in Zone across GCO you need to follow below steps:

1. On Primary cluster run the hazonesetup script which creates a VCS user, Group and updates the Administrators attribute of the group that operates the Zone, Listener, and the Oracle resource.
2. Running the `# hauser -display`command will display the user created and the groups to which priviliges are associated.
3. Set the Administrator attribute attribute for the failover group with OraDG resource manually by running the command `# hauser -addpriv <zone vcs user> Administrator -group <service group name>`
4. Create the same VCS user created by running the hazonesetup script on the DR cluster:`# hauser -add <zone vcs user> -priv Administrator -group <group with OraDG resource> <group with Zone, Oracle, Listener resource>`
5. Enter password.

6 Run the steps from 1 to 5 and then vice versa.

7 Provide the same password as in step 5.

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

Configuration example:

```
group global_db_rep (
        SystemList = { sec-host = 0 }
                ContainerInfo @ sec-host = { Name = dr_zone , Type = Zone,
        ClusterList = { clus-pm = 1, clus-dr = 0 }
        Administrators = { z_zoneres_pm-host, z_zoneres_sec-host }
        )

        OraDG dg_res (
                LinkRes = oradb_stby
                Flashback = 1
                )

        requires group zone_orasg online local soft

group zone_orasg (
  SystemList = { sec_host = 0 }
        ContainerInfo @ sec-host = { Name = dr_zone , Type = Zone, Enabled
        Administrators = { z_zoneres_pm-host, z_zoneres_sec-host }
        )

        Netlsnr lsnr (
                Enabled = 0
                Owner = oracle
                Home = "/u01/app/oracle/product/11.2.0/dbhome_1"
                Listener = DGUARD
                )

        Oracle oradb_prod (
                Enabled = 0
                Sid = dguard
                Owner = oracle
                Home = "/u01/app/oracle/product/11.2.0/dbhome_1"
                StartUpOpt = CUSTOM
                )

        Zone zone_res (
```

```
                )

        lsnr requires zone_res
        oradb_prod requires lsnr

group fd_sg (
        SystemList = { vcssx208 = 0 }
        ContainerInfo @ sec-host = { Name = dr_zone , Type = Zone, Enabled = 1
        Administrators = { z_zoneres_pm-host, z_zoneres_sec-host }
        )

        OraDGSnap fd_res (
                Critical = 0
                TargetRes = dg_res
                )
requires group  global_db_rep offline local
```

Chapter 4

Managing and testing clustering support for Oracle Data Guard

This chapter includes the following topics:

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.

Chapter 5

Setting up a fire drill

This chapter includes the following topics:

About fire drills

A fire drill procedure verifies the fault-readiness of a disaster recovery configuration. This procedure is done without stopping the application at the primary site and disrupting user access.

A fire drill is performed at the secondary site using a special service group for fire drills.The fire drill service group uses a read-only copy or snapshot of the database that is used by the application service group. Bringing the fire drill service group online demonstrates the ability of the application service group to come online as a Primary database at the remote site when a failover occurs.

The agent supports FireDrill in a single instance environment for Oracle11gR1 and later.

About Snapshot Attributes

OraDGSnap agent supports the following fire drill configurations based on the SnapMode attribute value:

ro — In this configuration, the Standby database is converted to an Active Physical Standby database. The database is available for querying, reporting, backup, etc. Nothing can be written to the database. The changes on the Primary database are applied to the Standby database in real time.

In the 'ro' configuration, VCS does the following:

- Stop the redo apply process on the Physical Standby database.
- Open the database in Read Only mode.
- Start redo apply.

rw — In this configuration, the Standby database is converted to a Snapshot Standby database. The database is available for read and write modifications. However, the changes on the Primary database are archived at the Standby database but not applied.

In the 'rw' configuration, VCS does the following:

- Stop the redo apply process on the Physical Standby database.
- Convert the database to Snapshot standby.
- Open the database for read and write modifications.

TargetRes should be set to oradg resource.

About the OraDGSnap agent

The OraDGSnap agent is the fire drill agent for Oracle DataGuard. The agent handles how the Standby database can be opened so that users can check the integrity of the database or use it for additional purposes such a reporting, backups, etc. The behavior of the OraDGSnap agent is based on the SnapMode attribute. If the value is "ro", the agent will open the Standby database in read only mode with redo apply. If the SnapMode is set to "rw", the agent will open the Standby database in read/write mode. In this case, redo logs are received and archived but not applied to the standby database.

Note: No changes made on the primary database are visible on the snapshot standby database during the period of the Fire Drill.

Switchover/Failover of the OraDG resource will fail if the Standby database is in a Snapshot Standby database mode and ClusterFailover policy is set to manual.

OraDGSnap agent functions

The OraDGSnap agent performs the following functions:

online	It acts based on the value of SnapMode. It invokes activateStandby if it is 'ro' and SnapshotOn if 'rw' and creates a lock file.
offline	It acts based on the value of SnapMode. It invokes deactivateStandby if it is 'ro' and SnapshotOff if 'rw' and removes the lock file.
monitor	Verifies the existence of the lock file to make sure the resource is online.
clean	It invokes SnapshotOff or deactivateStandby and removes Lock file.

Resource type definition for the OraDGSnap agent

Following is the resource type definition for the OraDGSnap agent:

```
type OraDGSnap (
        static int OnlineRetryLimit = 1
        static int OnlineTimeout = 1200
        static int RestartLimit = 1
        static boolean FireDrill = 1
        static str ArgList[] = { TargetRes, SnapMode }
        str TargetRes
        str SnapMode
)
```

Attribute definitions for the OraDGSnap agent

To customize the behavior of the OraDGSnap agent, configure the following attributes:

TargetRes	Set this attribute to the name of the OraDG type resource Type-Dimension: string-scalar

SnapMode	Specifies whether the Standby database will be open in an Active Standby or Snapshot Standby mode. For Active Standby set this attribute to “ro” and for Snapshot Standby set this attribute to “rw”. Type-Dimension: string-scalar

Before you configure the fire drill service group

Before you configure the fire drill service group, follow the steps below:

- Make sure the application service group is configured with a OraDG resource.
- To use the Fire Drill option with SnapMode set to “rw”, the standby database must have Flashback option enabled on the database level.

Sample configuration for a fire drill service group

This is a sample configuration of a fire drill service group where a OraDG resource dgu1 is configured under a global service group and a OraDGSnap resource is configured under the oradgfd fire drill service group. A local offline dependency is created between the fire drill service group and the global service group.

You can configure a resource of type OraDGSnap in the main.cf file as follows.

```
group globaldg (
          SystemList = { vcssx208 = 0 }
          ClusterList = { clus-dg1 = 1, clus-dg2 = 0 }
          )

          OraDG dgu1 (
                  LinkRes @vcssx208 = ora1
                  AgentDebug @vcssx208 = 1
                  Flashback = 1
                 )

         requires group oradgst online local soft


 group oradgfd (
          SystemList = { vcssx208 = 0 }
         )

         OraDGSnap oradgsnap (
```

```
    TargetRes = dgu1
        SnapMode = rw
)
```

Troubleshooting

While bringing the the Fire Drill service group to offline on a Snapshot standby database may cause the action to timeout and cause the database to be left in an unusable state. Check the engine logs to identify any such problems. If the oracle resource is not configured with detailed monitoring option then the resource may not report a fault. In such a situation increase the Monitor Interval Attribute of OraDGSnap and OraDG attribute to a larger value.

To recover from the above problem, perform the following steps:

1. Run the DGStatus action entry point on the standby database to know its current role and state. Run

   ```
   # hares -action <OraDG resource> DGStatus 0 -sys <hostname>
   ```

2. If the output of step 1 is DATABASE_ROLE = SNAPSHOT STANDBY and OPEN_MODE = MOUNTED, open a SQL session to the snapshot standby database or go to to step 6.
3. Run `SQL> ALTER DATABASE CONVERT TO PHYSICAL STANDBY`
4. Bring the the database service group to Offline. Run

   ```
   # hares –offline <database resource> -sys <hostname>
   ```

5. Bring the the database service group. Run

   ```
   # hares –online <database resource> -sys <hostname>
   ```

6. If the output of step 1 shows Error `ORA-01507: database not mounted`, bring the database service group to offline. Run `# hares –offline <database resource> -sys <hostname>`
7. Bring the the database service group to online. Run

   ```
   # hares –online <database resource> -sys <hostname>
   ```

Index

R

S

T

U