Capgemini

Oracle 11g DBA Fundamentals Overview

Lesson 13: Backup and Recovery Concepts

Objectives

After completing this you should be able to do the following:

- Describe the basics of database backup, restore and recovery.
- List the types of failure that may occur in an Oracle Database.
- Describe ways to tune instance recovery.
- Identify the importance of checkpoints, redo log files, and archived log files.

Backup and Recovery Issues

The administrator’s duty is to:

- Protect the database from failure wherever possible.
- Increase the Mean-Time-Between-Failures (MTBF).
- Decrease the Mean-Time-To-Recover (MTTR).
- Minimize the loss of data.

Categories of Failures

Failures can generally be divided into the following categories:

- Statement failure
- User process failure
- Network failure
- User error
- Instance failure
- Media failure

Statement Failures

Typical Problems	Possible Solutions
Attempts to enter invalid data into a table	Work with users to validate and correct data.
Attempts to perform operations with insufficient privileges	Provide appropriate object or system privileges.
Attempts to allocate space that fail	Enable resumable space allocation. Increase user quota. Add space to tablespace.
Logic errors in applications	Work with developers to correct program errors.

User Process Failure

Typical Problems	Possible Solutions
User performed an abnormal disconnect.	DBA action is not usually needed to resolve user process failures. Instance background processes roll back uncommitted changes and release locks. Watch for trends.
User's session was abnormally terminated.	
User experienced a program error which terminated the session.	

Network Failure

Typical Problems	Possible Solutions
Listener fails	Configure a backup listener and connect-time failover.
Network Interface Card (NIC) fails	Configure multiple network cards.
Network connection fails	Configure a backup network connection.

User Errors

Typical Causes	Possible Solutions
User inadvertently deletes or modifies data.	Roll back or use flashback query to recover.
User drops a table.	Recover table from recycle bin.

Instance Failure

Typical Causes	Possible Solutions
Power outage	Restart the instance using the "startup" command. Recovery from instance failure is automatic including rolling forward changes in the redo logs and then rolling back any uncommitted transactions. Investigate causes of failure using the alert log, trace files, and Enterprise Manager.
Hardware failure	
Failure of one of the background processes	
Emergency shutdown procedures	

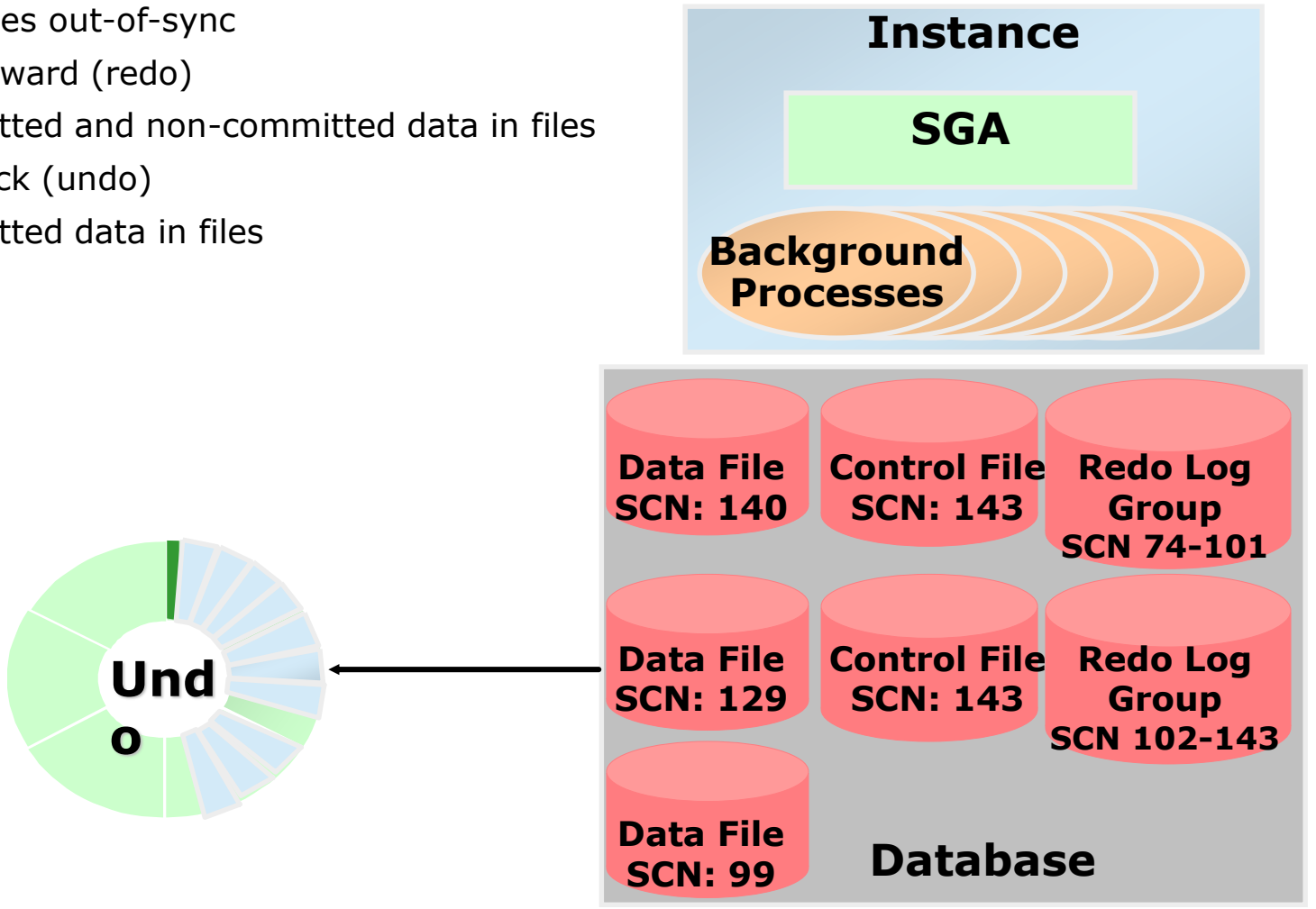
Instance Recovery

Instance or crash recovery:

- Is caused by attempts to open a database whose files were not synchronized on shutdown
- Is automatic
- Uses information stored in redo log groups to synchronize files
- Involves two distinct operations
  - Rolling forward: Data files are restored to their state before the instance failed.
  - Rolling back: Changes made but not committed are returned to their original state.

Phases of Instance Recovery

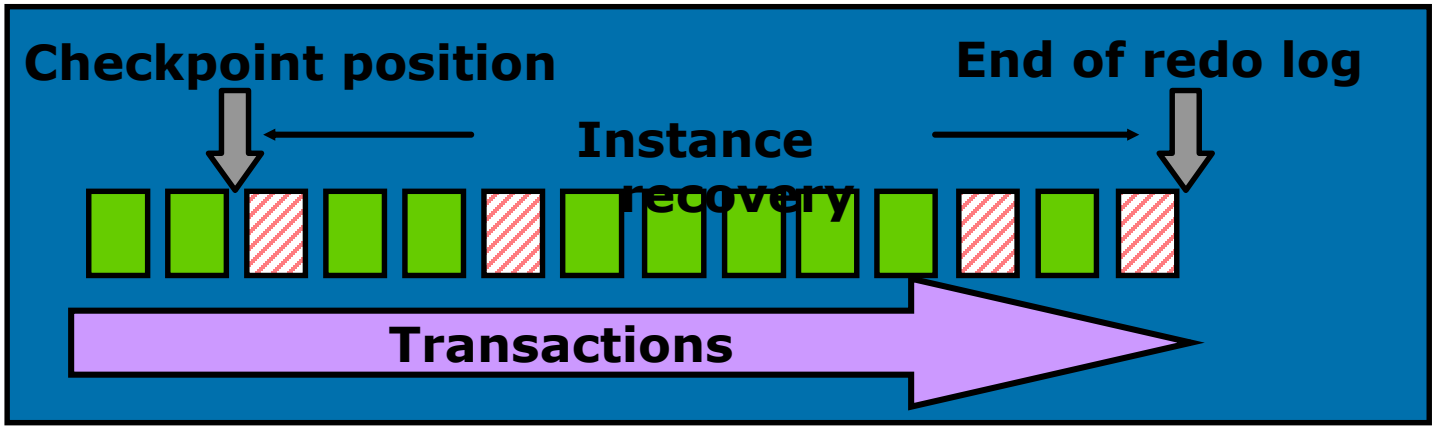
1. Data files out-of-sync
2. Roll forward (redo)
3. Committed and non-committed data in files
4. Roll back (undo)
5. Committed data in files



Tuning Instance Recovery

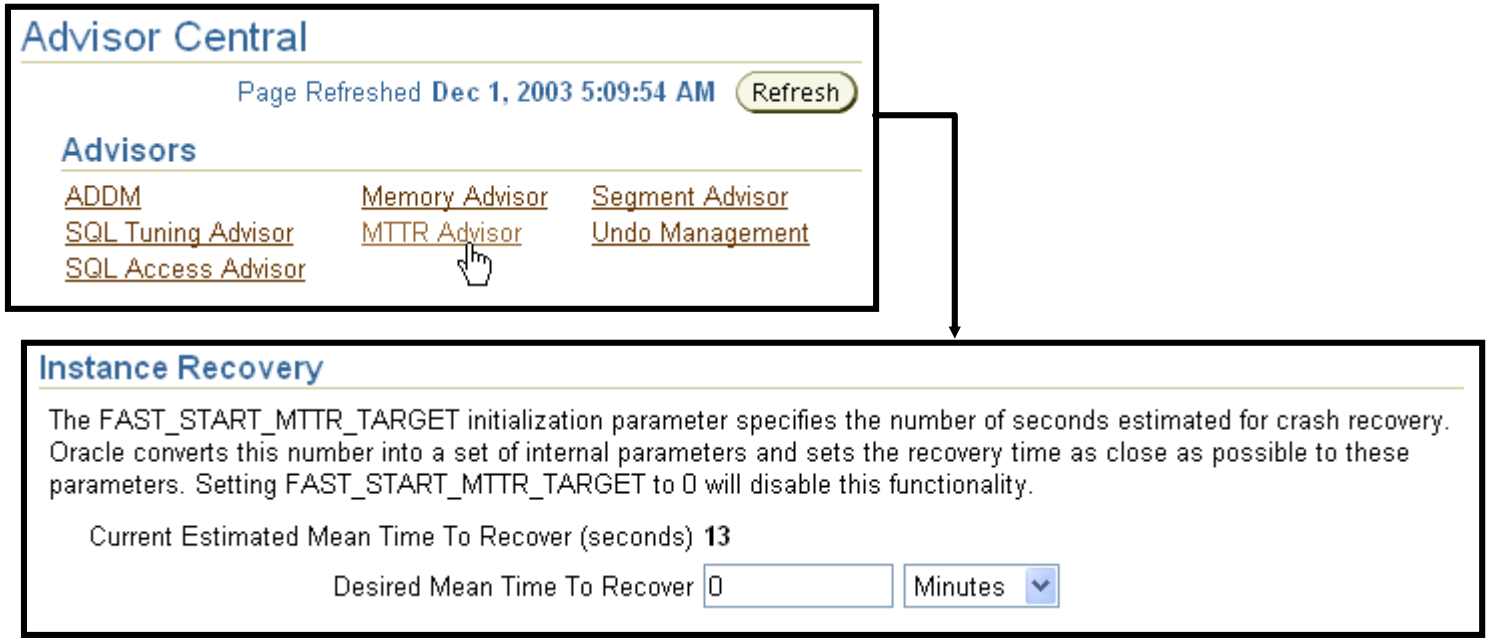
During instance recovery the transactions between the checkpoint position and end of redo log must be applied to the data files.

Tune instance recovery by controlling the difference between the checkpoint position and end of redo log.



Using the MTTR Advisor

- Specify the desired time in seconds or minutes.
- Default value is 0 (disabled).
- Maximum value is 3600 seconds (one hour).



Media Failure

Typical Causes	Possible Solutions
Failure of disk drive	1. Restore the affected file from backup. 2. If necessary, inform the database of a new file location. 3. If necessary, recover the file by applying redo information.
Failure of disk controller	
Deletion or corruption of database file	

Configuring for Recoverability

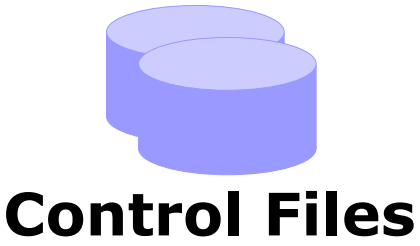
To configure your database for maximum recoverability:

- Schedule regular backups
- Multiplex control files
- Multiplex redo log groups
- Retain archived copies of redo logs

Control Files

Protect against database failure by multiplexing control files.

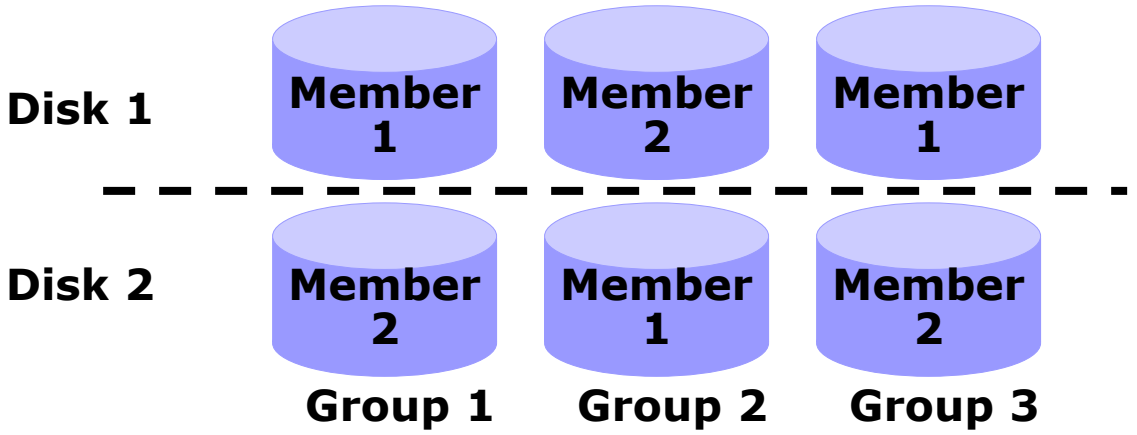
- At least two copies (Oracle suggests three)
- Each copy on a separate disk
- At least one copy on a separate disk controller



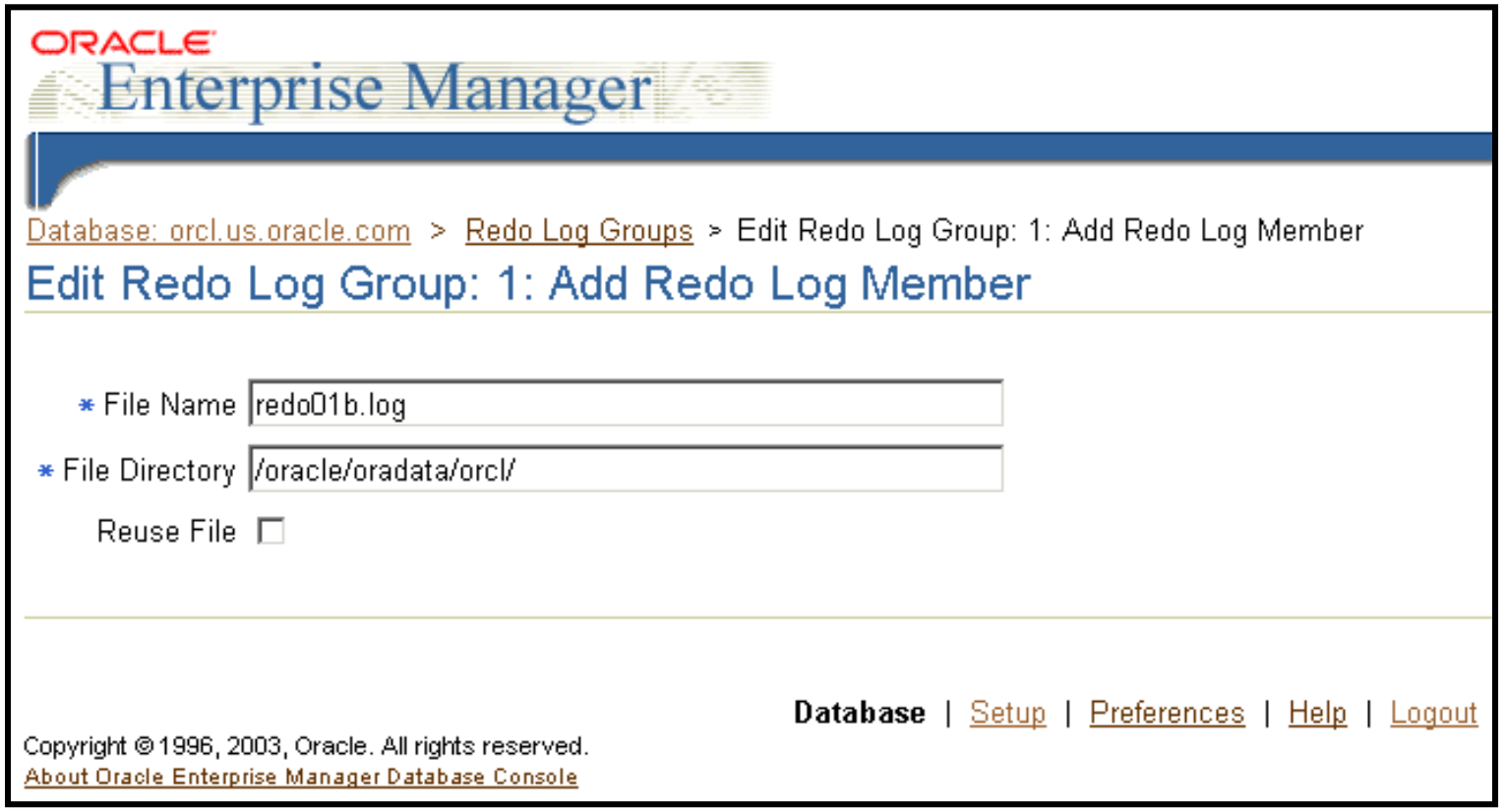
Redo Log Files

Multiplexing redo log groups to protect against media failure and loss of data.

- At least two members (files) per group
- Each member on a separate disk drive
- Each member on a separate disk controller
- Redo logs heavily influence performance



Multiplexing the Redo Log



Archived Log Files

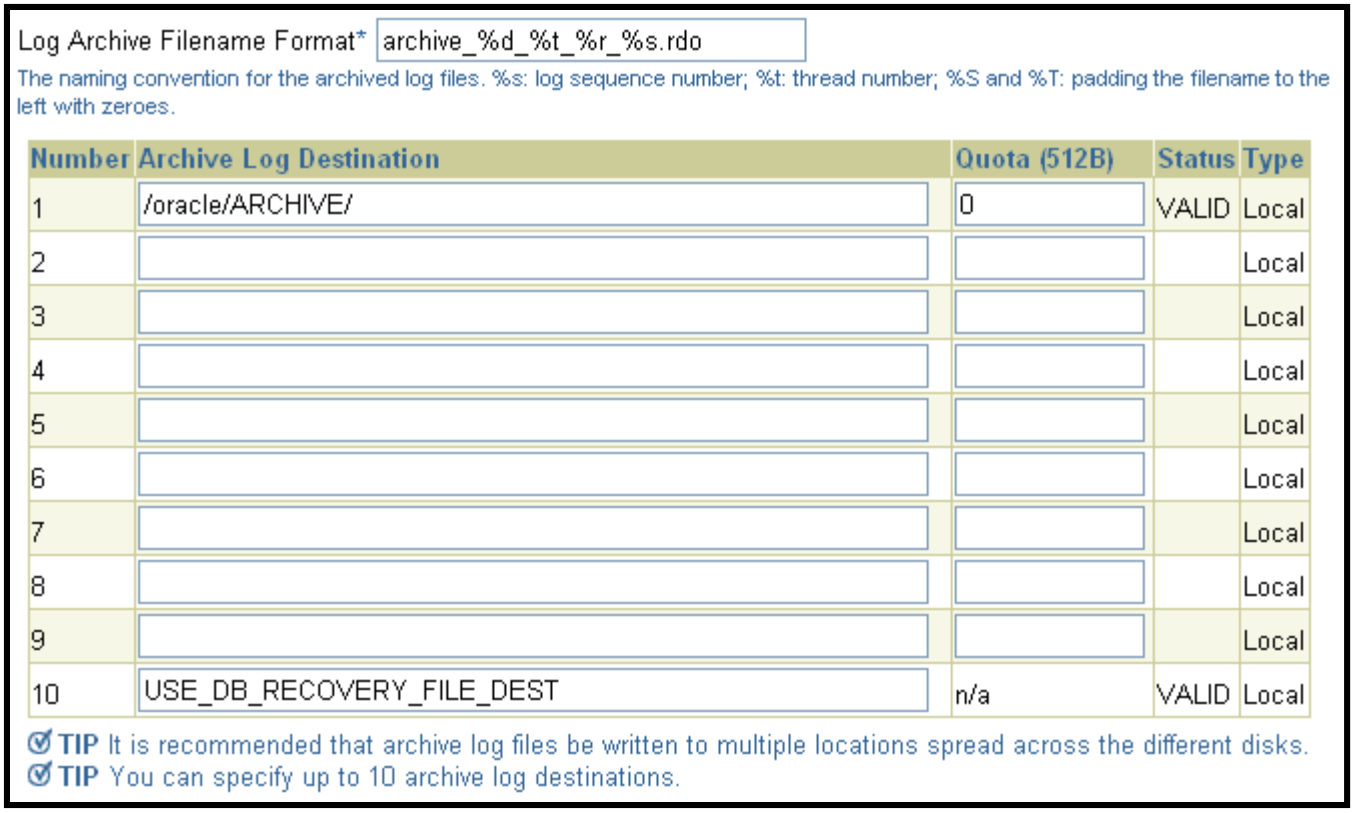
To preserve redo information, create archived copies of redo log files.

- Specify archived log file naming convention.
- Specify one or more locations to archive logs to.
- Switch the database to ARCHIVELOG mode.

- Online Redo Log Files
- Archived log files

Archive Log File Naming and Destinations

Specify archived log file name and destinations.



Log Archive Filename Format* archive_%d_%t_%r_%s.rdo

The naming convention for the archived log files. %s: log sequence number; %t: thread number; %S and %T: padding the filename to the left with zeroes.

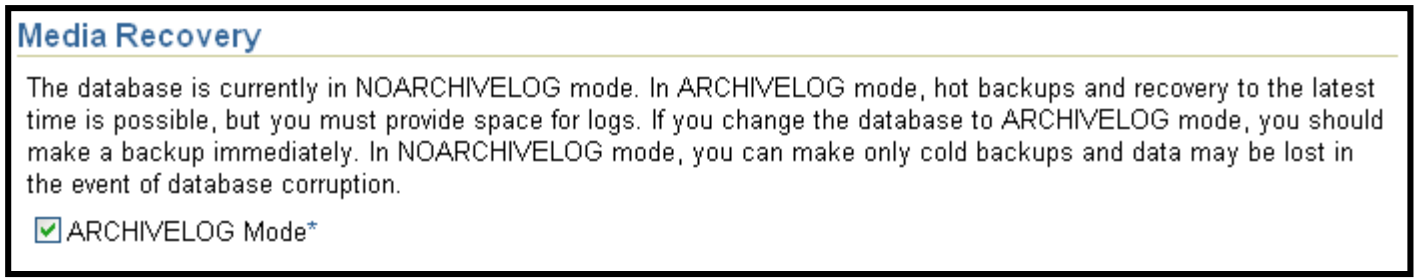
Number	Archive Log Destination	Quota (512B)	Status	Type
1	/oracle/ARCHIVE/	0	VALID	Local
2				Local
3				Local
4				Local
5				Local
6				Local
7				Local
8				Local
9				Local
10	USE_DB_RECOVERY_FILE_DEST	n/a	VALID	Local

TIP It is recommended that archive log files be written to multiple locations spread across the different disks.
TIP You can specify up to 10 archive log destinations.

ARCHIVELOG Mode

Place the database in ARCHIVELOG mode.

- Click the ARCHIVELOG Mode checkbox
- Click Apply. The database can only be set to ARCHIVELOG mode from the MOUNT state. Click Yes when asked if you want to restart the database.



SUMMARY

- In this lesson you should have learned how to:
  - Describe the basics of database backup, restore and recovery
  - List the types of failure that may occur in an Oracle Database
  - Identify the importance of checkpoints, redo log files, and archived log files
  - Configure ARCHIVELOG mode
  - Describe ways to tune instance recovery