14

Backup and Recovery Concepts

Objectives

After completing this lesson, you should be able to:

- Identify the types of failure that can occur in an Oracle database
- Describe ways to tune instance recovery
- Identify the importance of checkpoints, redo log files, and archive log files
- Configure the fast recovery area
- Configure `ARCHIVELOG` mode

Part of Your Job

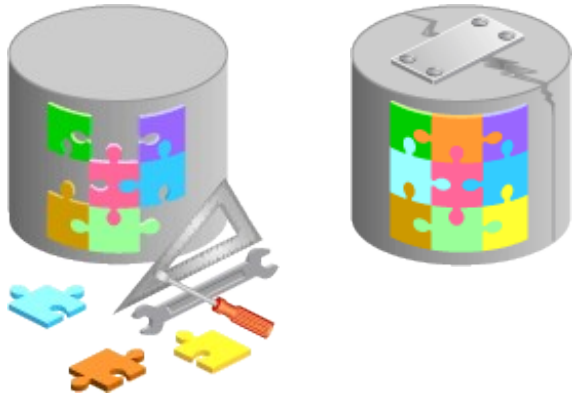
The database administrator's duties are to:

- Protect the database from failure wherever possible
- Increase the mean time between failures (MTBF)
- Protect critical components by redundancy
- Decrease the mean time to recover (MTTR)
- Minimize the loss of data

Categories of Failure

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
User inadvertently deletes or modifies data.	Roll back transaction and dependent transactions or rewind table.
User drops a table.	Recover table from recycle bin.

Oracle LogMiner

Flashback Technology

Using Flashback technology:

- Viewing past states of data
- Winding data back and forth in time
- Assisting users in error analysis and recovery

For error analysis:	For error recovery:
Oracle Flashback Query	**Oracle Flashback Transaction Backout**
Oracle Flashback Versions Query	**Oracle Flashback Table**
Oracle Flashback Transaction Query	**Oracle Flashback Drop**
	Oracle Flashback Database

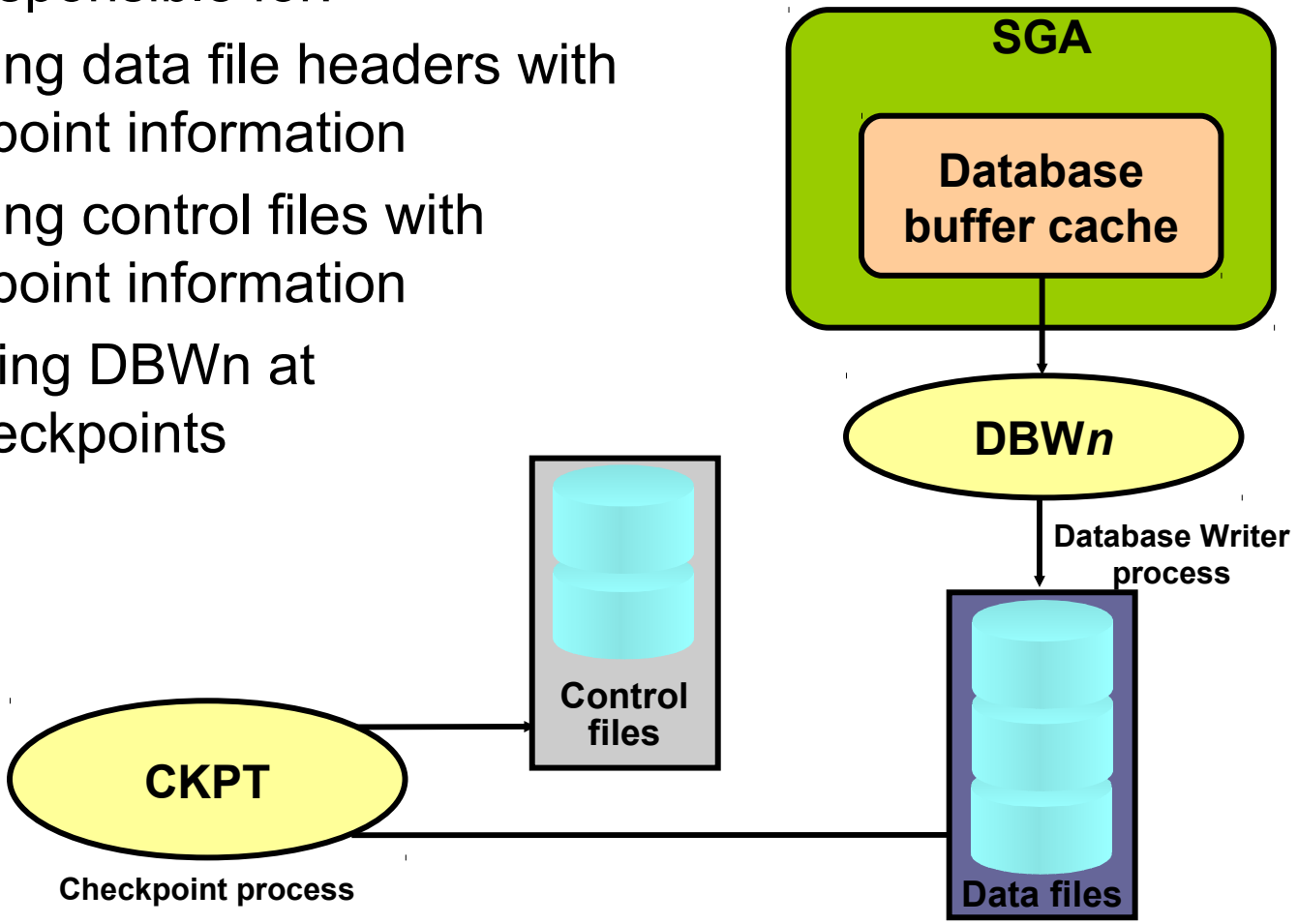
Instance Failure

Typical Causes	Possible Solutions
Power outage Hardware failure Failure of one of the critical background processes Emergency shutdown procedures	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.

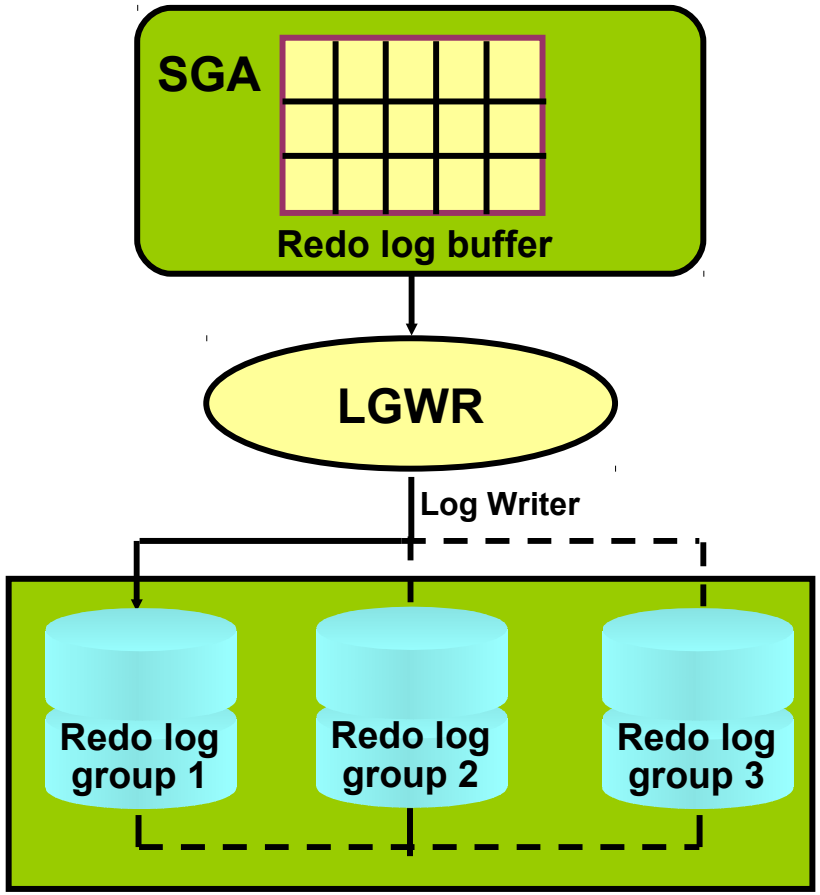
Understanding Instance Recovery: Checkpoint (CKPT) Process

CKPT is responsible for:

- Updating data file headers with checkpoint information
- Updating control files with checkpoint information
- Signaling DBWn at full checkpoints



Understanding Instance Recovery: Redo Log Files and Log Writer



Redo log files:

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

Log Writer writes:

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

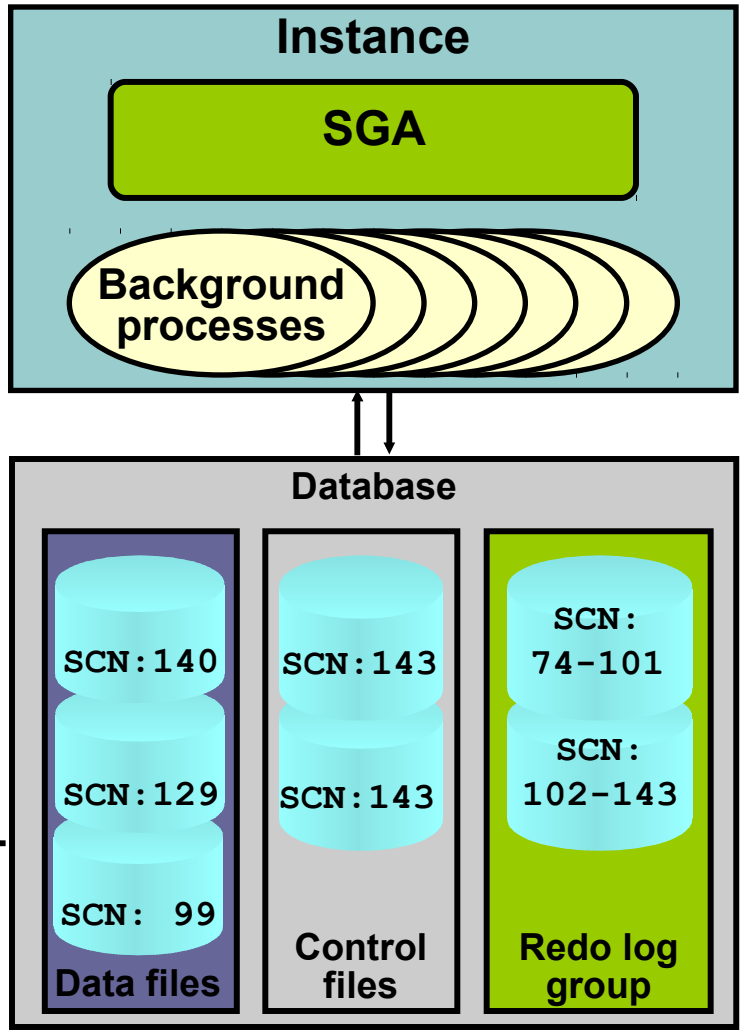
Understanding Instance Recovery

Automatic instance or crash recovery:

- Is caused by attempts to open a database whose files are not synchronized on shutdown
- Uses information stored in redo log groups to synchronize files
- Involves two distinct operations:
  - Rolling forward: Redo log changes (both committed and uncommited) are applied to data files.
  - Rolling back: Changes that are made but not committed are returned to their original state.

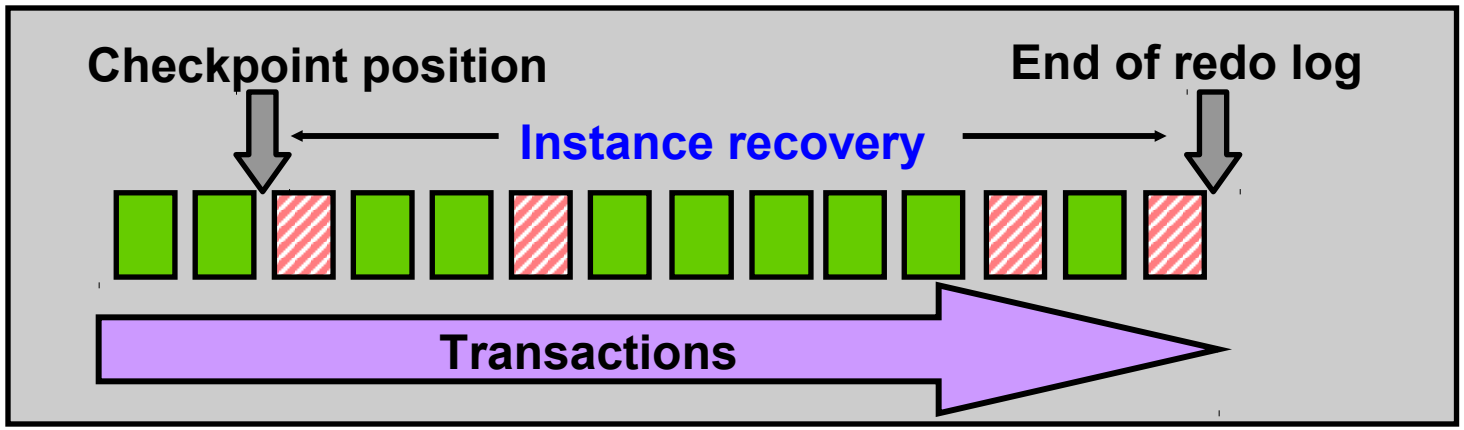
Phases of Instance Recovery

1. Startup instance (data files are out of sync)
2. Roll forward (redo)
3. Committed and uncommitted data in files
4. Database opened
5. Roll back (undo)
6. Committed data in files



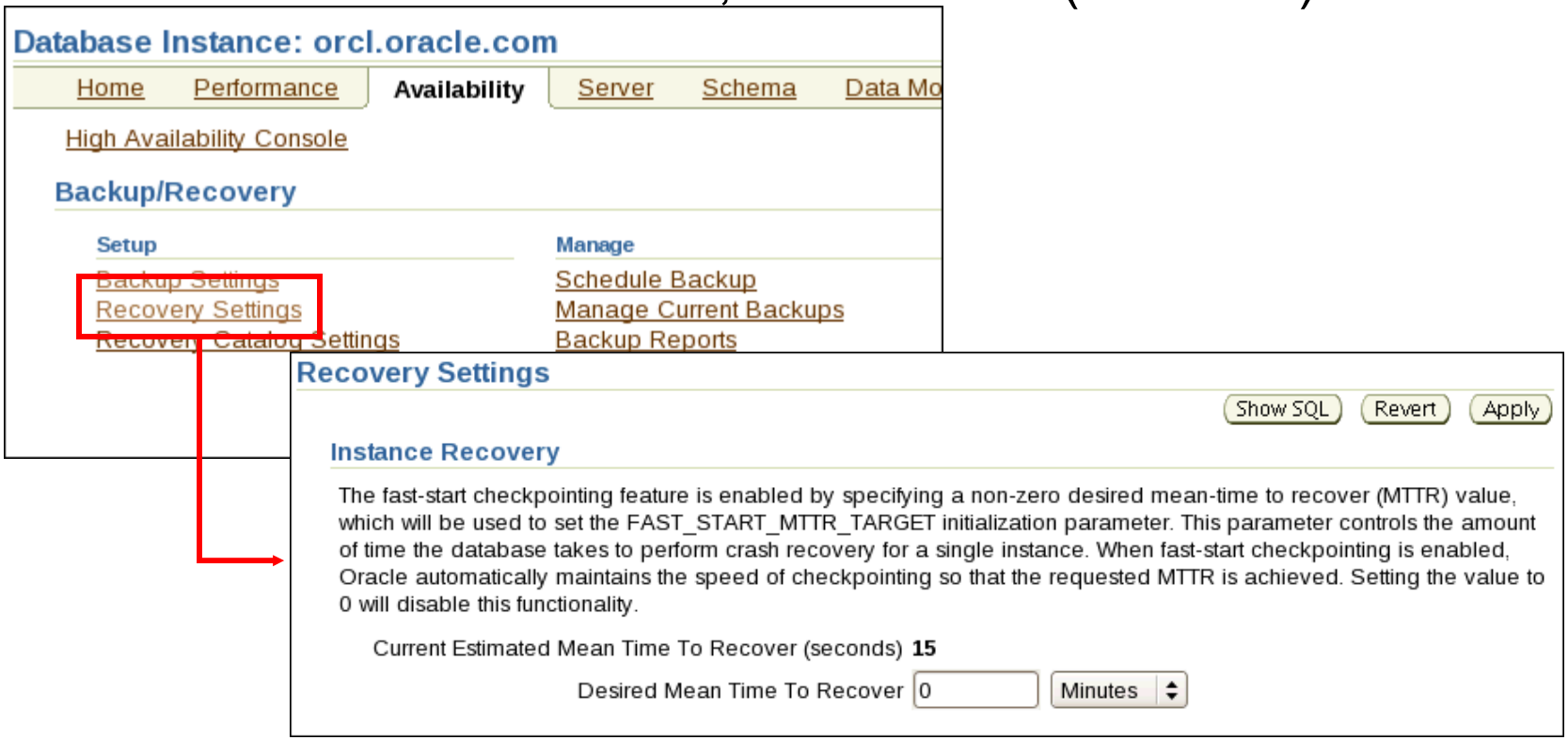
Tuning Instance Recovery

- 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).



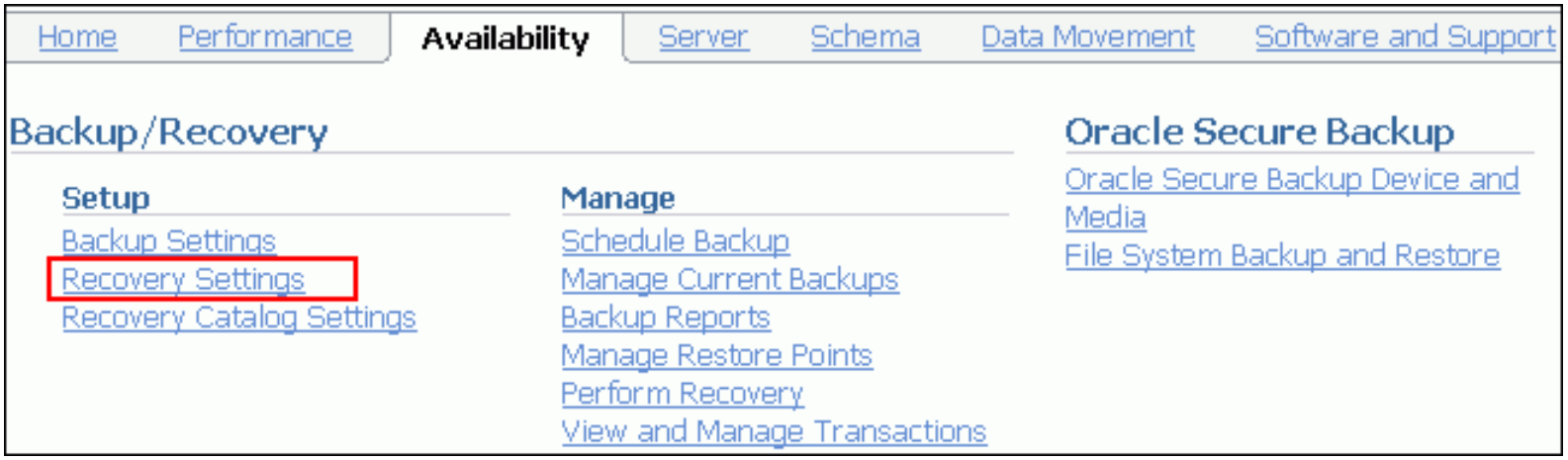
Media Failure

Typical Causes	Possible Solutions
Failure of disk drive	1. Restore the affected file from backup. 2. Inform the database about a new file location (if necessary). 3. Recover the file by applying redo information (if necessary).
Failure of disk controller	
Deletion or corruption of a file needed for database operation	

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



Configuring the Fast Recovery Area

Fast recovery area:

- Strongly recommended for simplified backup storage management
- Storage space (separate from working database files)
- Location specified by the `DB_RECOVERY_FILE_DEST` parameter
- Size specified by the `DB_RECOVERY_FILE_DEST_SIZE` parameter
- Large enough for backups, archived logs, flashback logs, multiplexed control files, and multiplexed redo logs
- Automatically managed according to your retention policy

Configuring the fast recovery area means determining location, size, and retention policy.

Multiplexing Control Files

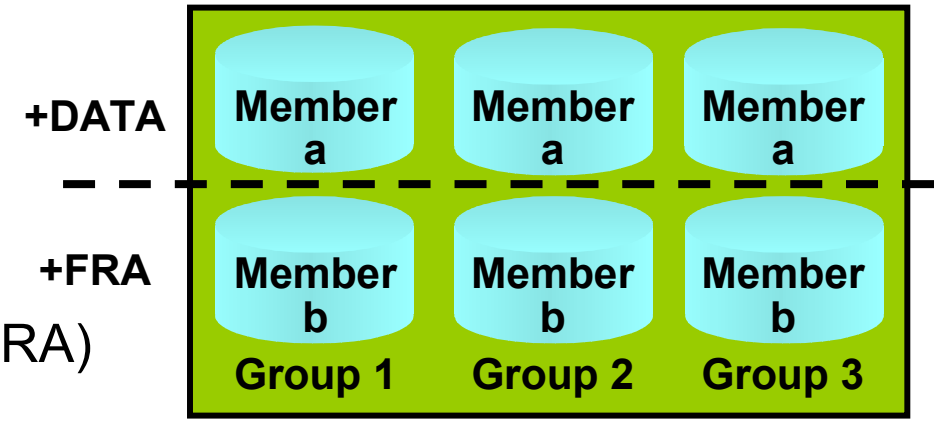
To protect against database failure, your database should have multiple copies of the control file.

	ASM Storage	File System Storage
Best Practice	One copy on each disk group (such as +DATA and +FRA)	At least two copies, each on separate disk (at least one on separate disk controller)
Steps to create additional control files	No additional control file copies required.	1. Alter the `SPFILE` with the `ALTER SYSTEM SET control_files` command. 2. Shut down the database. 3. Copy control file to a new location. 4. Open the database and verify the addition of the new control file.

Redo Log Files

Multiplex redo log groups to protect against media failure and loss of data. This increases database I/O. It is suggested that redo log groups have:

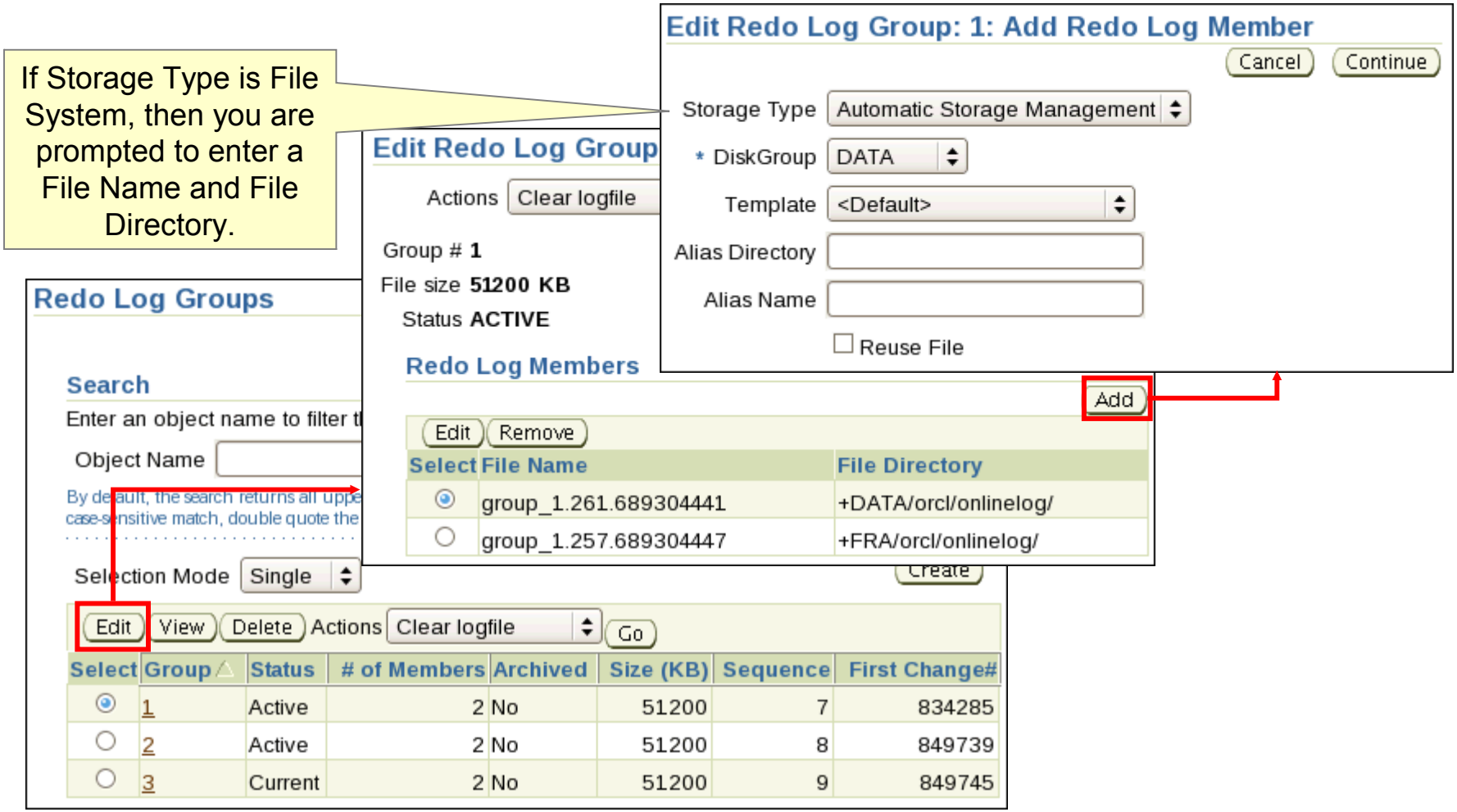
- At least two members (files) per group
- Each member:
  - On a separate disk or controller if using file system storage
  - In a separate disk group (such as +DATA and +FRA) if using ASM



Note: Multiplexing redo logs may impact overall database performance.

Multiplexing the Redo Log

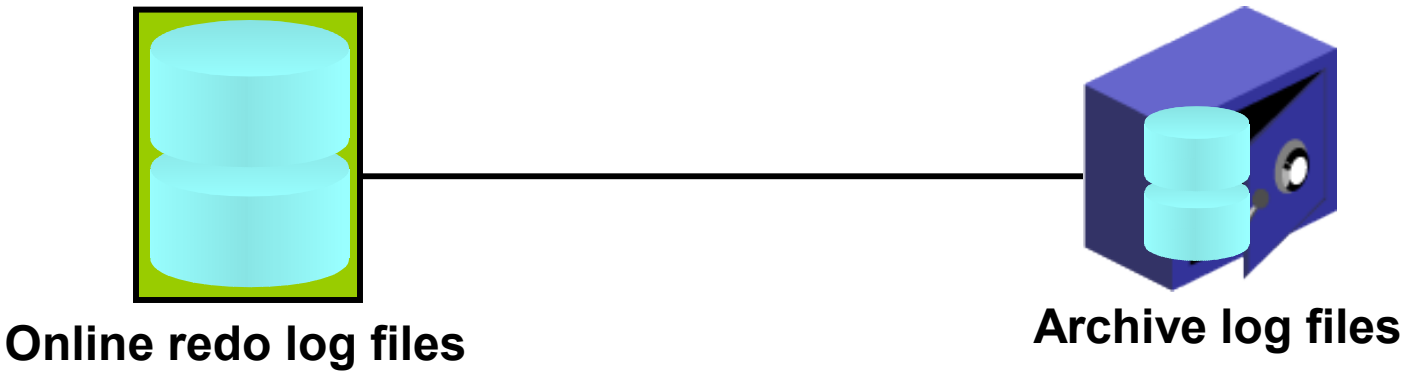
If Storage Type is File System, then you are prompted to enter a File Name and File Directory.



Archive Log Files

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

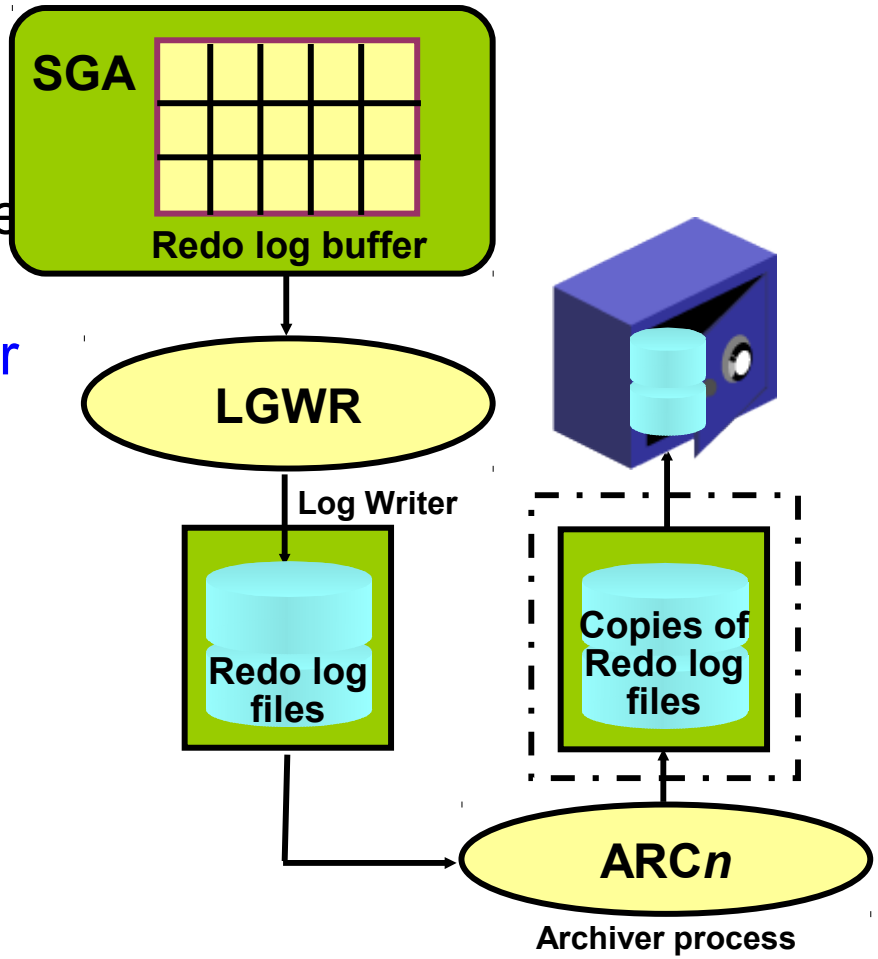
1. Specify archive log file-naming convention.
2. Specify one or more archive log file locations.
3. Switch the database to `ARCHIVELOG` mode.



Archiver (ARC*n*) Process

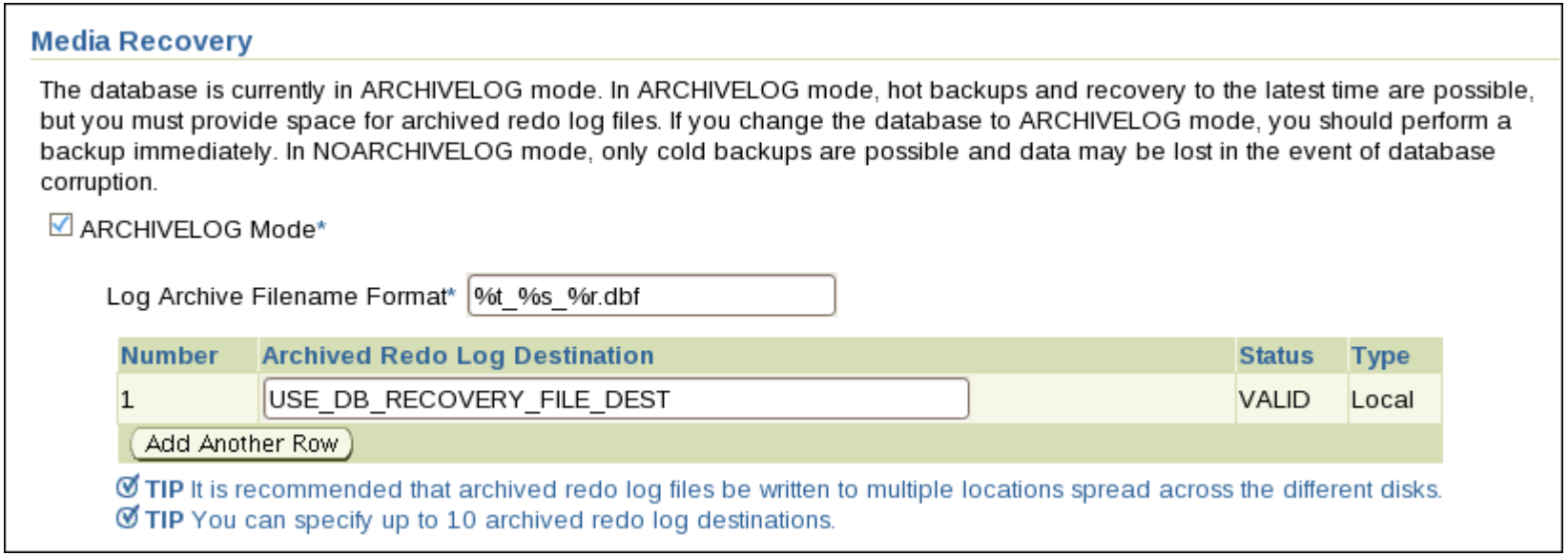
Archiver (ARC*n*):

- 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



Archive Log File: Naming and Destinations

Specify naming and archive destination information on the Recovery Settings page. If using file system storage then it is recommended that you add multiple locations across different disks.



Enabling ARCHIVELOG Mode

To place the database in ARCHIVELOG mode, perform the following steps in Enterprise Manager:

1. Select the ARCHIVELOG Mode check box and click Apply.

   The database can be set to ARCHIVELOG mode only from the MOUNT state.
2. Restart the database (with SYSDBA privileges).
3. (Optional) View the archive status.
4. Back up your database.

Note: Databases in ARCHIVELOG mode have access to the full range of backup and recovery options.

```
sqlplus / as sysdba

shutdown immediate
startup mount
alter database archivelog;
alter database open;
archive log list
```

Quiz

Statement failure is never by design and always requires the DBA to address the issue.

1. True
2. False

Quiz

Which parameters configure the fast recovery area?

1. FLASH_RECOVERY_AREA_SIZE
2. DB_RECOVERY_FILE_DEST
3. FLASH_RECOVERY_AREA_LOC
4. DB_RECOVERY_FILE_DEST_SIZE

Summary

In this lesson, you should have learned how to:

- Identify the types of failure that can occur in an Oracle database
- Describe ways to tune instance recovery
- Identify the importance of checkpoints, redo log files, and archive log files
- Configure the fast recovery area
- Configure ARCHIVELOG mode

Practice 14 Overview: Configuring for Recoverability

This practice covers the following topics:

- Verifying control files
- Configuring a default fast recovery area
- Multiplexing redo log groups
- Placing your database in ARCHIVELOG mode
- Ensuring that redundant archive logs are created