14

Backup and Recovery Concepts

Objectives

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

- Identify 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 archive log files
- Configure `ARCHIVELOG` mode

Part of Your Job

The administrator's duties are 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 Failure

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 owner quota. • Add space to tablespace.
Logic errors in applications	Work with developers to correct program errors.

User Process Failure

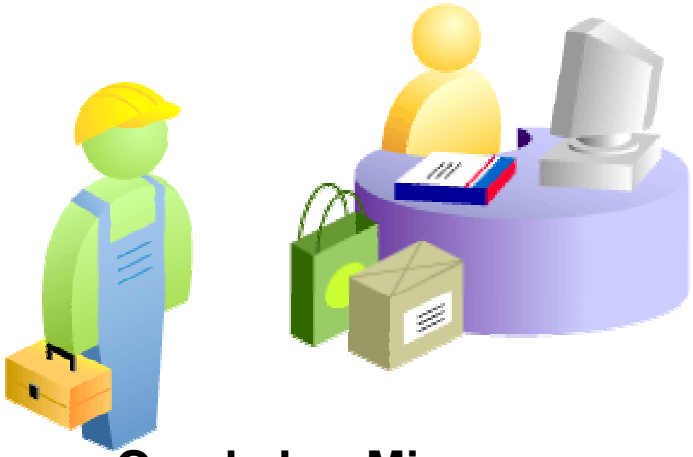
Typical Problems	Possible Solutions
A user performs an abnormal disconnect.	A DBA's action is not usually needed to resolve user process failures. Instance background processes roll back uncommitted changes and release locks.
A user's session is abnormally terminated.	
A user experiences a program error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

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 Error

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



Oracle LogMiner

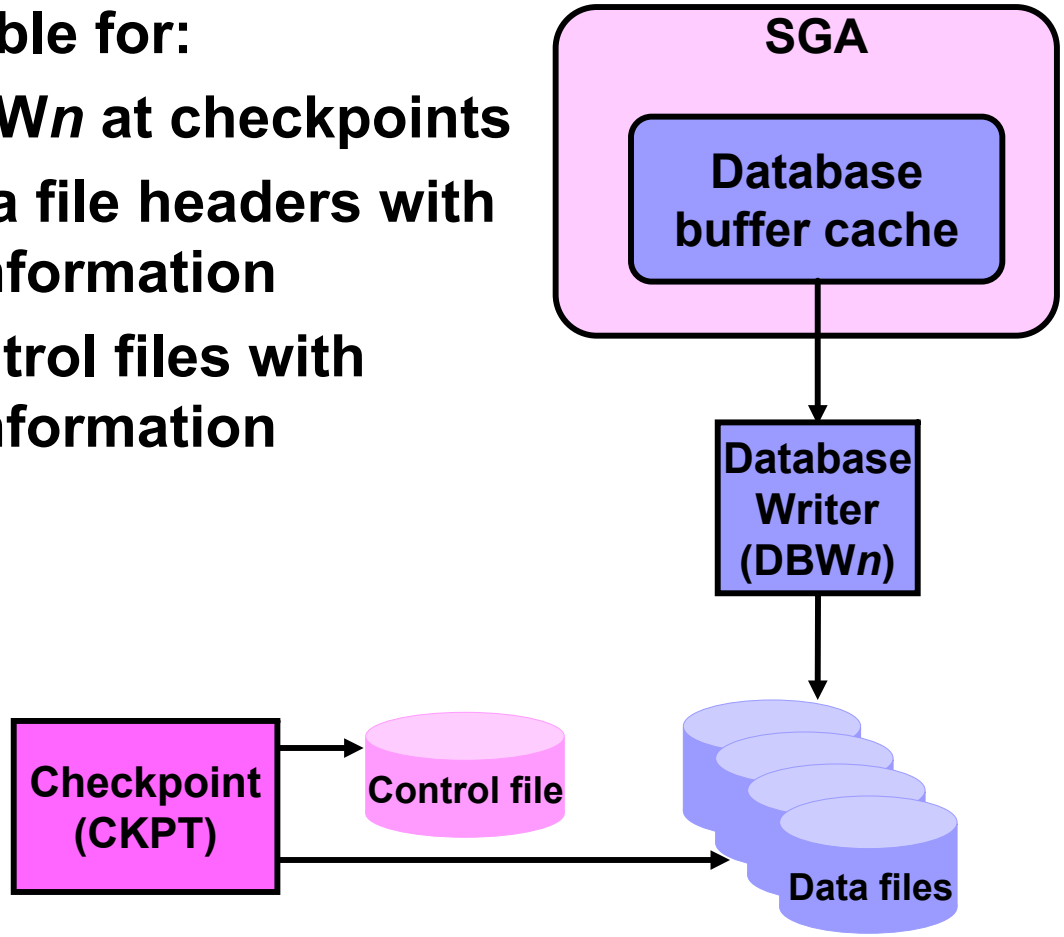
Instance Failure

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

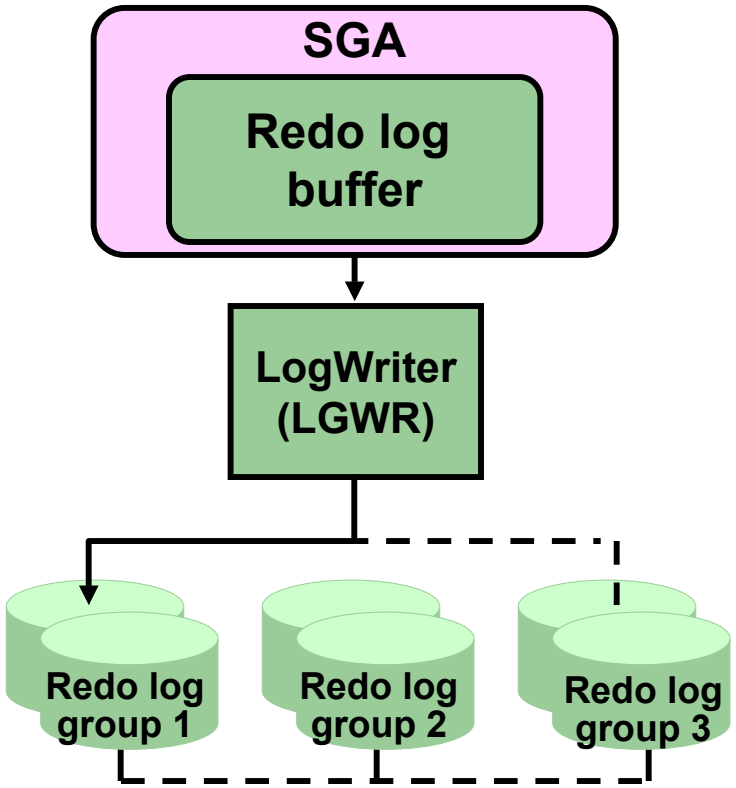
Background Processes and Recovery: Checkpoint (CKPT)

CKPT is responsible for:

- **Signaling DBW*n* at checkpoints**
- **Updating data file headers with checkpoint information**
- **Updating control files with checkpoint information**



Background Processes and Recovery: Redo Log Files and LogWriter



Redo log files:

- Record changes to the database
- Should be multiplexed to protect against loss

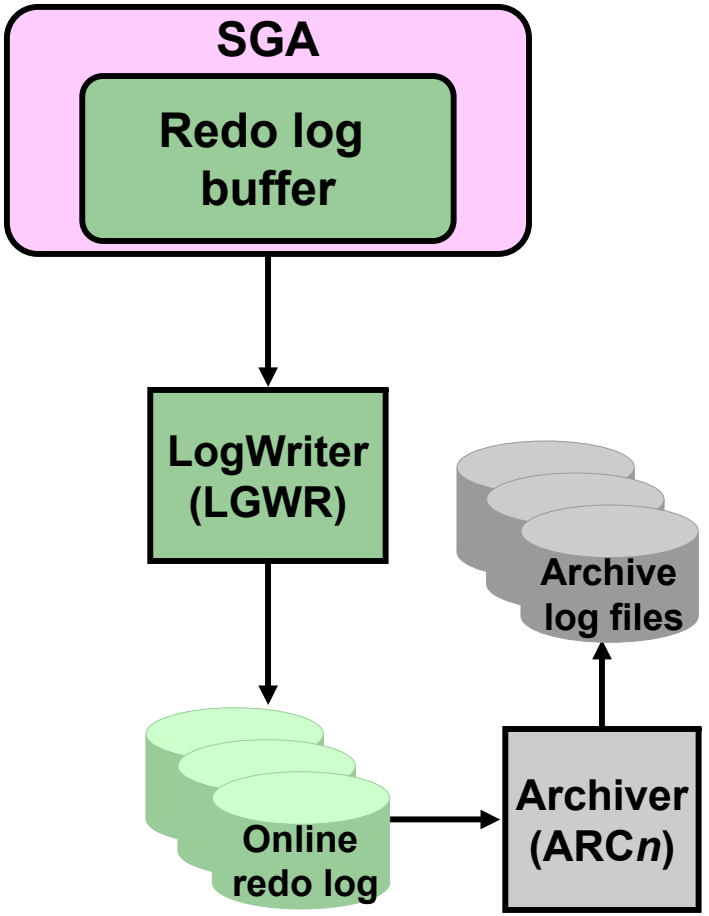
LogWriter writes:

- At commit
- When one-third full
- Every three seconds
- Before DBW*n* writes

Background Processes and Recovery: Archiver (ARC*n*)

Archiver (ARC*n*):

- **Is an optional background process**
- **Automatically archives online redo log files when `ARCHIVELOG` mode is set for the database**
- **Preserves the record of all changes made to the database**



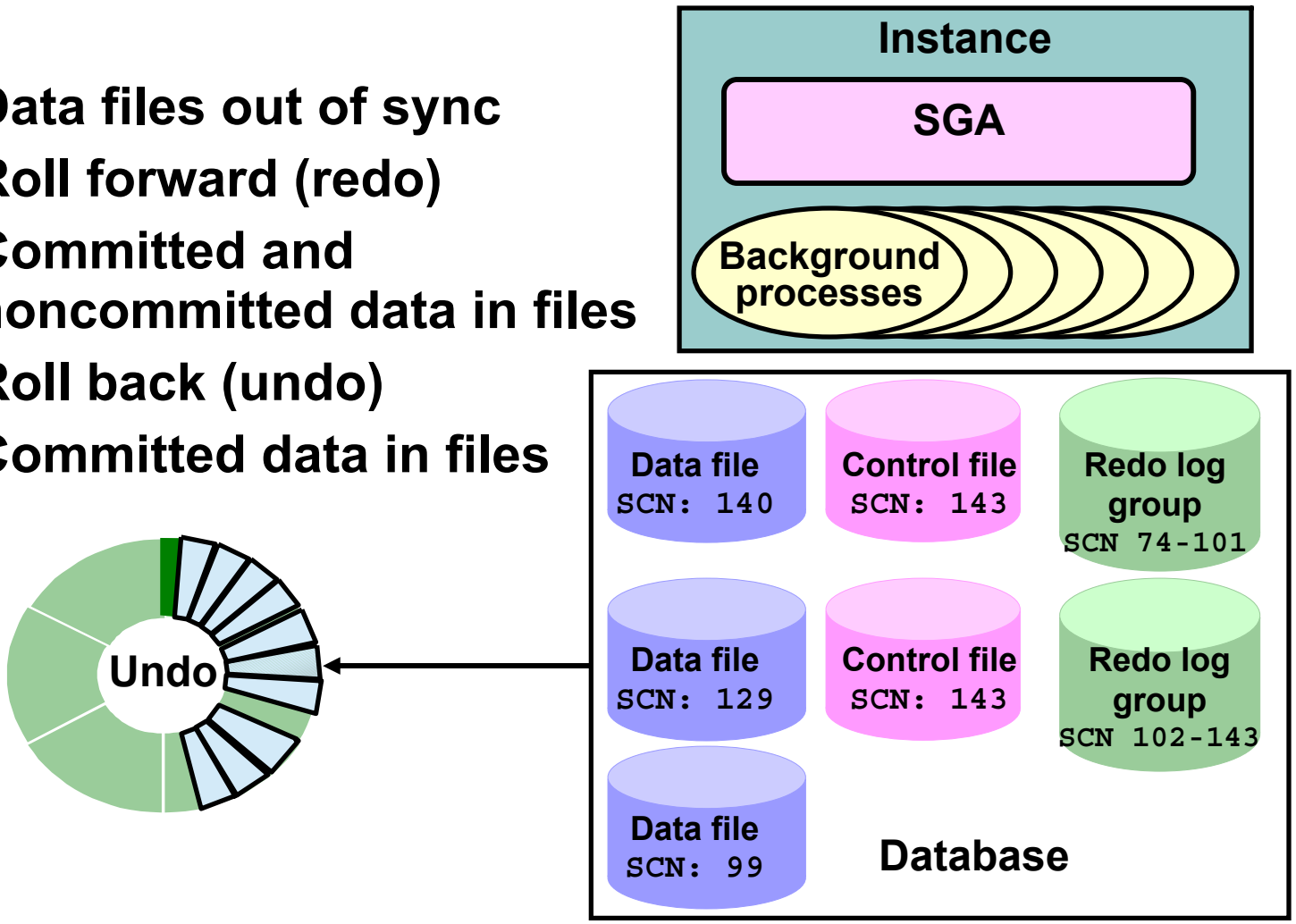
Instance Recovery

Instance or crash recovery:

- Is caused by attempts to open a database whose files are 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.

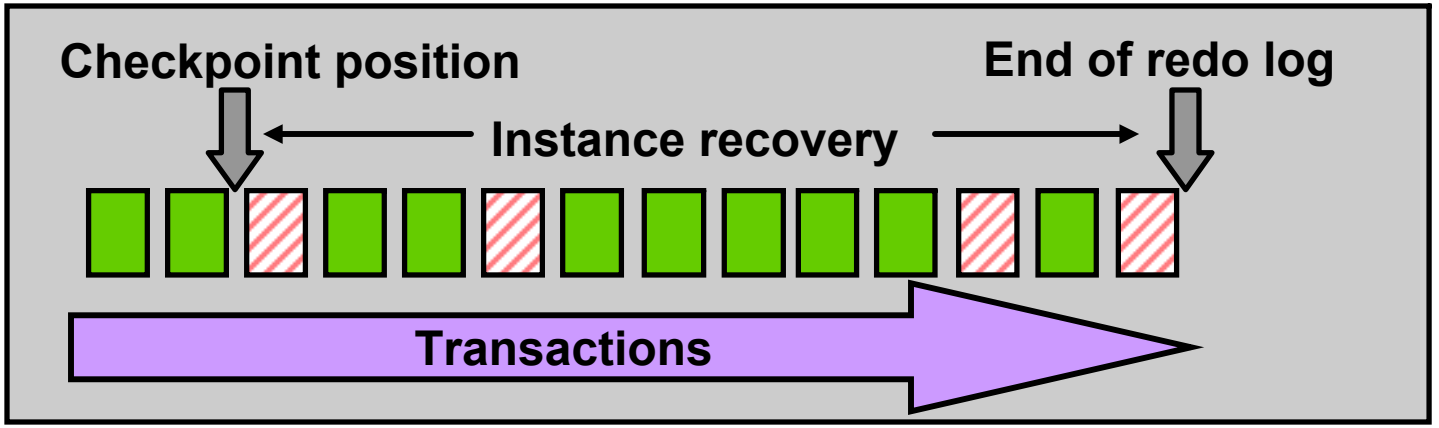
Phases of Instance Recovery

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



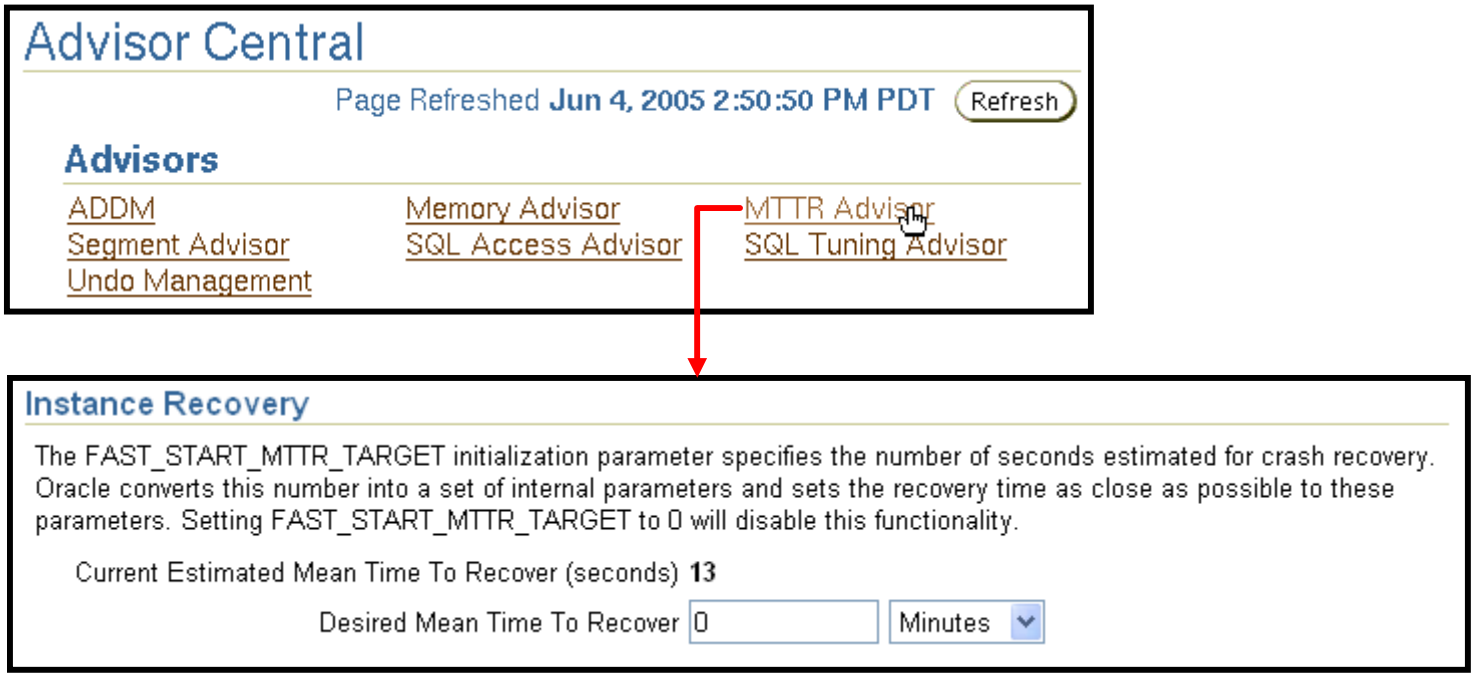
Tuning Instance Recovery

- During instance recovery, the transactions between the checkpoint position and the end of redo log must be applied to data files.
- You tune instance recovery by controlling the difference between the checkpoint position and the end of redo log.



Using the MTTR Advisor

- Specify the desired time in seconds or minutes.
- The default value is 0 (disabled).
- The maximum value is 3,600 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 about 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

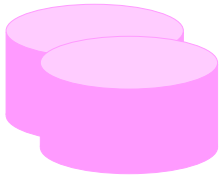
To configure your database for maximum recoverability, you must:

- 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. It is suggested that your database has:

- At least two copies (Oracle recommends three) of the control file
- Each copy on a separate disk
- At least one copy on a separate disk controller



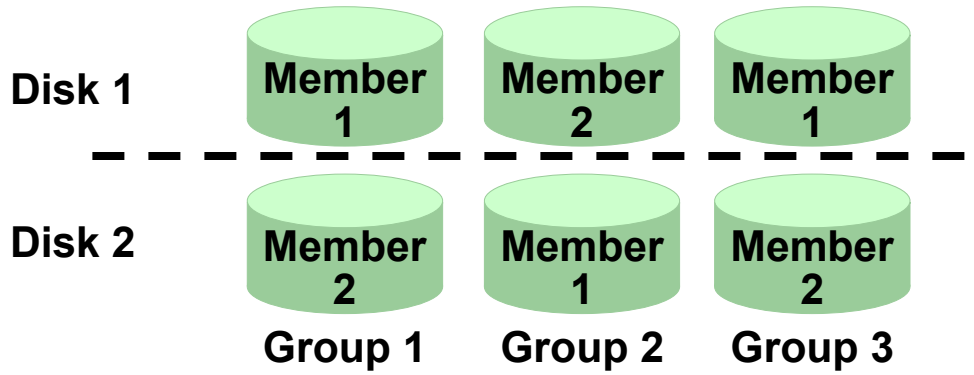
Control files

Redo Log Files

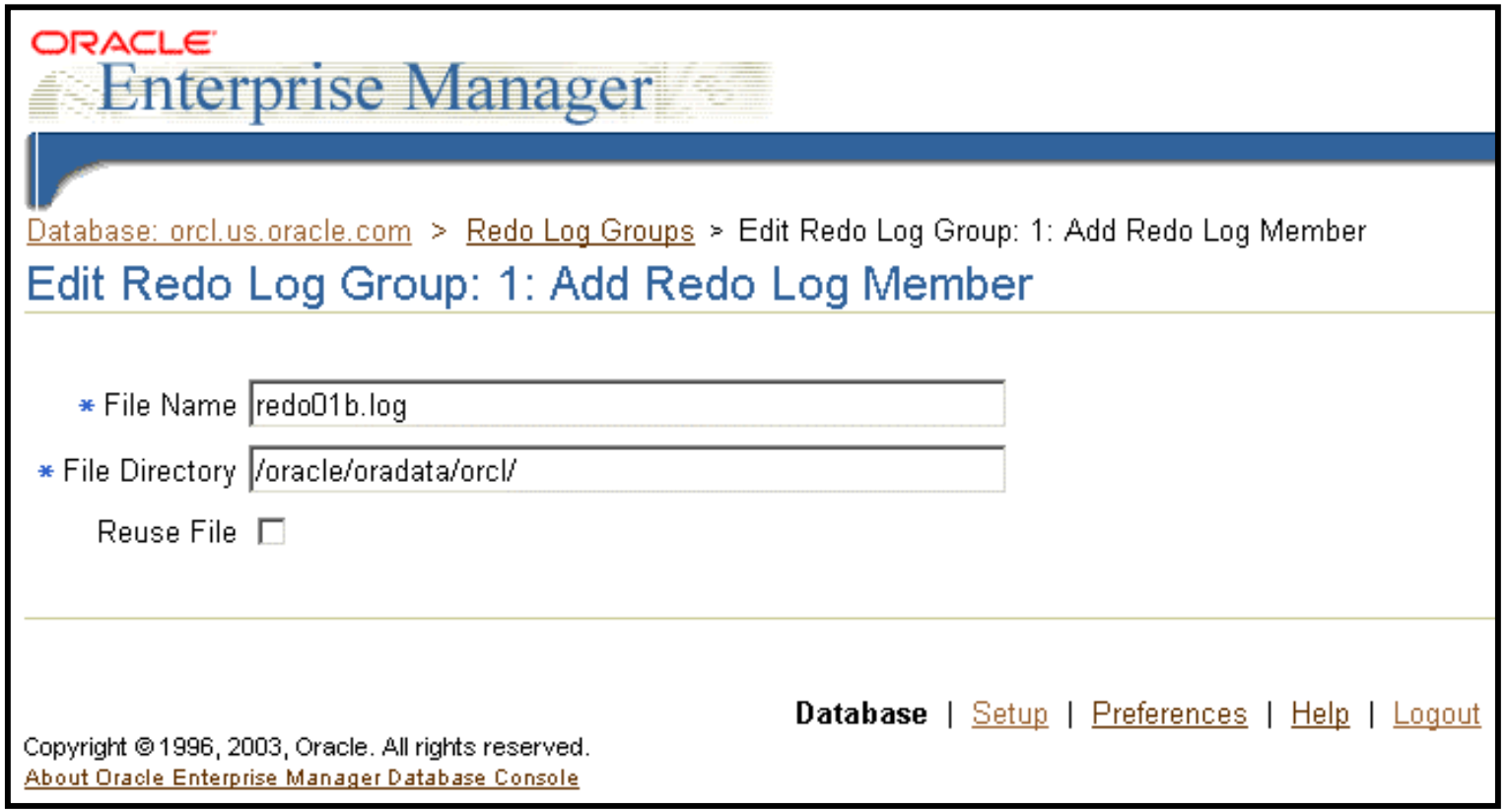
Multiplex redo log groups to protect against media failure and loss of data. It is suggested that redo log groups have:

- At least two members (files) per group
- Each member on a separate disk drive
- Each member on a separate disk controller

Note: Performance is heavily influenced by writing to redo logs.



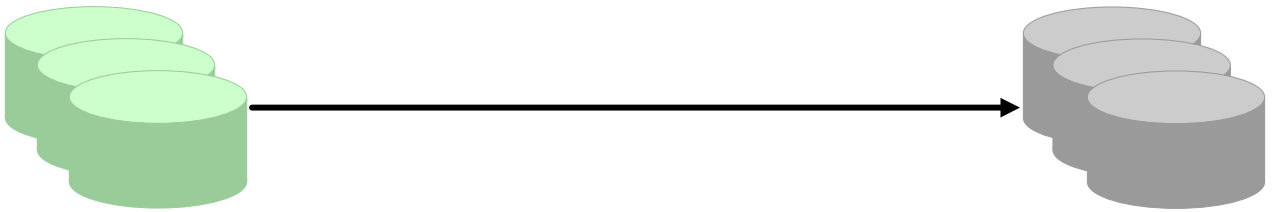
Multiplexing the Redo Log



Archive Log Files

To preserve redo information, create archived copies of redo log files by performing the following steps.

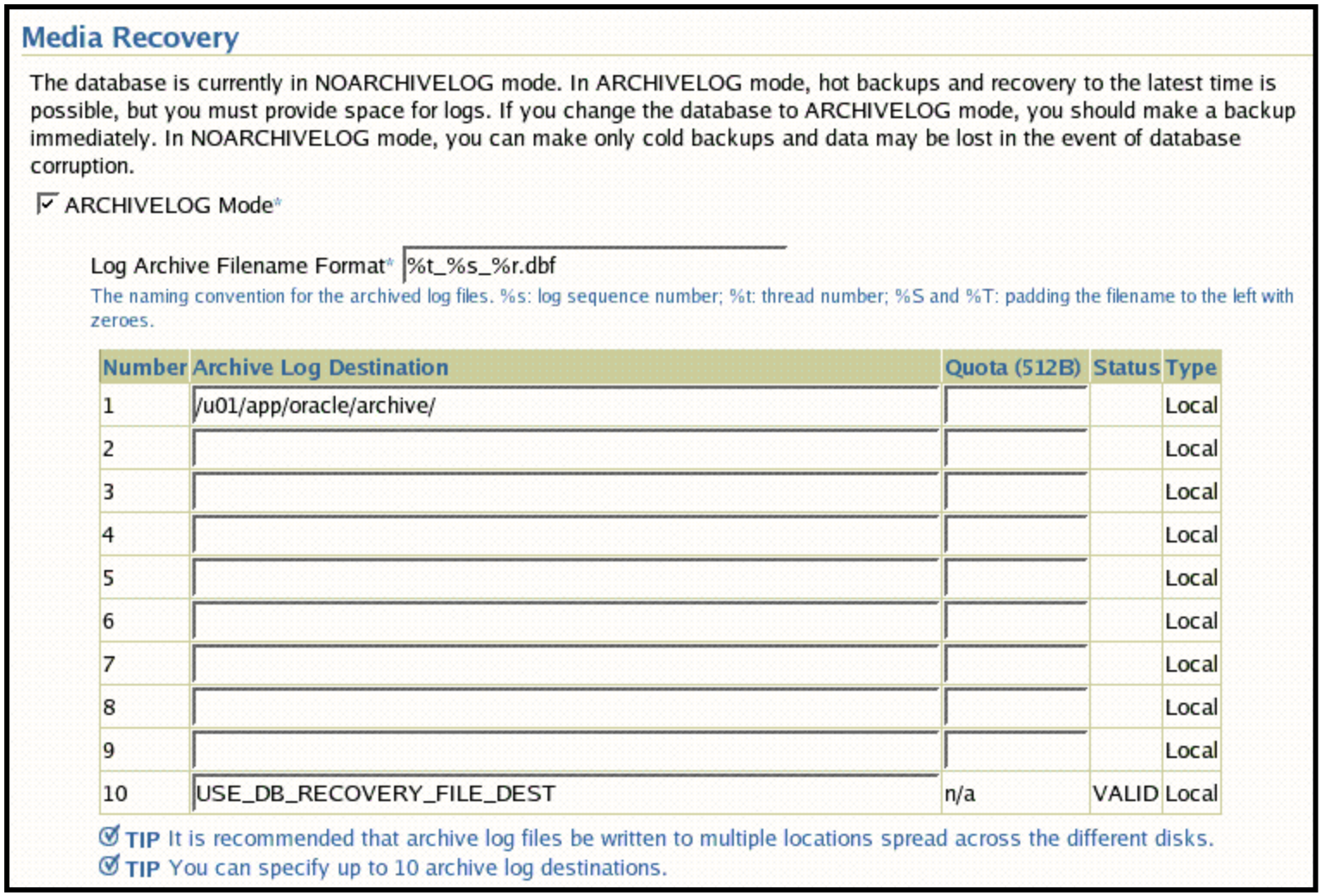
1. Specify archive log file naming convention.
2. Specify one or more archive log file locations.
3. Switch the database to `ARCHIVELOG` mode.



Online redo log files

Archive log files

Archive Log File: Naming and Destinations



Media Recovery

The database is currently in NOARCHIVELOG mode. In ARCHIVELOG mode, hot backups and recovery to the latest time is possible, but you must provide space for logs. If you change the database to ARCHIVELOG mode, you should make a backup immediately. In NOARCHIVELOG mode, you can make only cold backups and data may be lost in the event of database corruption.

☑ ARCHIVELOG Mode*

Log Archive Filename Format* %t_%s_%r.dbf

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	/u01/app/oracle/archive/			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

- To place the database in ARCHIVELOG mode, perform the following steps:
  1. Select the ARCHIVELOG Mode check box.
  2. Click Apply. The database can be set to ARCHIVELOG mode only from the MOUNT state.
  3. Click Yes when asked whether you want to restart the database.
  4. Back up your database.
- Databases in ARCHIVELOG mode have access to the full range of backup and recovery options.

Summary

In this lesson, you should have learned how to:

- Identify 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 archive log files
- Configure `ARCHIVELOG` mode

Practice Overview: Configuring for Recoverability

This practice covers the following topics:

- Multiplexing control files
- Multiplexing redo log groups
- Placing your database in `ARCHIVELOG` mode
- Ensuring that redundant archive logs are created