Office of the State Treasurer
Debt Management System

Disaster Recovery Plan

Release <1.4>

[redacted]

Acceptance of Disaster and Recovery Plan Deliverable

Office of The State Treasurer
DMS PHASE I
SOT001

Accepted by:		Accepted by:	
	Date		Date
Office Of The State Treasurer		[redacted]	
	Date	[redacted]	Date
Project Manager Office Of The State Treasurer			

Revision History

Date	Description	Author
	Draft (Version 1.0)	[redacted]
06/19/2003	Version 1.1	[redacted]
07/14/2003	Version 1.2 (Revisions)	[redacted]
07/18/2003	Version 1.3 (Revisions)	[redacted]
09/08/2003	Version 1.4 (Revisions) [FINAL]	[redacted]

Table of Contents

1. Introduction and Objectives 5

2. Production and Standby Server Configuration 6

The following is the configuration for the Production Database Server and Application Server: 7

3. Traditional Backup vs Standby Server 8

4. Overview of Oracle Standby Database 9

5. DMS Disaster Recovery Implementation 9

6. DMS Disaster Recovery Maintenance 12

7. DMS Disaster Recovery Operation 13

8. Return to Normal Operations 17

9. Test Plans 19

10. Vendor Support 22

11. Technical References 23

1. Introduction and Objectives

Debt Management System (DMS) is a web-based multi-tiered application: Its core components are the **Oracle Database** and **Application Server**; therefore, the main focus of this document describes the process of backing up and protecting an Oracle database; the development and implementation of the Debt Management System's Disaster Recovery Plan (DMS-DRP) should be part of STO's day-to-day activities.

The primary objective of the DMS DRP is to enable STO to survive a disaster (as defined in the STO Enterprise Disaster Recovery Document) and continue close-to-normal servicing and operations. The two most important requirements are:

- To restore and make accessible to end users the critical and vital operating environments and data described in the DMS-DRP within **48** hours of a disaster declaration
- To assist STO in accomplishing a speedy, orderly return to normal production operations, while complying with the Department of Information Technology (DOIT) standards

In order to survive, the organization must assure that critical operations can resume/continue normal processing. Throughout the recovery effort, the plan establishes clear lines of authority and prioritizes work efforts. The key objectives of the contingency plan should be to:

- Continue critical business operations
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources)
- Facilitate effective co-ordination of recovery tasks
- Reduce the complexity of the recovery effort
- Document a detailed process so that if the system is operational, there is a process identified to walk the user through getting the system back up

The roles and responsibilities for STO IT staff for the execution of the disaster recovery plan will be as defined in the Enterprise Disaster Plan for STO. Staff from the STO IT and the Technical Support will be identified to perform the execution of this plan.

Assumptions

This document is based in the following assumptions and conditions:

- This is NOT a simple “backup here, restore there solution”
- This is NOT an Enterprise-wide backup strategy
- This is a very specific solution to increase the availability of an application, by having a single Standby server in a different geographical location, waiting to be activated to replace the functionality of several others, in case of a disaster
- Servers and systems switchover to the redundant unit(s) will NOT occur automatically; it rather requires some administrator’s and end-user’s interaction/configuration
- DMS (and its Oracle database) will be running 7x24
- The redundant systems will function degraded-mode information processing activities until the problem is resolved
- The redundant server and required software will be located at [redacted]
- Daily tape backups of the DMS server(s) will be taken to a secured site/location. These tapes are to be shipped to the redundant facility [redacted] in the event of an emergency; production data of the redundant site is within 24 hours of being synchronized with the production site
- A permanent LAN/WAN link exists between the Sacramento [redacted] sites; servers can connect to each other during non-emergency conditions

2. Production and Standby Server Configuration

The following software is required for the Standby Database Server:

- Windows [redacted]
- Terminal Services [redacted]
- Oracle [redacted]
- Oracle [redacted]
- Oracle [redacted]
- Veritas [redacted]

And the hardware configuration:

	Description	Item #	Part #
Vendor	[redacted]		
Base Unit	[redacted]	[redacted]	[redacted]
Processor	[redacted]	[redacted]	[redacted]
Memory	[redacted]	[redacted]	[redacted]
Hard Drive	[redacted]	[redacted]	[redacted]
Hard Drive Controller	[redacted]	[redacted]	[redacted]
Operating	[redacted]	[redacted]	[redacted]

	Description	Item #	Part #
system			
Operating System			
Additional Storage Products			
Features (1)			
Miscellaneous			
Support			
Support(2)			

The following is the configuration for the Production Database Server and Application Server:

- Windows
- Terminal Services
- Oracle
- Oracle
- Oracle
- Veritas

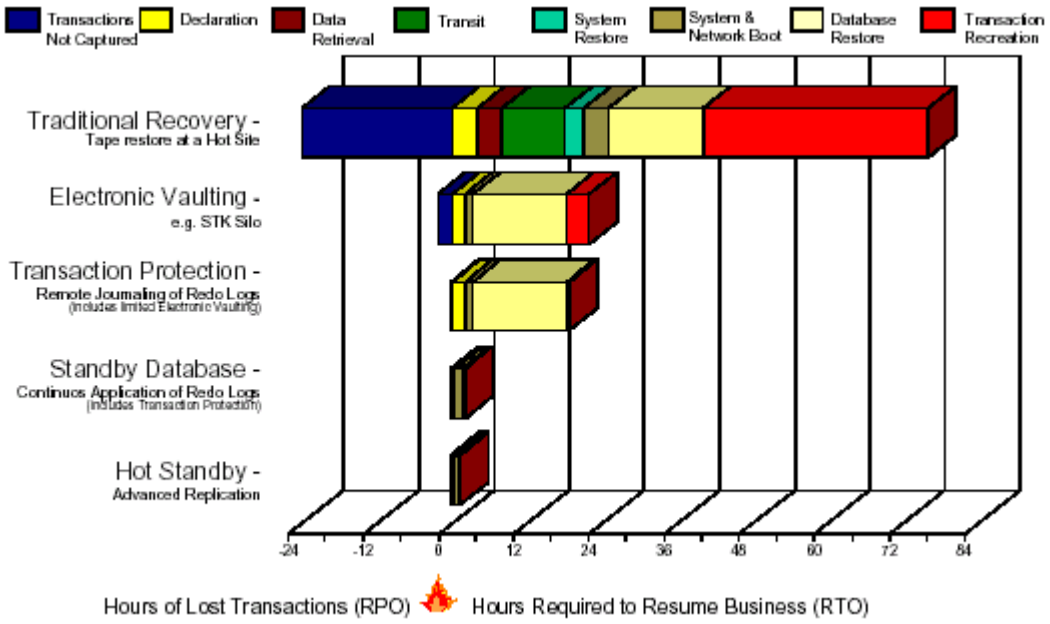
And the hardware configuration:

	Description	Item #	Part #
Vendor			
Base Unit			
Processor			
Memory			
Hard Drive			
Hard Drive Controller			
Operating system			
Operating System			
Additional Storage Products			
Features (1)			
Miscellaneous			
Support			
Support(2)			

The Client Access Licenses for Windows will not impact the number of users accessing the application via the Web interface.

3. Traditional Backup vs Standby Server

A study published by Comdisco Recovery Services, Inc. shows the recovery times using different techniques, including the *Traditional Backup/Restore* and *Standby Database Server*. The chart is based upon several actual customer data.



The horizontal axis shows the time of failure as “0 Hours”, with *Hours of Lost Transactions* (Recovery Point Objective) to the left (negative) and *Hours Required to Resume Business* (Recovery Time Objective) in the positive range.

In the *Traditional Recovery* approach:

- Nightly backups are performed
- Courier services pick up the backup media from the production site daily
- Tapes are stored at a secure location, which is usually not the Recovery Site
- In the event of a failure of the Production Site, backups are restored, then Redo Logs are applied to re-build the database
- The recovery process is very long and moderately difficult
- A high number of transactions is lost

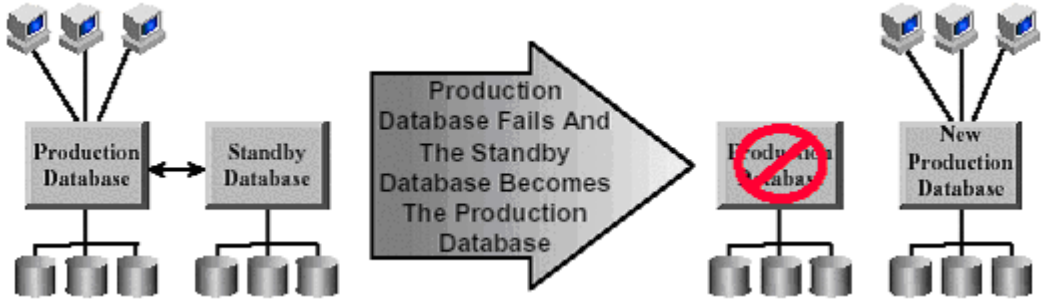
In the Standby Database approach:

- The Redo Logs are continuously shipped and applied to the dedicated Standby system as they are created
- Automated log shipping can be used to send the archive logs
- Finally, the Standby System must be reconfigured to become the Production System
- Full backups are still recommended at the Sites
- The recovery process is very fast and moderately difficult
- A very small number of transactions is lost

Oracle *Standby Database* performing continuous application of Redo Logs is the disaster recovery solution most frequently used for Oracle mission critical applications. While a *Hot Standby* provides slightly higher improved fail-over characteristics, a Standby Database is easier to implement and does not require application program modification.

4. Overview of Oracle Standby Database

An automated Standby Database provides a means to create and maintain a remote copy of a production Database. The Standby Database can take over processing from the primary Production Database, providing near continuous database availability.



Under normal conditions:

- The Production Database is servicing the clients and sending the Redo Logs to the Standby Database
- The Standby Database is in constant Recovery Mode, applying the archive logs to ensure proper synchronization with the Production Database

When a catastrophe occurs:

- The Production Database is NO longer available
- The Standby Database is reconfigured for servicing the clients and opened in read/write mode. Once this process has occurred, the database can NOT be put back to the Standby mode

While a Standby Database can also be used as a read-only database, to temporarily off-load query processing from the production database, such process does not directly relate to DRP and will not be discussed in this document.

It is imperative that the production database be run in archive log mode and that the archived redo logs are archived to a suitable media so that they can be used for recovery. The DBA unit of STO must take “Hot” backups of the production database on a daily basis.

5. DMS Disaster Recovery Implementation

DMS consists of three interacting components:

- Supporting Operating System and Servers (database/application)
- DMS data (stored in the Oracle Database)
- And DMS application, programs, reports and forms

To successfully implement a Primary-Standby Database synchronization schema, the following conditions exist:

- Primary and Standby Databases must reside on the same hardware type [redacted] and base operating system [redacted]
- The database versions should also be identical; at the very least, Standby and Primary databases should never cross major releases [redacted]
- The init.ora parameter *compatible* must be identical, and configurations with different releases need to be tested and validated.

Then, a simple 3-phase implementation process begins:

- Preparation and configuration of the Primary Site (STO – Sacramento)

- Shipment of files
- Preparation and configuration of the Standby Site [redacted]

The standby database will be created using the automated tool “Data Guard”, provided with the Oracle Enterprise Manager (OEM). Oracle Data Guard is the management. monitoring and automation software that automates the creation and subsequent maintenance of a standby copy of the primary (production) database. If the primary database becomes inactive, then the standby database can be activated and can take over the data serving needs for STO.

The Data Guard architecture incorporates the following items:

- **Primary Database:** which is the actual production database, running in archive log mode and which is used to create the standby. The archived logs from the primary database are transferred and applied to the standby database(s). Each standby database can be associated with a single primary database, but a single primary database can be associated with multiple standby databases.
- **Standby Database:** which is the replica of the primary database.
- **Log Transport Services:** Control the automatic transfer of archive redo log files from the primary database to the standby database(s).
- **Log Apply Services:** Apply the archived redo logs to the standby database.
- **Role Management Services:** Control the changing of database roles from primary to standby. These services include switchover, switchback and fail over.
- **Data Guard Broker:** Controls the creation and monitoring of the Data Guard. It comes with a GUI or a command line interface.

Data Guard currently supports two architectures:

- Data Guard Redo Apply Architecture (Physical Standby)
- Data Guard SQL Apply Architecture (Logical Standby)

- STO IT has decided to go in with the **Physical Standby Architecture**. In this architecture;
  - The physical standby database is a block-for-block copy of the primary database.
  - Uses the database recovery functionality to apply the changes made to the primary.
  - Standby database can be opened in read only mode for queries/reporting.

It is recommended to use the **Redo Apply Architecture** for the DMS for the following reasons:

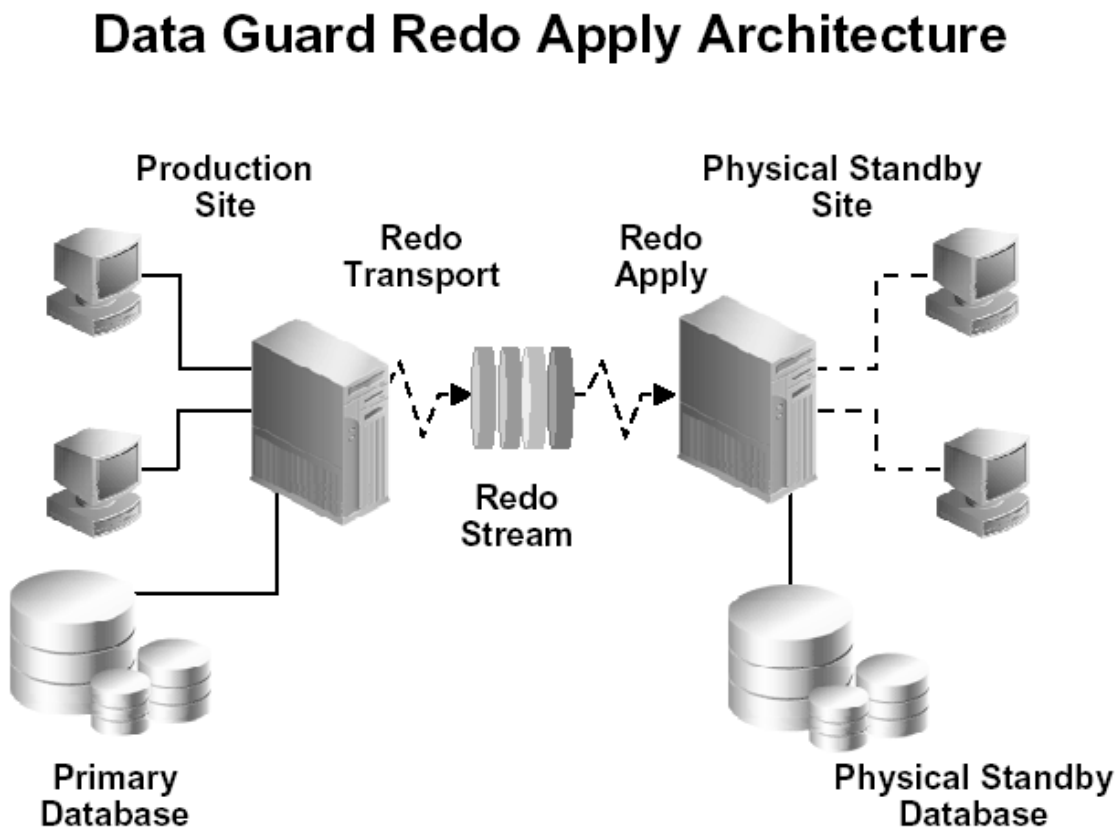
- **Proven and robust apply mechanism**.

- **Support for all DDL and DML** (with no restrictions of data types such as LONG, LONG RAW, ROWID, UROWID) and Table Types (Nested Tables and VARRAYS). Note: These data types and table types are not supported in the SQL Apply architecture.

- **Performance:** The Redo Apply technology applies changes using low-level recovery mechanisms, which bypass all SQL level code layers and therefore is the most efficient mechanism for applying changes. This makes the Redo Apply a highly efficient mechanism to propagate changes between databases.

- Oracle Data Guard also offers the flexibility to enable the physical standby database switch between recovery and read-only modes. E.g. running the database in recovery mode, then opening in read-only mode

to run reports, and then returning to recovery mode to apply outstanding redo data.



An important consideration while implementing the standby database is the **data protection mode**.

Currently, Oracle Data Guard provides three modes for data protection.

Protection Mode	Risk of Data Loss	Redo Shipment Mode by Log Writer Process	Comments
Maximum Protection	Zero data loss	Synchronous	Primary stops processing if standby unavailable
Maximum Availability	Zero data loss	Synchronous	Primary stops processing if standby unavailable
Maximum	Minimal Data Loss	Asynchronous	Least impact on

Performance (Default)	(usually zero to few seconds)		performance of primary database.

STO IT will select the **maximum performance data protection mode** as DMS is not a highly transaction based system.

At the Primary site, the following tasks are required:

- Setup the database in archive log mode.
- Setup the database in the Oracle Enterprise Manager
- Setup parameters necessary for physical standby database (example: COMPATIBLE,REMOTE_PASSWORD_FILE, STANDBY_FILE_MANAGEMENT etc.)
- Backup initialization file(s) and database files (RMAN)
- Backup DMS-related programs and files (all files under [redacted] on the Application Server)
- Document the locations and special settings of DMS-related programs and files, services and subsystems, as well as the Operating System.

Setup the Data Guard configuration and identify the standby database; file locations for the data files and control files.

At the Standby site, the following tasks are required:

- Using the documented configuration from the Production Site, install and configure:
  - The supporting Operating System, services and subsystems, including matching service patches
  - Application and Database servers
  - DMS-related programs and files, insuring the locations correspond to the ones defined at the Production site.
- Establish monitoring scripts using the inherent OEM Data Guard tools.(See examples in Section 9. Test Plans)
- Restore data files and standby control files (RMAN)
- Modify init.ora files
- Mount the Standby Database using the *standby controlfile*
- Initiate the Standby Database in recovery mode.

6. DMS Disaster Recovery Maintenance

→ Supporting Operating System and Servers Maintenance

Any upgrades, patches and new versions of the Operating System and Servers applied to the Production servers must be also applied to the Standby server, in order to keep them consistent, as well as fully compatible and operational. A full hot Backup of the database must be taken before performing any such upgrade.

When changes are done at the Production Site, these need to be fully documented, and then promptly reproduced and applied to the Standby Site.

→ DMS Data Maintenance

After the Standby Database is created, it needs to be in recovery mode and continuously, applying archives to ensure changes from the Production are propagated to the Standby.

Standby database maintenance should be automatic, so that propagation occurs quickly thus ensuring that the Standby is very current with the Production. How closely the Standby concurs

with the Production Database depends on how quickly/often changes are propagated to the Standby, to meet STO's service level requirements (MTTR).

For example, if STO's MTTR is 48 hours, the configuration of the total times to log switch, archive a log, propagate a log, and recover needs to be set to less than 48 hours.

The maintenance cycle can be outlined as follows:

- Continue archiving to archive log files (Production Site)
- Monitor for any errors or NOLOGGING operations (Production Site)
- Transfer completed archive log files (from the Production to the Standby Site)
- Continue backing up the Production Database and shipping media to the Standby Site
- Continue applying archives to Standby Database
- Monitor for Standby Database status and errors

Maintaining a Standby Database imposes no overhead on the Production Database. Log files are normally created by the Production Database to recover from a system failure and no extra logging is done to maintain a Standby Database.

Any structural changes made in the Production database such as when new columns are added to tables or data types changes; then these changes must be manually made in the standby database as well.

→ DMS Application, Programs, Reports and Forms Maintenance

Any modifications, upgrades, and patches performed to the DMS application and programs at the Production servers, must be also applied to the Standby server, in order to maintain system consistency and integrity.

These changes need to be fully documented, and then promptly reproduced and applied to the Standby Site. To accomplish this task, the following approaches exist:

- Fully automated scripts, that transfer the appropriated files and programs Over-the-Wire, from the Production to the Standby server
- On-site installation, where the physical media is sent to the Standby Site and installed locally to the server.

The automated scripts method works best if the DMS application is constantly being updated, since the update scripts can be set to run and apply changes as often as required.

As a general rule for major upgrades and updates, a local (on-site) installation at the Standby Site is always preferred, in place of *Remote* or *Over-the-Wire* installs; this practice works best to eliminate or minimize errors.

[redacted]

7. DMS Disaster Recovery Operation

The Standby Site should necessarily be activated in case of a Disaster.

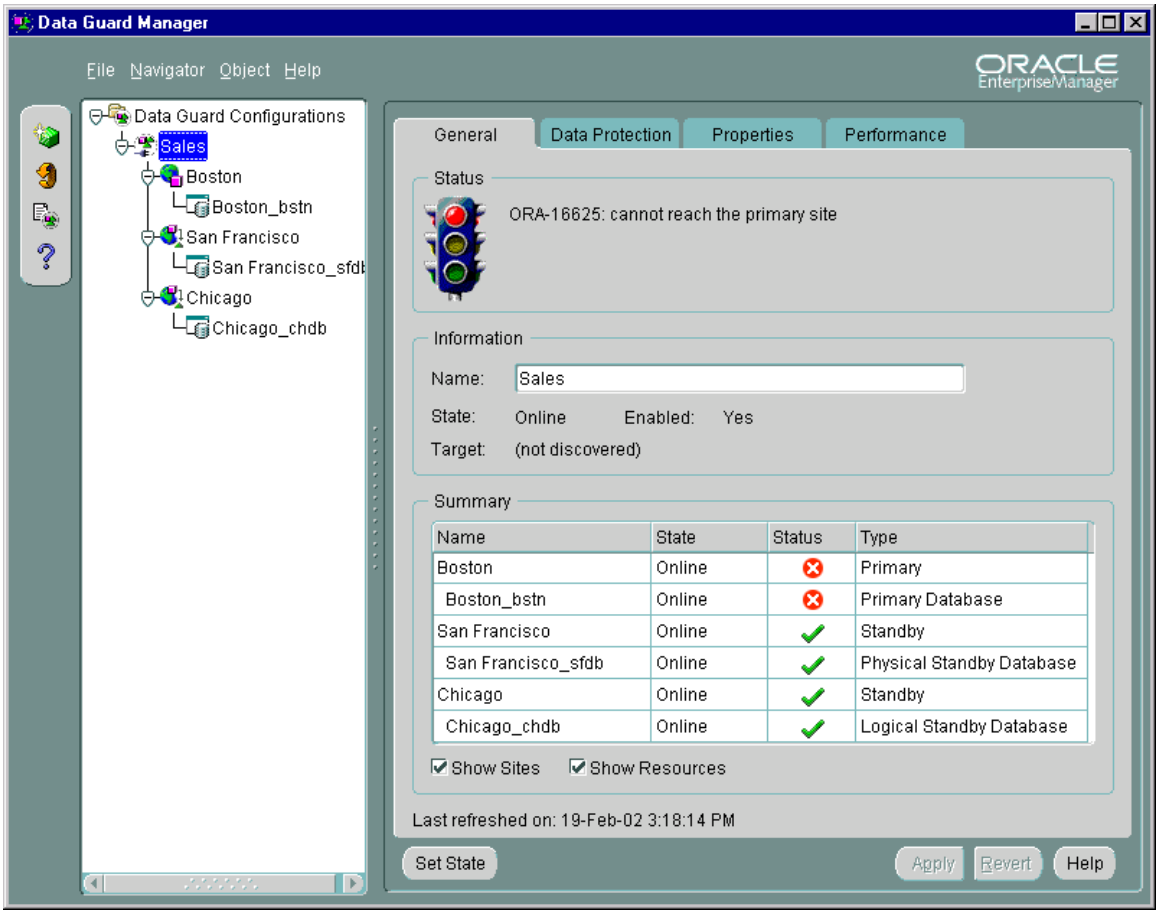
While the Standby site could also be used to temporarily service the users in case of a planned outage of the Production Site (e.g. major software or hardware upgrade needing to get the Production Site off-line), this document will not cover that switch-over option.

The following steps are required to activate the Standby Site:

- Assuming the Supporting Operating System and Servers have been properly updated and maintained, nothing needs to done.
- In the unlikely event that a few upgrades have not been applied according to the documentation from the Production Site, those must be applied prior to switching operations to the Standby Site
- The above statements apply for the DMS Application, Programs, Reports and Forms
- At this point, the Standby Database can be configured to act as the New Production Database and start servicing requests at the Standby Site. The Oracle Data Guard "fail over" functionality can be used to activate the standby database. Data Guard supports a graceful as well as a forced switch over. A graceful fail over is generally recommended as it attempts to minimize the data loss by finishing the application of unapplied logs. A forced fail over is fast compared to the graceful method but makes no attempt to finish applying of the logs.
- Finally, the DMS users can be switched to run the DMS application from the Standby Site (using the New Production Database). This task could be accomplished by either:
    - Instructing the users to re-point their applications to the new server, located at the Standby Site. While this is a faster approach, its implementation needs some end-user interaction; or
    - Replacing the servers' IP address of the Production Site (now defunct and unavailable) with the server's IP of the Standby Site (now providing the Production Database) via DNS updates. This method requires no end-user interaction, but may be slower due to DNS propagation

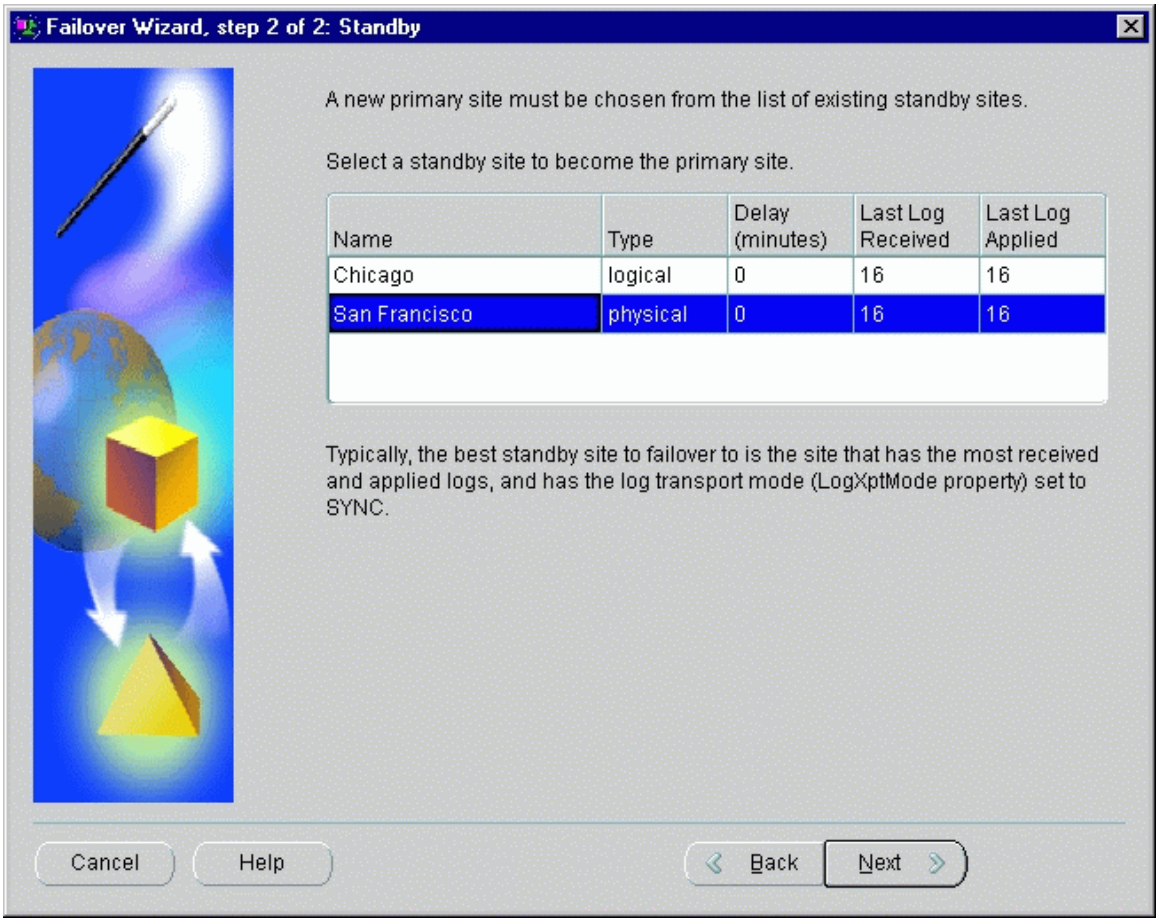
The following screen-shots illustrate how the "fail-over" functionality is performed from the OEM Data Guard once the physical standby configuration has been created.

The screen-shot below indicates that there is a problem with the Primary Database as there is a red cross sign next to the Status column and the primary site cannot be reached.

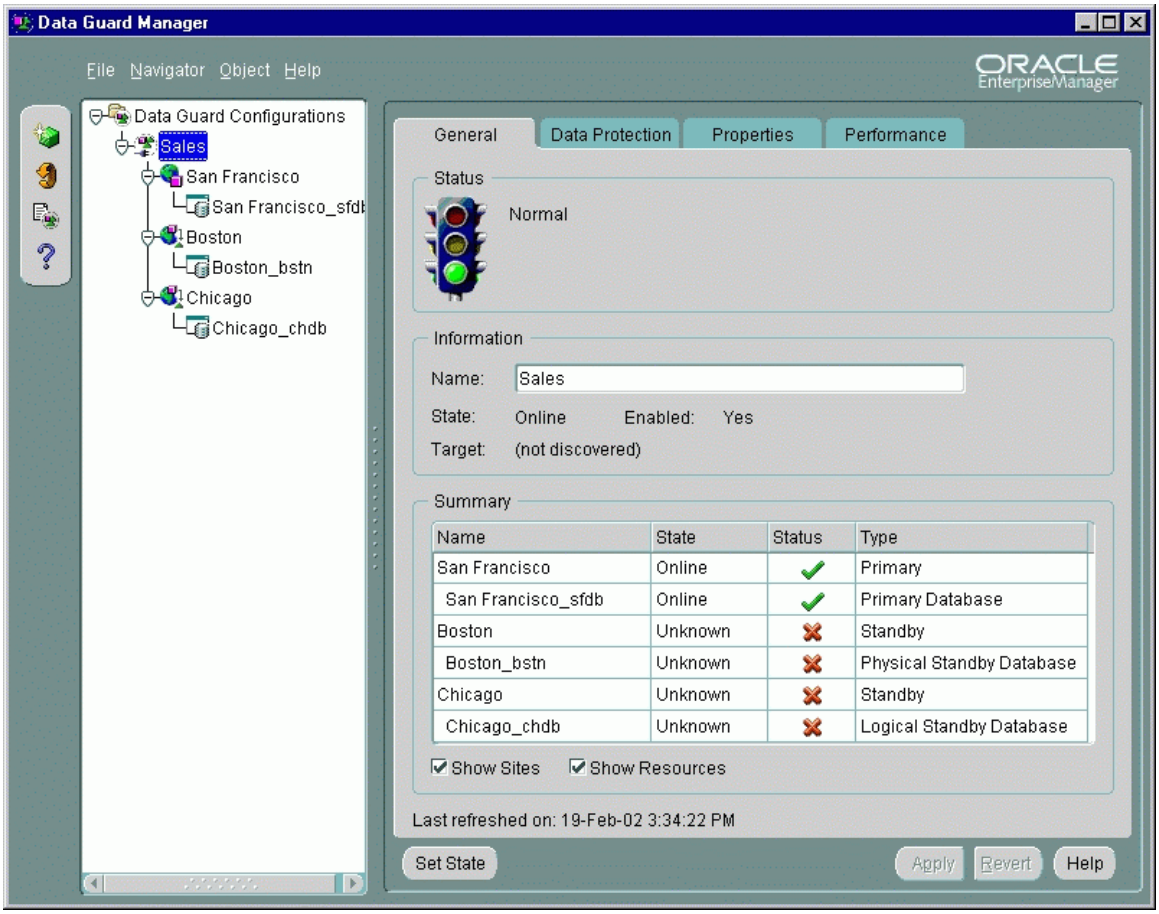


If you determine that a failure has occurred on the primary database and there is no possibility of recovering the primary database in a timely manner, you can start the Failover wizard by selecting **Failover** on the Object menu.

The following screen shows the list of available standby sites and the DBA will have to select the standby site which will become the new primary site.



During the failover operation, the wizard opens a window to display the progress of the operation as it transitions the selected standby site into the primary role and restarts all online physical standby database instances involved in the failover operation. When completed, the configuration General page reflects the updated configuration with the new primary site taking over. (Note : the standby database is displayed as Primary and the earlier Primary database is displayed as standby and its status is unknown.



NOTES:

When a RESETLOGS operation occurs, the Primary and Standby Databases are no longer compatible. Previous redo is invalidated and cannot be applied. A new Standby Database (or the original Production Database) needs to be re-built as soon as possible.

Only new data will be entered to the New Production Database at the Standby Site, using the DMS applications and programs.

In general, NO modifications to the Operating System or the DMS application should be allowed during the emergency-mode operation at the Standby Site; if an update is absolutely required for the proper operation of the Standby server, this has to be fully documented for future deployment, once the Original Production Site is reactivated.

To improve Standby Site survivability, implement regular backups, following the techniques used at the Original Production Site. Store the media at another location.

It will be the STO IT DBA task to do database backups or to perform a manual switchover from the primary to the secondary site in case of a disaster. Network Support will be needed in case there is a problem in the WAN/LAN communication links.

8. Return to Normal Operations

Reconditioning of the original Production Site and servers must commence as soon as the site and resources become available and are secure. Proper WAN connectivity is also required to adequately accomplish this task.

If the Original Production Site was lost due to a LAN/WAN link failure:

- Test connectivity to the Standby Site thoroughly using terminal services or using the Oracle OEM Data Guard Switchover functionality.
- Insure that any modifications applied to the Operating System, services and servers during the interim operation, are replicated to the Original Production servers
- Same as above applies for the DMS application, programs and files

If any of the servers at the Original Production site were lost due to hardware failure(s):

- Rebuild the failed hardware, according to the documented configuration
- Install and configure the Operating System, patches, servers, and services, as well as the DMS applications, programs, files, etc. as detailed in the documentation
- Test proper connectivity to the Standby Site

Synchronize the DMS data, from the Standby to the Original Production Site:

- A full hot or cold database (control files, database files, init.ora) backup of the Production Database (located at the Standby Site) needs to be shipped to the Original Production Site
- The Database server, located at the Original Production Site needs to be configured in Standby Database mode, as documented previously
- Backed up DMS data from the Standby Site needs to be loaded at the Production Site
- Activate the changes and run the Production Site's Database server in Standby-mode, allowing the Standby Site to send updates
- Plan for a DMS service outage (during a weekend or after-hours, if possible)
- Perform a Controlled Switchover, turning the Production Site's database as the current Production Database, effectively switching the Standby Site's database to Standby mode
- Redirect the users/clients to the recently re-enabled Production Site, using either the manual or DNS-supported schema

To Controlled Switchover:

- Standby Site: The Production Database must be properly SHUTDOWN
- Production Site: The Standby Database is updated with all the archived logs and SHUTDOWN NORMAL
- Standby Site: Online Redo Logs are sent to the Standby Site
- Production Site: A new *controlfile* is created; the Database is restarted, running now as the Production database
- Standby Site: A new *controlfile* is created, enabling the database in Standby mode operation. Then the database is mounted, effectively running in Standby mode, accepting updates and logs from the Production Site's Database.

Upon completion of the above procedures, the Production Site hosts again the Production Database, while the Standby database resides at the Standby Site, and the DMS application is back to its normal mode of operation and performance.

New DMS Database and Application Server Configuration in case of a Disaster:

In case, a new database server needs to be configured; then the following steps need to be followed to setup the DMS Application:

- Install the [redacted] Oracle Database on the new Database Server.
- Generate the DMS Application from the Oracle Designer Repository or last backup.
    - [redacted]

- [redacted]

- This will generate the database objects (tables, views, indexes, packages and other DMS database objects) as well as the application modules in terms of the forms, reports and libraries.
  The database objects from the Designer Repository need to be created in the new database created.
- Restore the data from the last export or any cold / hot backup performed.
- Setup the Batch Jobs on the Oracle OEM.

In case, a new application server needs to be configured; then the following steps need to be followed to setup the DMS Application:

- Install the [redacted] on the new Application Server.
- Create a folder [redacted].
- Create sub-folders called Help, Template, Reports
- Copy the forms (.fmx), reports (.rep) and libraries (.pll) from the Oracle Designer Repository to a folder [redacted]
- Copy the Online Help Files to the Help folder.
- Copy the Template Files for Reports under the Template Folder.
- The Reports Folder is designated for run time reports.

9. Test Plans

When the Disaster Recovery Server is configured; then the following tests should be performed:

- Before shipping the server to [redacted]
  - Test that the archive redo logs are transferred from the primary to the secondary. [redacted])
  - Test that the Failover and Switchover activities function correctly using the configuration set in the OEM Data Guard.
  - Ship the server to Los Angeles and setup the server with the pre-assigned IP Address.

- After shipping the server [redacted]
  - Test that the archive redo logs are transferred from the primary to the secondary. [redacted]
  - Test that the Failover and Switchover activities function correctly using the configuration set in the OEM Data Guard.

The Test Application is a good way to make sure that the configuration is set up and functioning properly before using live data and to test relative performance.

Running the Test Application

You use the Test Application dialog to help you evaluate the performance of your broker configuration by adding and deleting rows in a test schema (eg. [redacted]) on your primary database. To set up a Test Application, perform the following steps:

1. On the Performance Page, click **Options**.

2. Click **Start Test** and start a test on the primary database (the default). You can also select logical standby databases and physical standby databases that are in read-only mode.

3. Click **Setup** at the bottom of the page to create the test tables.

4. Choose **Single Update Mode** or **Continuous Update Mode**:

Single Update Mode

Single Update Mode inserts one row of the value you specify into the Test Application. To use Single Update Mode:

On the primary database:

5. Enter a value (using a VARCHAR datatype) in the text box under Single Update Mode.

6. Click **Apply**.

On the physical standby databases:

7. Set the state of the physical standby database to read-only mode.

8. Click **Options** on the Performance Page and start another Test Application for each physical standby database.

5. View the **Value** field in the Test Application to see the inserted value.

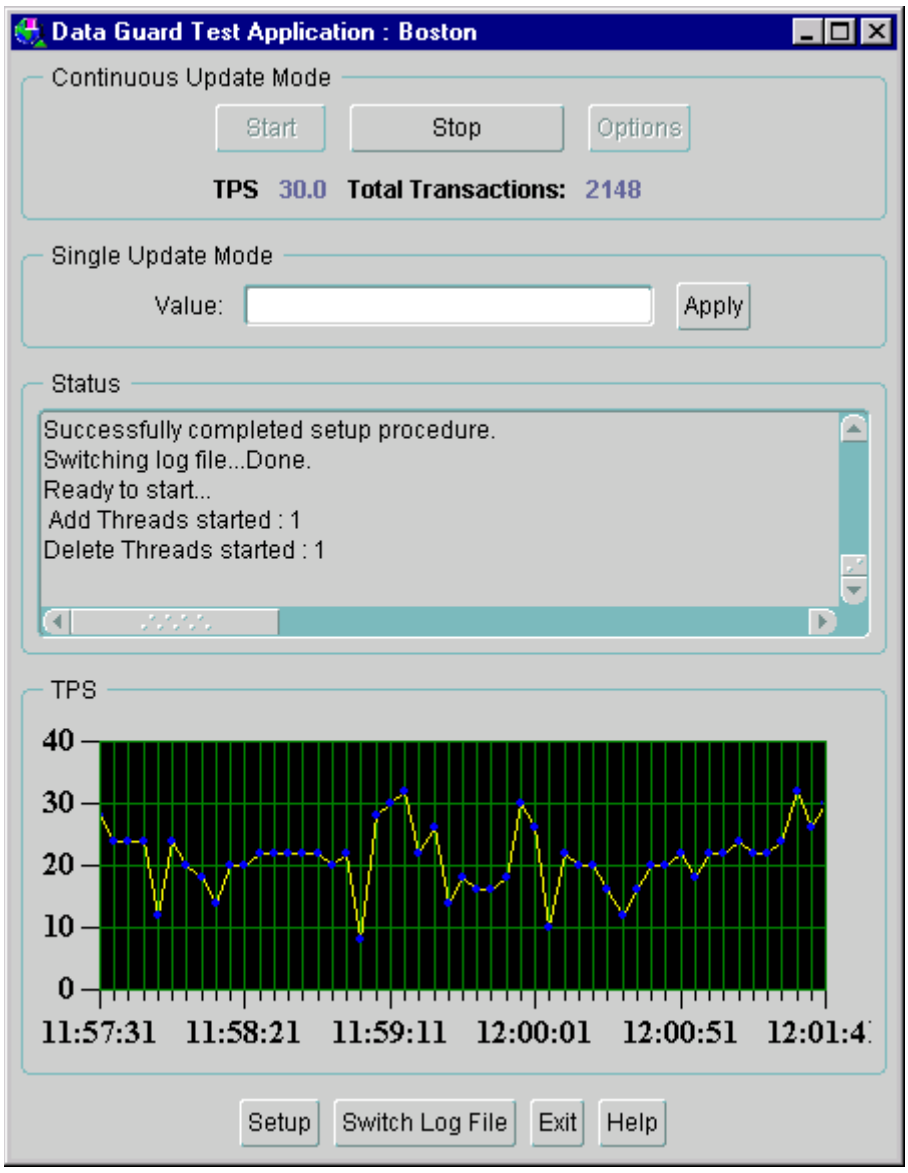
When the value from the primary database is inserted into the standby database, the value will appear in the Test Value text area of the Test Application started on the logical.

Continuous Update Mode

Continuous Update Mode inserts a number of insert and delete threads in the Test Application. To set it up, select **Options** in the Continuous Update Mode section of the Test Application page and enter the number of Insert and Delete threads.

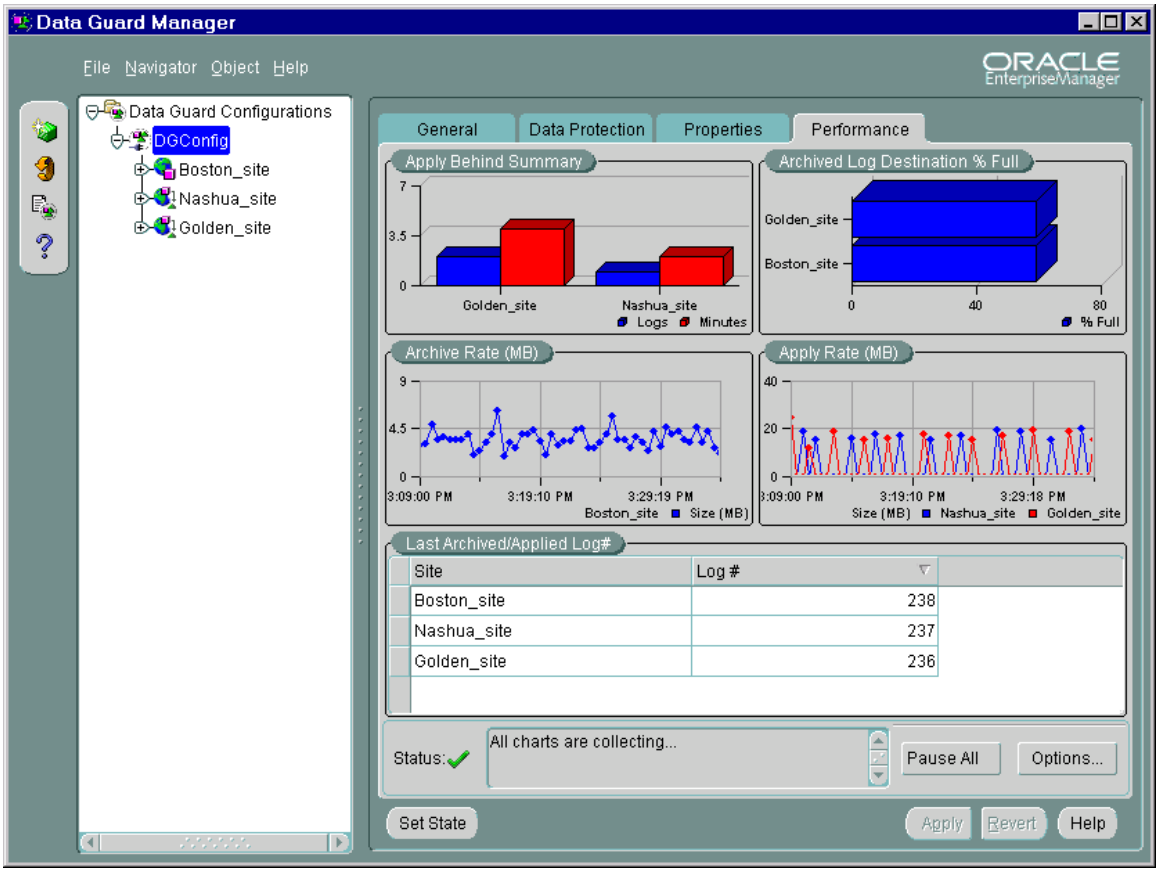
More threads will produce more transactions resulting in more log traffic. The Test Application will run until you click **Stop** or until there is a lack of resources. There are no restrictions on how many threads may be started and it is possible to exceed the hardware or database resource limits (which can also be a very useful test).

The figure below shows the Test Application dialog for setting up single or continuous update mode tests.



STO IT must plan to test the Disaster Recovery Configuration (planned switch-over from primary to secondary) as part of the preventive maintenance plan. This should be performed using the OEM Data Guard at least once in two weeks (or as per the Enterprise Disaster Recovery Plan for STO) to ensure that the archived redo logs are getting shipped and applied correctly.

For more in-depth performance and monitoring, you can display detailed performance statistics for a broker configuration using performance charts that provide a graphical summary of all redo log activity in the configuration. The charts are refreshed based on a collection interval (the rate at which data is sampled from the primary database) that you can specify.



10. Vendor Support

The following table lists all vendors who can be contacted in case software licenses/upgrades are needed in case of a disaster.

Software/ Hardware	Vendor	Contact Person/Address	Phone #
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]

11. Technical References

[redacted]