

# Backup & Recovery

WEEK 12

We'll talk about:

How to backup  
the data.

Types of  
backups.

How to restore  
the data from  
backups.

# How the data might get lost?

---

## Faulty hardware:

- Storage devices (most likely to crash)

## Human errors:

- Dropping a table by mistake
- An erroneous UPDATE statement
- Delete some datafiles by accident
- Dorel unleashed, etc.

## Cybercrime:

- Deliberate data lost

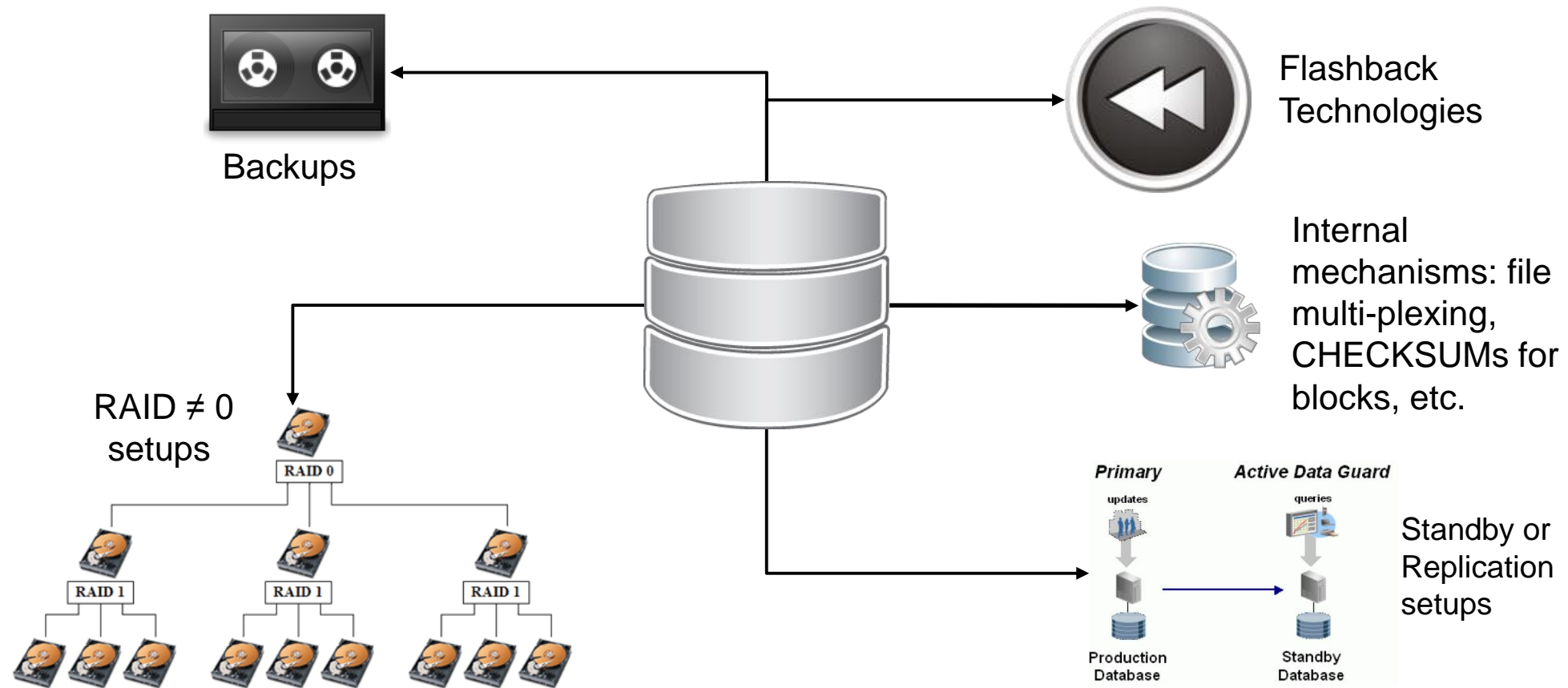
## Bugs:

- Right into the firmware (low level/hardware device)
- Into the operating system
- Into the Oracle/DBMS kernel
- Into the client application

## Disaster scenarios:

- earthquakes, floods, fire etc.

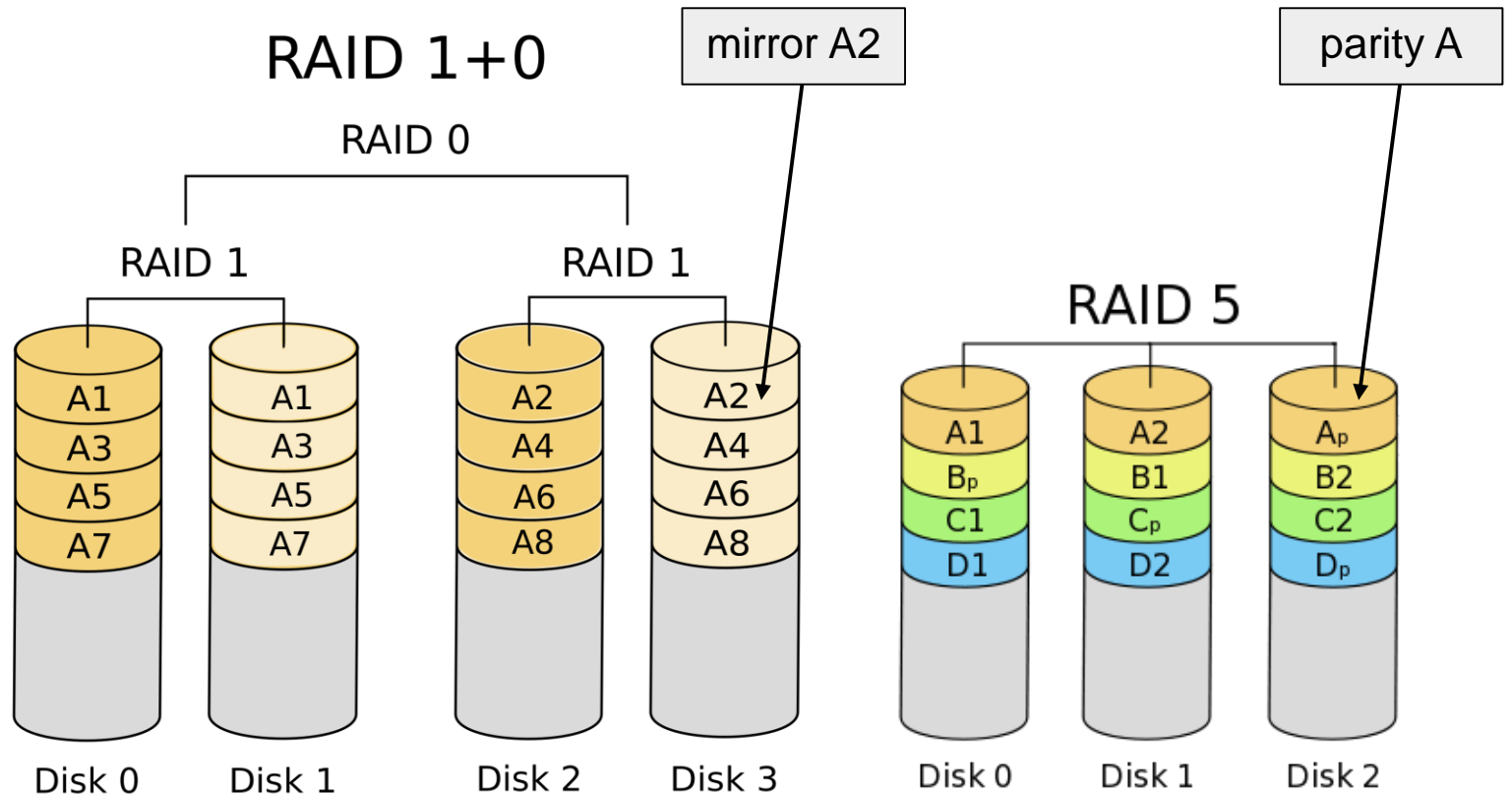
# How to Protect Data



# RAID Setups

# RAID10 vs RAID5

- It refers to a specific way of putting together more HDDs so that to have an additional protection level and performance
- The most used RAID setups in the DB field are RAID10 and RAID5.

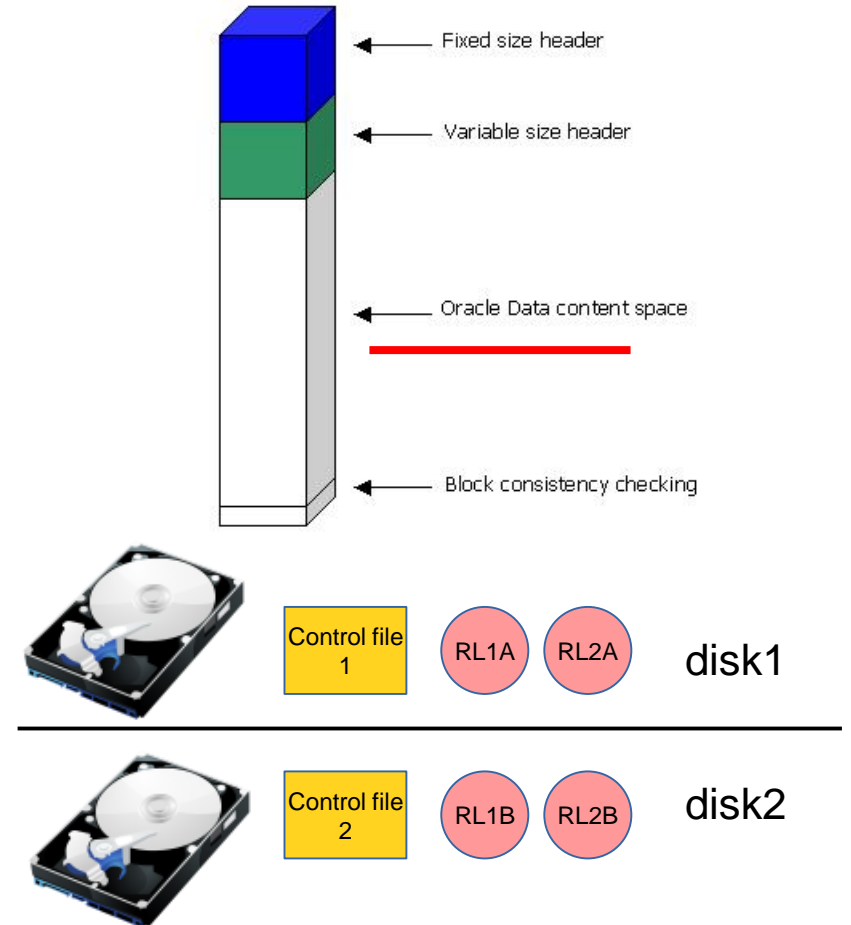


A solid orange vertical bar is positioned on the left side of the slide, extending from the top to the bottom.

# Internal mechanisms for data protection

# Oracle Provides

- The ARCHIVELOG mode through which the redo log stream is preserved in archives (offline redologs)
- File multiplexing: the control file or the redologs
- Checking the integrity of the Oracle block (see DB\_BLOCK\_CHECKING and DB\_BLOCK\_CHECKSUM)
- The possibility to configure multiple archiving destinations





# Backups

It's just a  
copy of  
the real  
data.

**Important:** It's not a good idea to take a backup into the same disk where the original data resides. If that disk fails, we lost the data and the backups as well.

It can be  
used:

- To recover if the data get lost
- To duplicate the data to other environments (usually TEST or DEVELOPMENT)

# What is a Backup

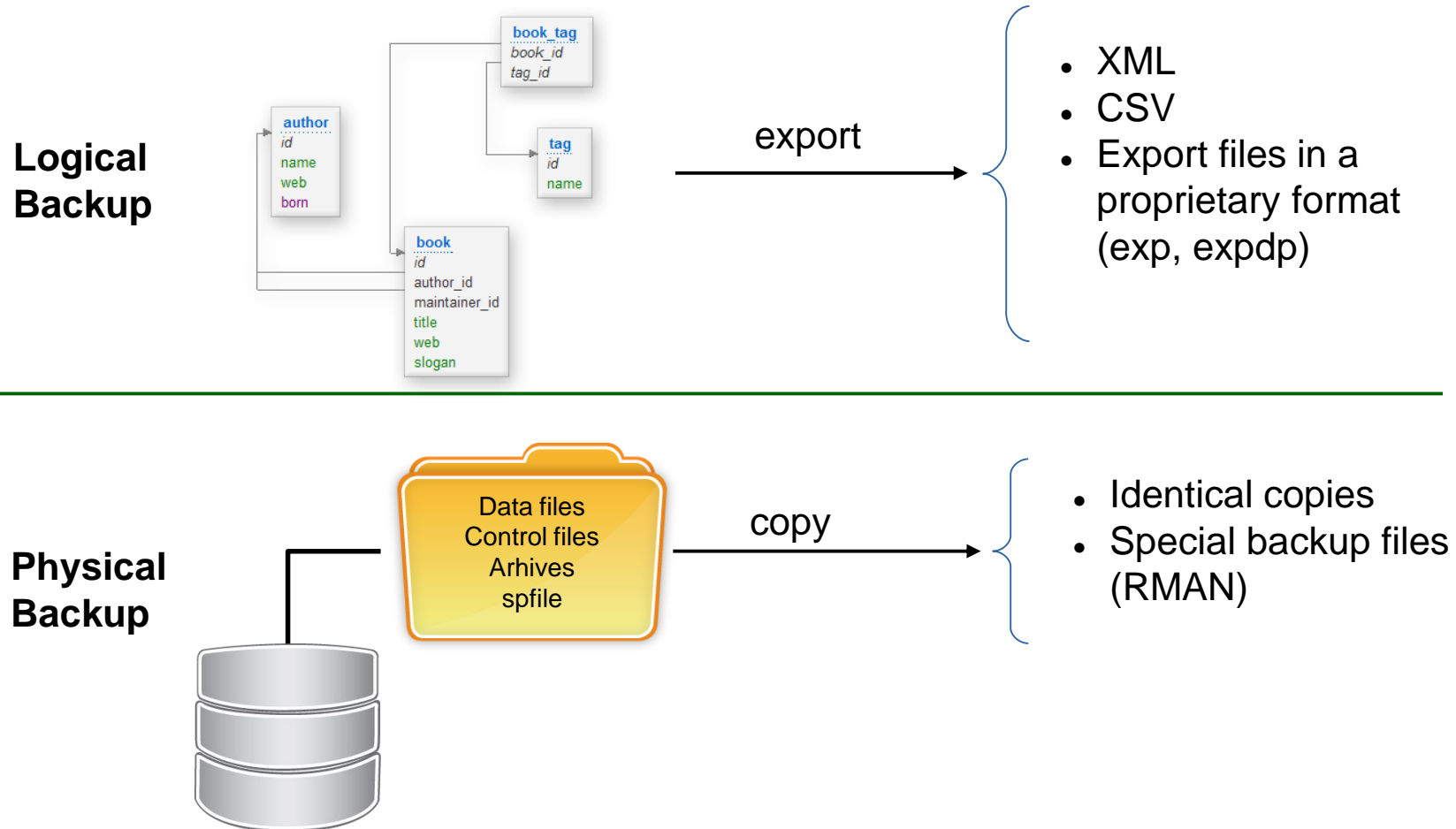
# Ah, but I don't have any backups

---



- To take regular backups is one of the main duties of a DBA.
- The data is exposed to many potential risks which might cause a partial or a total loss.
- The costs to recover when there are no backups are very high and sometimes it's impossible to get the data back.
- Failing to restore the data in a timely fashion might lead to bankruptcy.

# Types of Backups



## PROS:

- Can operate on a DB object (table, stored procedure etc.)
- Allows specifying the records to be backed up (in DataPump, the QUERY parameter)
- Relatively easy to obtain
- OS cross platform format

## CONS:

- Not good for big amounts of data (slow)
- Importing logical backups generate redo log
- The database must be open in order to be able to take or restore a logical backup.

# Logical Backups

# Examples of Logical Backups

---

Starting with Oracle 10g, it is advisable to use DataPump:

```
expdp scott/tiger@db tables=EMP,DEPT directory=TEST_DIR  
dumpfile=EMP_DEPT.dmp logfile=expdp.log
```

```
impdp scott/tiger@db tables=EMP,DEPT directory=TEST_DIR  
dumpfile=EMP_DEPT.dmp logfile=impdp.log
```

**Note:** *The old export/import tools are still available but they are deprecated, meaning that Oracle doesn't provide support for them, nor does new features.*

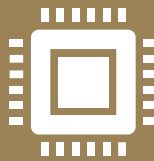
# Challenge



Developers want to start working on FaceBook 2.0. They come to you and ask if you can duplicate the current productive FB schema to a new one called FB2. FB2 should contain the same objects and data as FB.



How would you do it?



Implement the solution using our Oracle playground VM.

# Physical Backups

The most common way of taking DB backups

Suitable for backing up big databases

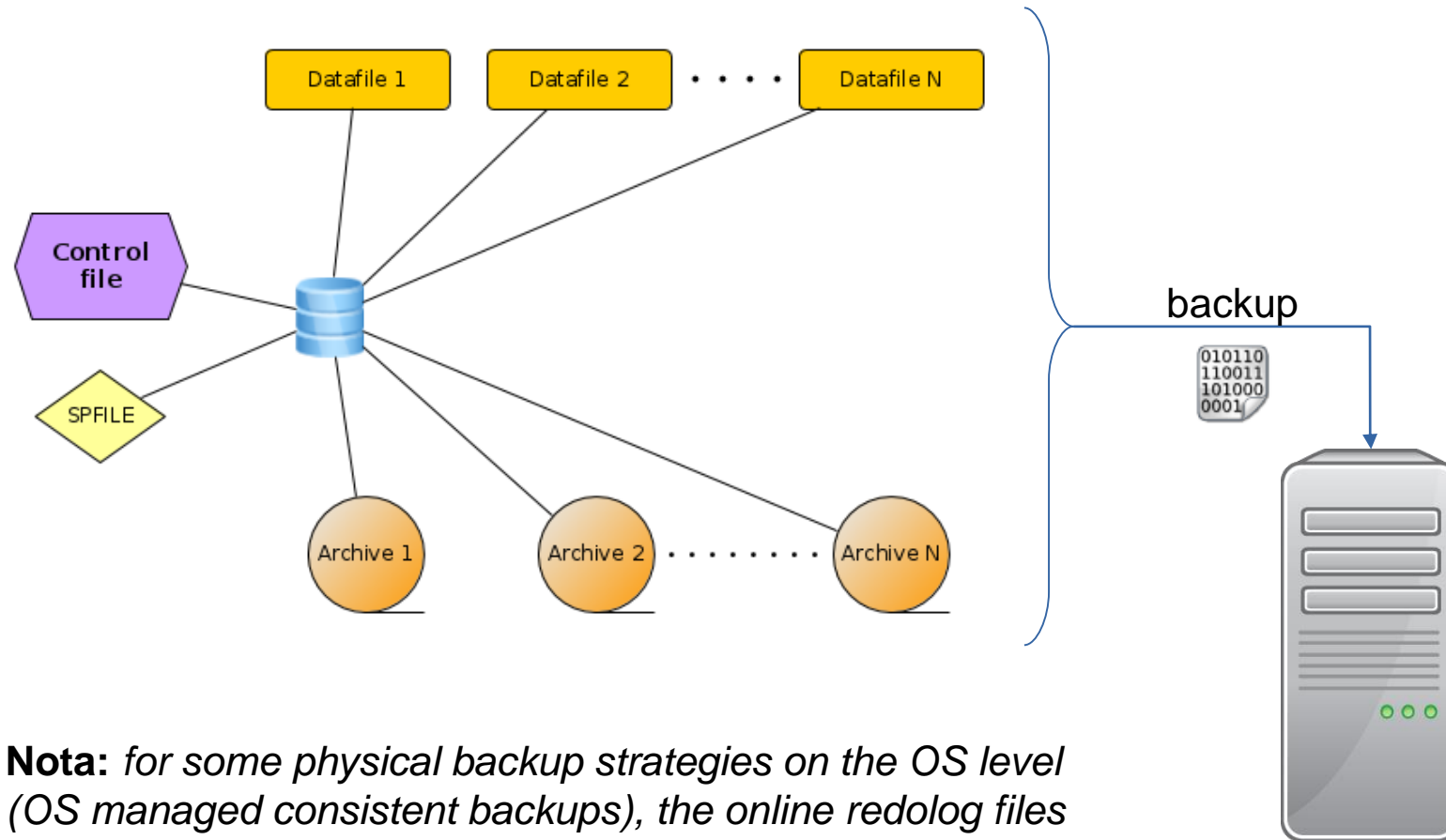
Can be:

- **Consistent backups:** when they are taken with a closed database
- **Inconsistent backups:** when the database is changed while the backup is running (open DB)

**Note:** there's also the concept of a consistent logical backup, but in this case it refers to a specific moment in time (see for expdp the *FLASHBACK\_TIME* and *FLASHBACK\_SCN* parameters).

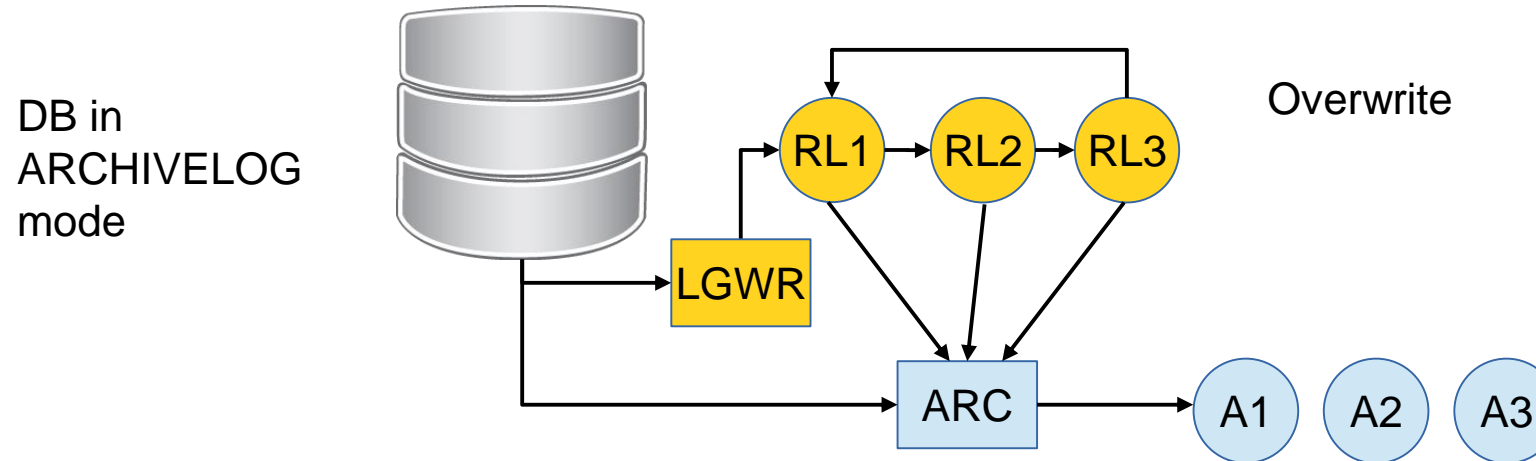
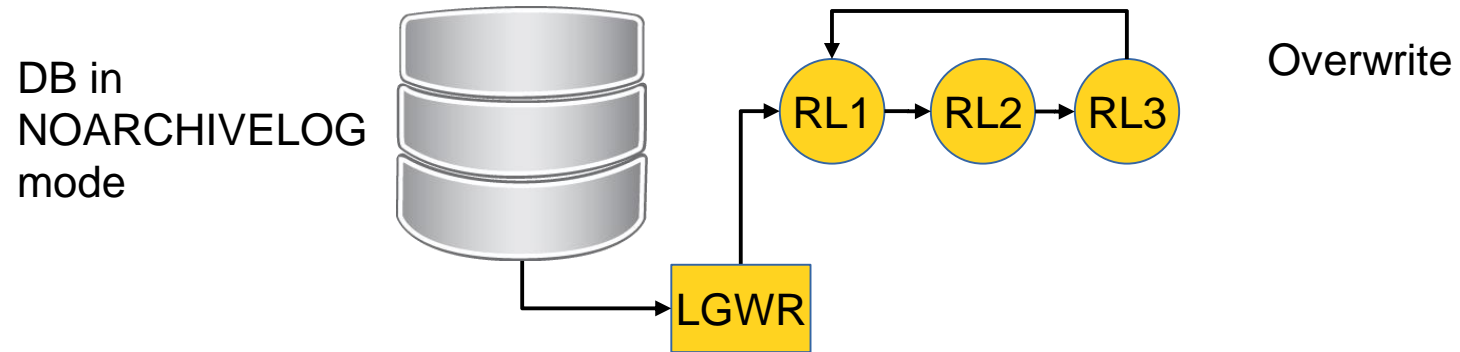


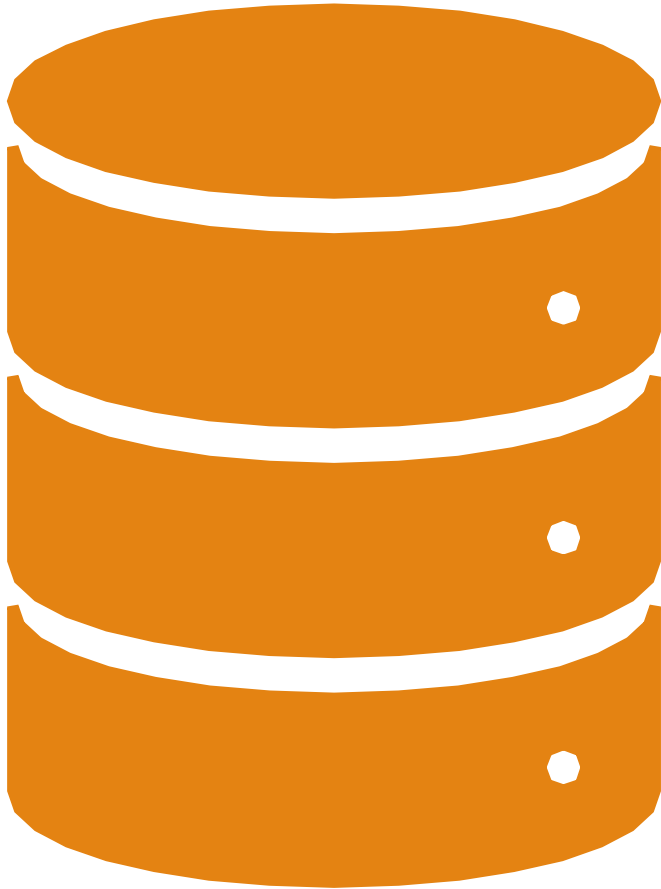
# Files which are Targeted by a Physical Backup



**Nota:** for some *physical backup strategies on the OS level (OS managed consistent backups)*, the online redolog files may also be considered.

# Back to the basics: ARCHIVELOG vs NOARCHIVELOG





# Workshop

---

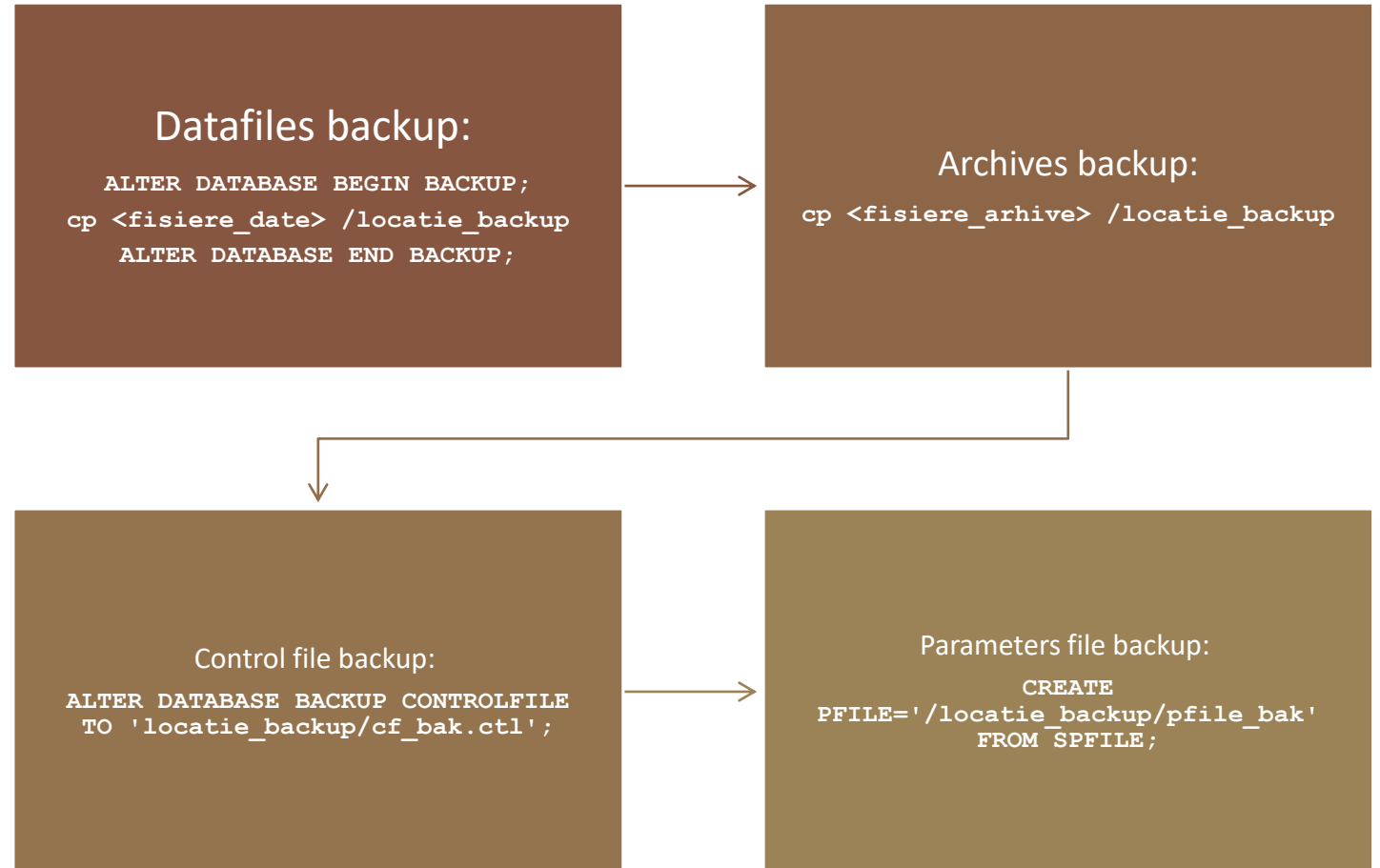
Put the database in ARCHIVELOG mode.

# OS Managed Backups

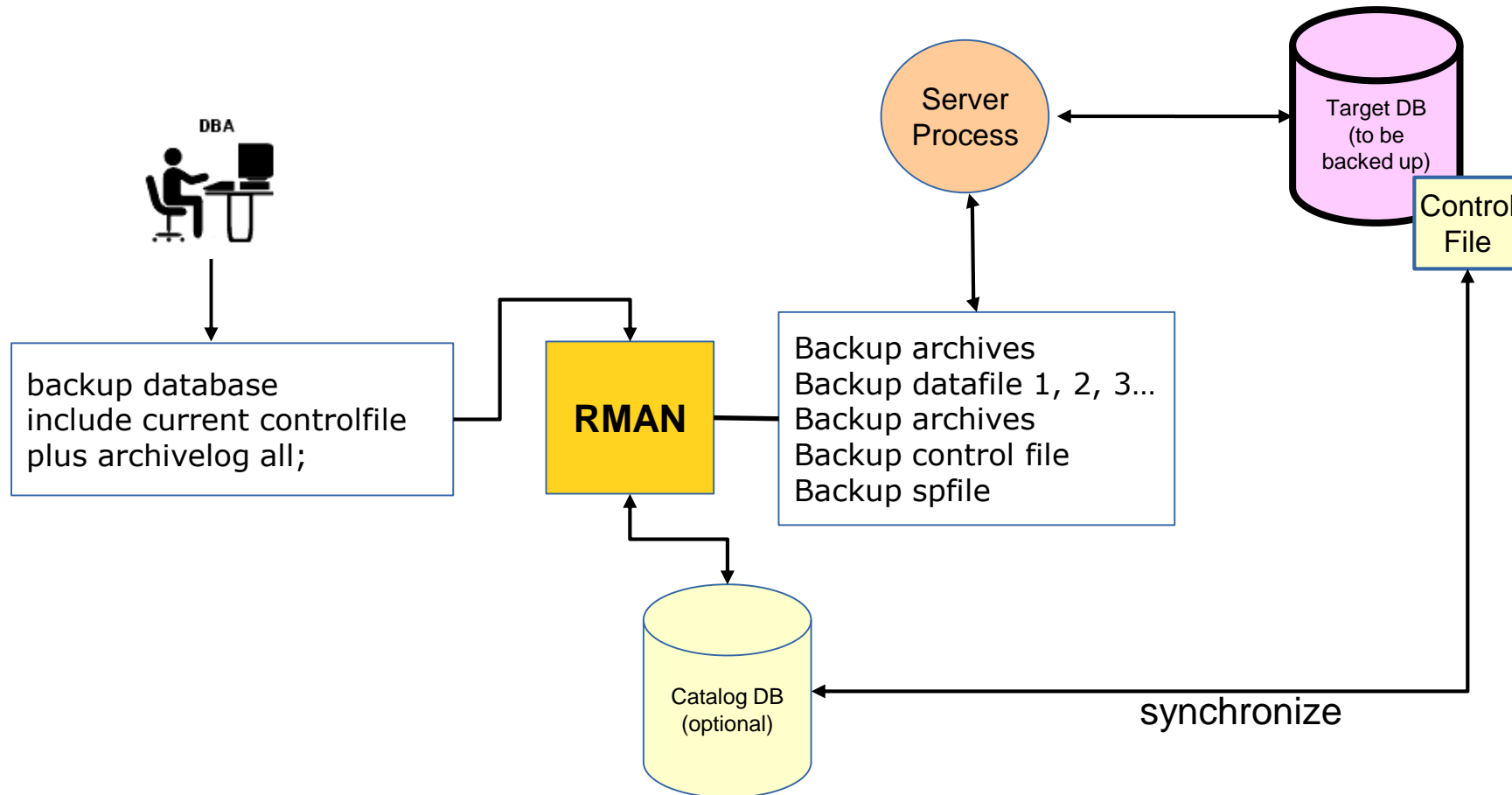
- It uses regular OS commands (cp, scp, xcopy, ftp etc.).
- If the database is opened (for R/W), before initiating the backup, we must ensure the DB is placed in the so-called BACKUP mode.

PROS	CONS
Simplicity as far as the OS commands are concerned	There is the possibility to leave out some database files and thus to invalidate the whole backup.
The only option for those databases older than Oracle 8i	Special care when implementing the retention of the current backups.
Fast when combined with facilities of snapshotting or low level replication.	The BACKUP mode may be problematic because it implies a performance penalty (more redo is generated)
Very appealing to sysadmins.	It's not so easy to validate the backups.

# Example of an OS Managed Physical Backup



# RMAN Overview



# RMAN Backups

---

- RMAN (Recovery Manager) is an Oracle tool especially designed to take and manage Oracle backups.
- Backing up with RMAN is the recommended way, as advised by Oracle.

Some PROS	CONS
The DB is not required to be in the BACKUP mode.	It takes time to learn this new tool.
It provides various retention policies.	Subject to various limitations on Oracle Standard Edition (no parallelism, no block recovery)
It can be used to take incremental backups.	
It validates the backups.	
It provides means to manage the RMNA catalog (in the control file or in a separate database)	
It can be easily integrated with tape libraries.	

# RMAN Configuration

Display all global settings.

```
C:\Windows\system32\cmd.exe - rman target /  
  
C:\Users\talek>rman target /  
Recovery Manager: Release 11.2.0.4.0 - Production on Sun Feb 28 20:50:22 2016  
Copyright (c) 1982, 2011, Oracle and/or its affiliates. All rights reserved.  
connected to target database: SIA1 (DBID=790291549)  
RMAN> show all;  
  
using target database control file instead of recovery catalog  
RMAN configuration parameters for database with db_unique_name SIA1 are:  
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default  
CONFIGURE BACKUP OPTIMIZATION OFF; # default  
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default  
CONFIGURE CONTROLFILE AUTOBACKUP OFF; # default  
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default  
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default  
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default  
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default  
CONFIGURE MAXSETSIZE TO UNLIMITED; # default  
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default  
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default  
CONFIGURE COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT' OPTIMIZE FOR LOAD TRUE ; # default  
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default  
CONFIGURE SNAPSHOT CONTROLFILE NAME TO 'C:\ORA\PRODUCT\11.2.0\DBHOME_1\DATABASE\SNCF5IA1.ORA'; # default
```

Important in some crash scenarios.

*Example of how to config something in RMAN:*

**configure device type disk parallelism 2 backup type to compressed backupset;**



# The Auto-backup Control File Feature

---

- If this feature is activated, Oracle will take an automatic backup of the control-file and SPFILE on every RMAN backup and whenever a structural DB change (like adding/dropping a new data-file) takes place.
- It is recommended to use this feature especially if no separate DB is used for the RMAN catalog.

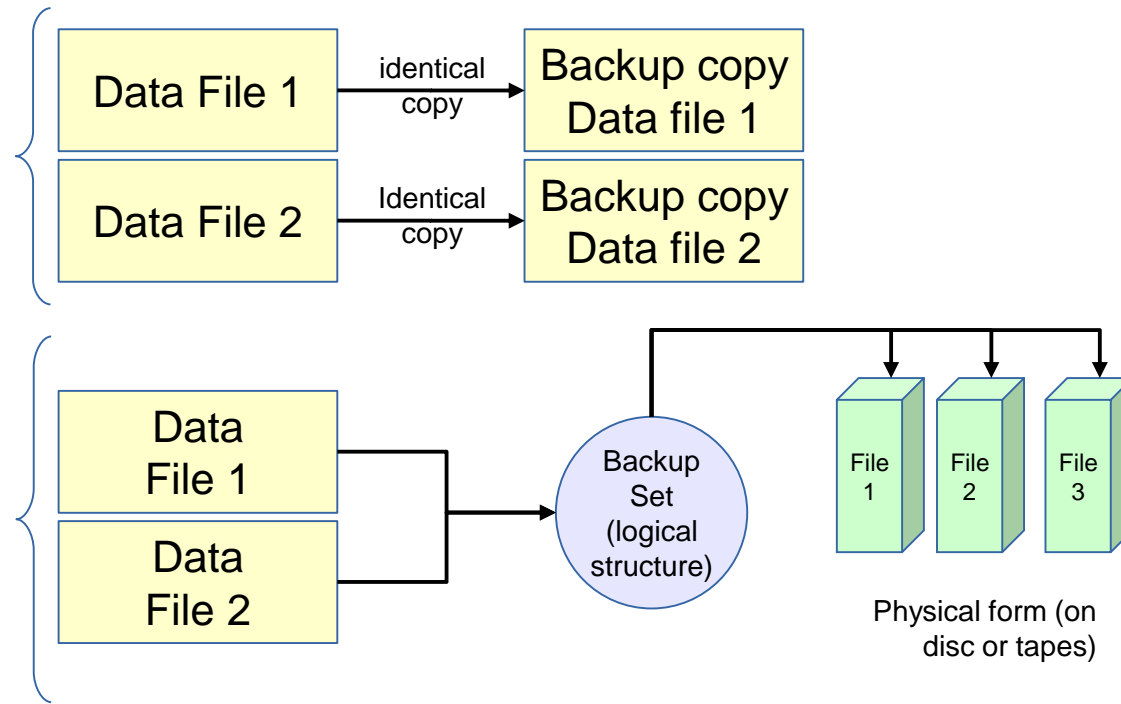
```
CONFIGURE CONTROLFILE AUTOBACKUP ON;  
CONFIGURE CONTROLFILE AUTOBACKUP FOR DEVICE TYPE DISK  
FORMAT '/backup/%F';
```

# RMAN Backup Files

It's about those files which are created by RMAN as part of a backup operation.

**File copies:** identical copies of the source files but in another location and, most likely, having a different name.

**Backupset files:** the source files may be combined in the same backupset, compressed etc. One backupset can have one or more backup pieces.



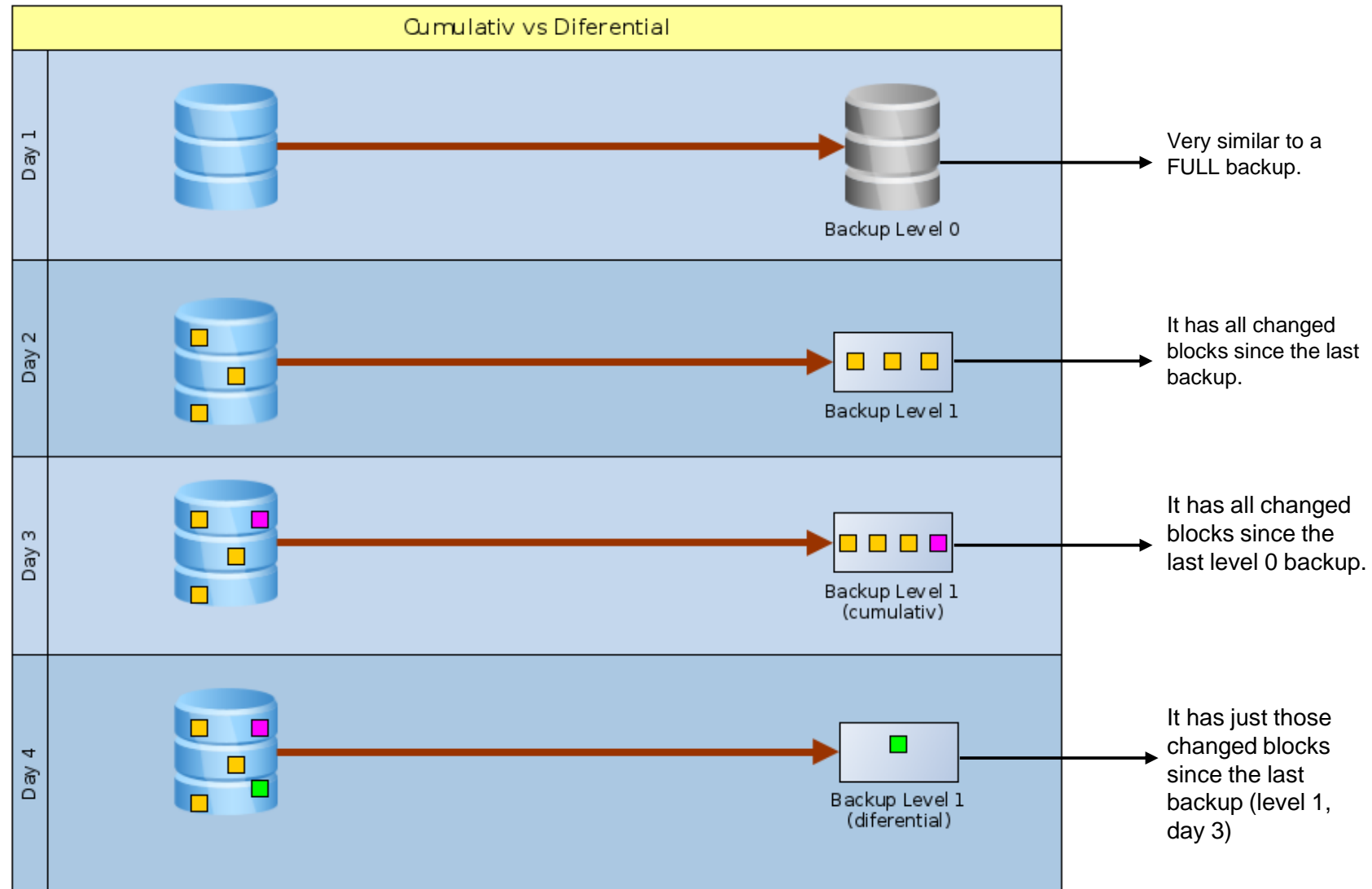
# Examples of RMAN Backup Commands

```
rman target /  
rman target sys/pwd@db catalog user/pwd@catdb
```

```
BACKUP AS COPY DATABASE TAG 'FULL_BACKUP_20160210';  
BACKUP CURRENT CONTROLFILE;  
BACKUP ARCHIVELOG ALL FORMAT '/BACKUP/%U' DELETE INPUT;  
BACKUP SPFILE;
```

```
RUN {  
  ALLOCATE CHANNEL C1 DEVICE TYPE DISK;  
  BACKUP AS COMPRESSED BACKUPSET  
    CHECK LOGICAL NOEXCLUDE  
    (DATABASE  
      FILESPERSET 5  
      FORMAT '/BACKUP/%d_%s_%p_%t'  
      NOT BACKED UP SINCE TIME 'SYSDATE-1'  
    ) PLUS ARCHIVELOG FORMAT '/BACKUP/ARCH/%U';  
  DELETE NOPROMPT OBSOLETE REDUNDANCY 2;  
  RELEASE CHANNEL C1;  
}
```

# Incremental Backups



### Day 1:

- backup incremental level 0 database;

### Day 2:

- backup incremental level 1 database;

### Day 3:

- backup incremental level 1 cumulative database;

### Day 4:

- backup incremental level 1 database;

## Incremental Backups Flow



# Workshop

WHILE THE DATABASE  
IS UP & RUNNING,  
FULLY BACKUP IT  
USING RMAN UTILITY.

## List Available RMAN Backups

```
RMAN> list backup of datafile 1;

List of Backup Sets
=====

BS Key   Type LV Size       Device Type Elapsed Time Completion Time
-----
11        Full  195.93M   DISK        00:00:27    28-FEB-16
BP Key: 11  Status: AVAILABLE Compressed: YES  Tag: TAG20160228T203045
Piece Name: C:\ORA\FAST_RECOVERY_AREA\SIA1\BACKUPSET\2016_02_28\01_MF_NNDF_TAG20160228T203045_CF6H60LY_.BKP
List of Datafiles in backup set 11
File LV Type Ckp SCN    Ckp Time  Name
-----
1        Full 915196    28-FEB-16 C:\ORA\SIA1\DISK1\SYSTEM01.DBF
```

**LIST BACKUP OF DATAFILE 1;  
LIST BACKUP OF DATABASE;  
LIST BACKUP SUMMARY;  
LIST BACKUPSET TAG 'FULL\_BACKUP\_20160210';  
LIST COPY OF DATAFILE 2 COMPLETED BETWEEN  
'10-DEC-2015' AND '17-JAN-2016';**

# Backups Retention

When a backup is considered obsolete.

The following backup retention policies are provided by RMAN:

- **REDUNDANCY policy:** a backup becomes obsolete as soon as there are at least N more recent backups.
- **RECOVERY WINDOW policy:** a backup is considered obsolete if cannot (or is not practical to) be used to recover the database as it was N days ago.
- **Explicit retention:** using the KEEP clause of the CHANGE command. It can be an explicit date or FOREVER if the intention is to keep that backup indefinitely.



# Retention Related RMAN Commands

```
CONFIGURE RETENTION POLICY  
  TO REDUNDANCY 2;  
CONFIGURE RETENTION POLICY  
  TO RECOVERY WINDOW OF 7 DAYS;
```

Global retention  
configuration.

```
REPORT OBSOLETE;  
REPORT OBSOLETE REDUNDANCY 3;
```

Listing obsolete  
backups.

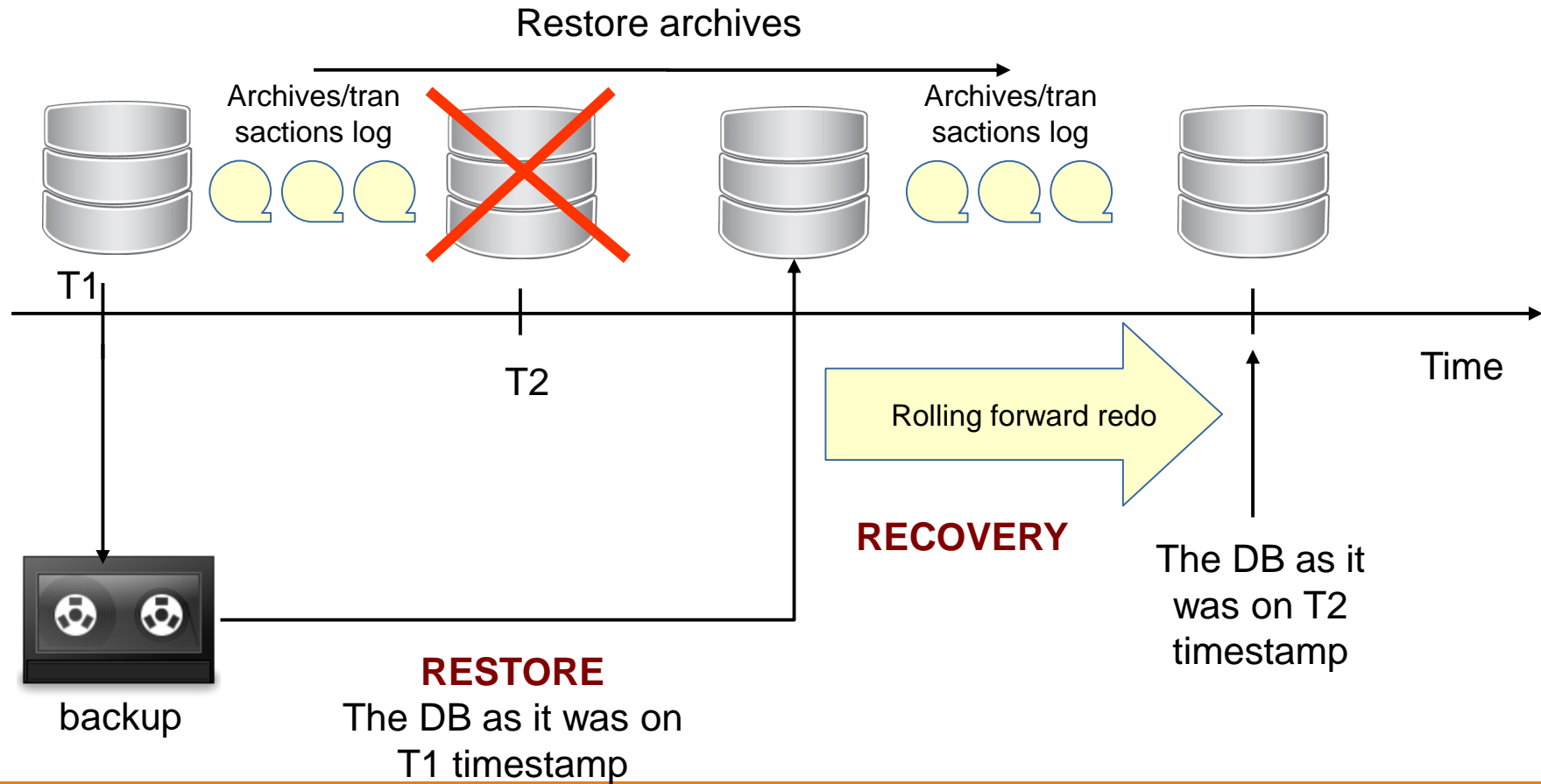
```
DELETE OBSOLETE;  
DELETE OBSOLETE REDUNDANCY 4;
```

Delete obsolete  
backups.

```
CHANGE BACKUPSET 123 KEEP UNTIL  
  'SYSDATE+180';  
CHANGE DATAFILECOPY  
'/tmp/control01.ctl' KEEP FOREVER;
```

Explicit retention  
settings.

# Restore vs. Recovery



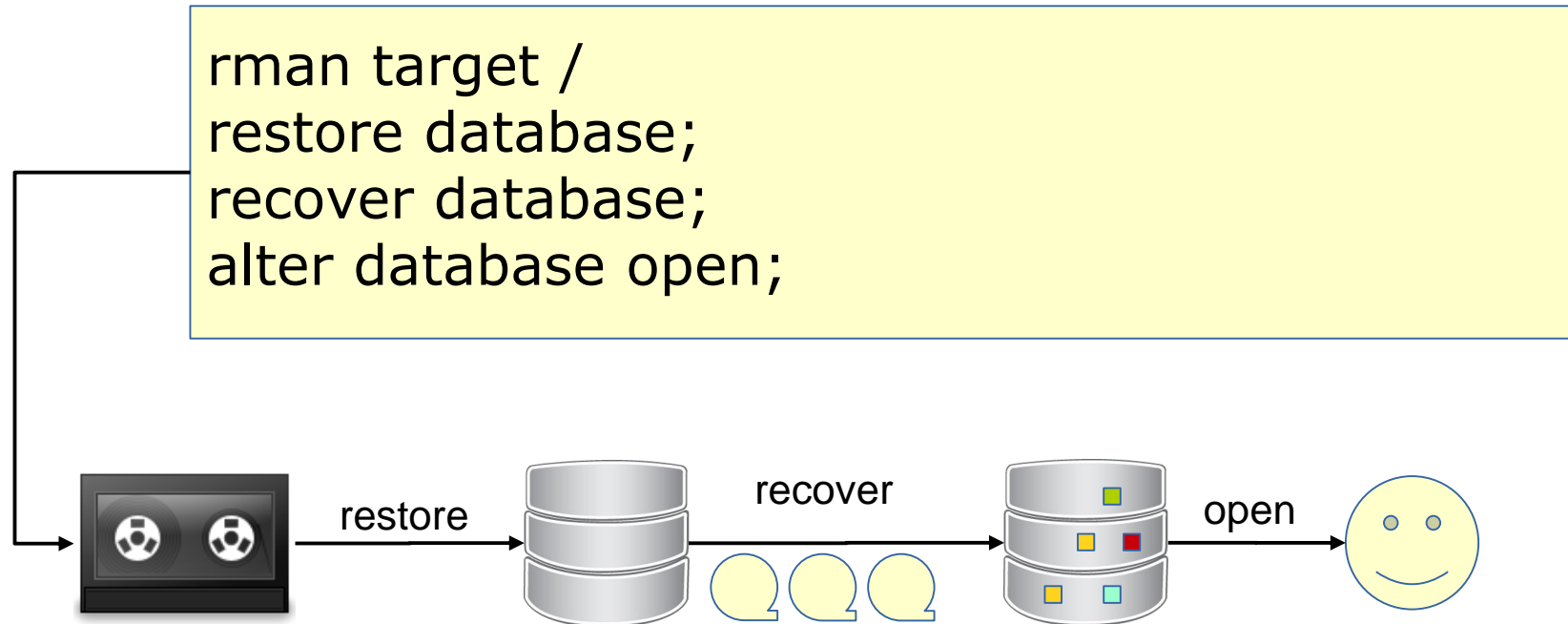
The  
recovery  
may be:

- **Complete:** when all the changes from the redo files (offline and online) are applied.
- **Incomplete:** when the database is recovered using a partial rolling forward from the redolog stream, ending up with a image of the database as it was on a specific time in the past, discarding all the other changes after that time (changes which are recorded into the “tail” of redolog stream).

## Recovery Types

# The Complete Recovery Using RMAN

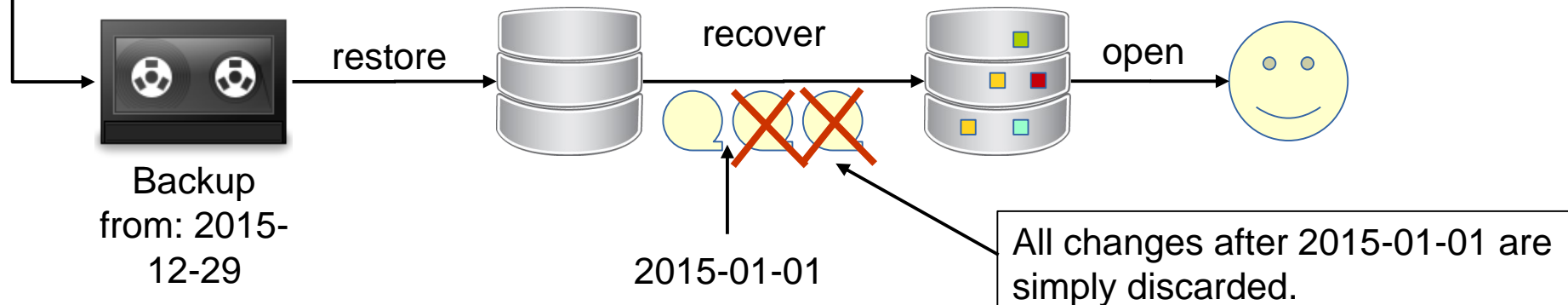
The Oracle instance is in the mount state:



# The Incomplete Recovery Using RMAN

The Oracle instance is in the “MOUNT” state:

```
rman target /  
run {  
  set until time "to_date('2015-01-01', 'yyyy-mm-dd')";  
  restore database;  
  recover database;  
  alter database open resetlogs;  
}
```



# That's all folks!

THANK YOU AND SEE YOU NEXT WEEK...