Gestió d'usuaris i permisos. Seguretat

Seguretat

Autenticitat
No repudi
+
Autorització
Comptabilitat

Confidencialitat
Encriptació
Auditoria

Integritat
Restriccions
Transaccions

Disponibilitat
Copies de seguretat
Recuperació

+

Normativa vigent en matèria de dades personals

LOPDGDD - RPGD (GDPR)

CCN-CERT BP/22

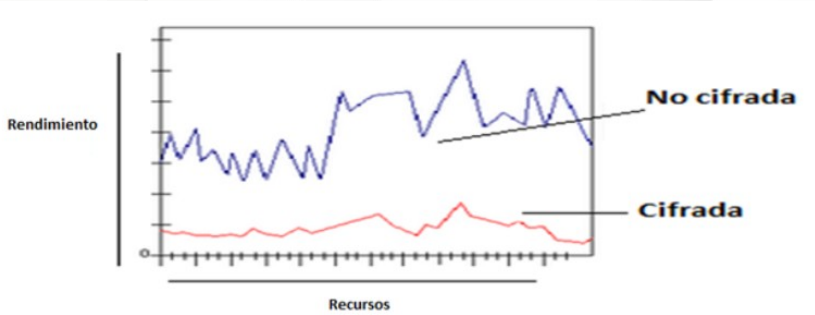
Encriptació

Perquè xifrar?

- Seguretat interna
- Exfiltració de dades
- Compliment llei (RGPD, ...)
- Normativa

Perquè no xifrar?

- Rendiment
- Comoditat
- Operativitat



S'ha de buscar l'equilibri !!

Encriptació (en Oracle)

Mitjançant funcions

- DBMS_CRYPTO.ENCRYPT()
- DBMS_CRYPTO.DECRYPT()
- DBMS_CRYPTO.Hash()
- DBMS_CRYPTO.MAC() -- Hash xifrat --

«manual»

Encriptació transparent

- TDE (Transparent Data Encryption)
  - TDE Tablespace encryption
  - TDE Column encryption

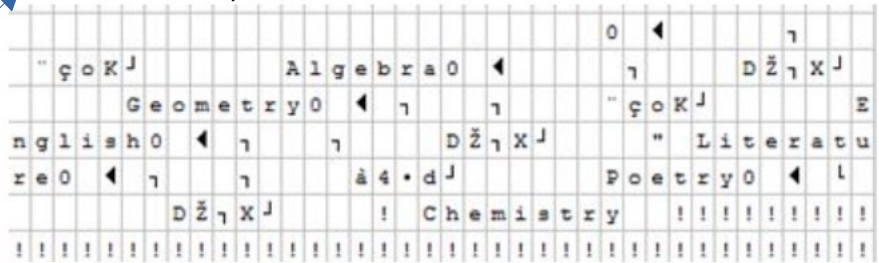
«automàtic»

Encriptació (en Oracle)

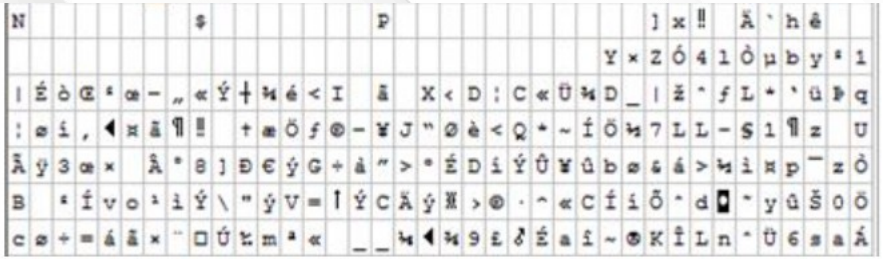
Taula d'exemple

classroomnumber	building	classsubject	classtime
1	2	Algebra	09:00:00.0000000
1	2	Geometry	10:30:00.0000000
2	2	English	09:00:00.0000000
2	2	Literature	10:30:00.0000000
2	2	Poetry	12:00:00.0000000
3	1	Chemistry	10:30:00.0000000

Dades en disc, amb codificació utf o altra



Dades en disc, amb TDE



Encriptació (en Oracle)

DBMS_CRYPTO.ENCRYPT()

```
DBMS_CRYPTO.ENCRYPT(
   src IN RAW,
   typ IN PLS_INTEGER,
   key IN RAW,
   iv  IN RAW  DEFAULT NULL)
 RETURN RAW;
```

paquet DBMS_CRYPTO

Què és un paquet d'Oracle ??

```
DBMS_CRYPTO.RANDOMBYTES (
   number_bytes IN POSITIVE)
 RETURN RAW;
```

Millor utilitzar el paquet dbms_random

Quants hi ha ??

Manipular funcions

Varchar2 to raw : `UTL_I18N.STRING_TO_RAW (string, 'AL32UTF8');`

Raw to varchar2 : `UTL_I18N.RAW_TO_CHAR (data, 'AL32UTF8');`

Guardar raw en string

RAWTOHEX

UTL_ENCODE.BASE64_ENCODE

Prova-ho en SQL Developer
Observa com funciona

EXEMPLE:

```
SQL> select dbms_random.value(1,20) from dual;
```

Encriptació (en Oracle)

DBMS_CRYPTO.DECRYPT()

```
DBMS_CRYPTO.DECRYPT(
   src IN RAW,
   typ IN PLS_INTEGER,
   key IN RAW,
   iv  IN RAW DEFAULT NULL)
 RETURN RAW;
```

El tipus RAW en Oracle representa cadenes binaries d'amplada variable expressades en bytes. (max 2000 bytes) RAW(2000)

Açò ho vorem millor en la unitat 04 (part procediments)

S'utilitza en procediments, funcions i triggers

Encriptació (en Oracle)

DBMS_CRYPTO.Hash() i DBMS_CRYPTO.MAC()

```
DBMS_CRYPTO.Hash (
   src IN RAW,
   typ IN PLS_INTEGER)
 RETURN RAW;

DBMS_CRYPTO.MAC (
   src IN RAW,
   typ IN PLS_INTEGER,
   key IN RAW)
 RETURN RAW;
```

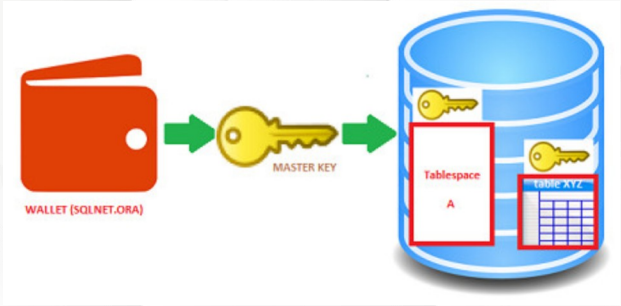
Com emmagatzemar contrasenyes en bases de dades correctament !!

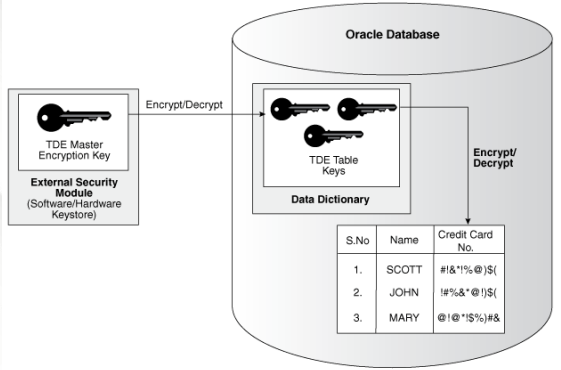
EXEMPLE:

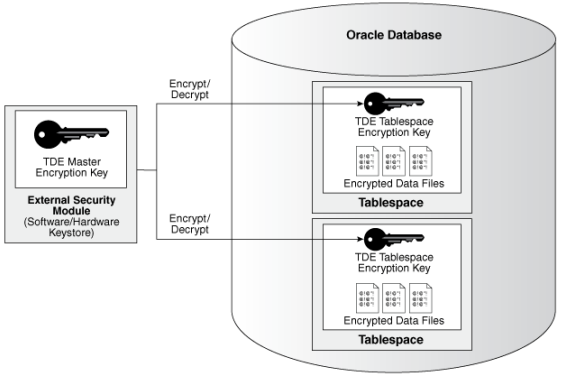
```
SQL> select dbms_crypto.hash('1AAF445C',1) from dual;
```

Prova-ho en SQL Developer
Observa com funciona

Encriptació transparent TDE







Necessitarem una **TDE Keystore Architecture**
- Un lloc on guardar les claus (wallet)
- Una clau mestra. TDE Master Encryption Key
- Unes claus per als tablespaces (cas de tablespaces)
  TDE Tablespace Encryption Key
- Unes claus per a les taules (cas de columnes)
  TDE Table Keys

Auditoria

L'auditoria sempre té a veure amb la rendició de comptes i, amb freqüència, es realitza per a protegir i preservar la privacitat de la informació emmagatzemada en bases de dades. L'auditoria permet veure i gestionar l'activitat en un SGBD (permet realitzar un seguiment de les accions específiques dels usuaris en la base de dades, com les actualitzacions de taules, les consultes de lectura, les assignacions de privilegis d'usuari i altres)

Es necessita privilegi:
`grant audit system to usuari;`
O rol de `audit_admin`
o `audit_viewer`

* Auditoria tradicional: Comandos `audit` i `noaudit`

* Auditoria de grau fi: Funcions del paquet `dbms_fga` Fine Grained Auditing

* Auditoria unificada: Comandos `audit policy <regla>`

* Registre d'auditoria en el DD o en SO

Auditoria tradicional (oracle)

AUDIT_TRAIL

1er Activar Auditoria

Vore estat d'auditoria

```
Select name,value from v$parameter where name like 'audit_trail';
```

Canviar estat d'auditoria

```
ALTER SYSTEM SET audit_trail = 'db' SCOPE=SPFILE;
```

```
none: no se recopilen dades
db: les dades van al DD, taula sys.aud$
os: les dades van al so
xml: les dades van al directori definit en 'audit_file_dest'

show parameter audit;
```

Auditoria tradicional: Comandos audit i noaudit

2on Que auditar ??

AUDIT (Traditional Auditing)

Comandos audit , noaudit

```
AUDIT privilegi     NOAUDIT privilegi
AUDIT grup_priv     NOAUDIT grup_priv
AUDIT operació      NOAUDIT operació
```

On vore les regles d'auditoria actives

```
DD-Regles
dba_stmt_audit_opts;
```

EXEMPLE: privilegi

```
SQL> audit create table;
SQL> audit drop table;
SQL> audit truncate table;
```

EXEMPLE: grup_priv

```
SQL> audit table;
SQL> audit session;
SQL> audit user;
SQL> audit procedure;
.....
```

EXEMPLE: operació

```
SQL> audit select table;
SQL> AUDIT SELECT TABLE, UPDATE TABLE
    BY hr, oe;
SQL> AUDIT DELETE ANY TABLE;
```

Auditoria tradicional: Comandos audit i noaudit

3er On es guarden els resultats ??

Comandos audit , noaudit : Exemple

(1) Des de SYS (o SYSTEM) en SQL Developer

```
SQL> create user prova1 identified by 1234;
SQL> grant connect, resource to prova1;
SQL> audit session;
```

On vore els events auditats

DD-Accions guardades
DBA_AUDIT_SESSION
DBA_AUDIT_OBJECT

(2) Des de CMD

```
C:\users\usuari1> sqlplus prova1/1234@localhost/pdb1
SQL> exit
C:\users\usuari1> sqlplus prova1/1234@localhost/pdb1
```

(3) Des de SYS (o SYSTEM) en SQL Developer

```
SQL> select * from dba_audit_session order by timestamp;
```

Auditoria tradicional: Comandos audit i noaudit

Comandos audit , noaudit : **Exemple**

(1) Des de SYS en SQL Developer

```
SQL> audit user;
```

DD-Accions guardades
DBA_AUDIT_SESSION
DBA_AUDIT_OBJECT

(2) Des de SYSTEM en SQL Developer

```
SQL> create user prova2 identified by 1234;
SQL> grant connect, resource to prova2;
SQL> create user prova3 identified by 1234;
SQL> grant connect, resource to prova3;
```

(3) Des de SYS en SQL Developer

```
SQL> select * from dba_audit_object order by timestamp;
SQL> select * DBA_COMMON_AUDIT_TRAIL;
```

Auditoria de grau fi. FGA Fine Grained Auditing

paquet DBMS_FGA

```
DBMS_FGA.ADD_POLICY (
   object_schema      =>  'rrhh',
   object_name        =>  'emp',
   policy_name        =>  'mypolicy1',
   audit_condition    =>  'id_dpto=50 and comisio>0',
   audit_column       =>  'dni,comisio,salari',
   handler_schema     =>   NULL,
   handler_module     =>   NULL,
   enable             =>   TRUE,
   statement_types    =>  'INSERT, UPDATE, DELETE, SELECT',
   audit_trail        =>   DBMS_FGA.XML + DBMS_FGA.EXTENDED,
   audit_column_opts  =>   DBMS_FGA.ANY_COLUMNS);

DBMS_FGA.DISABLE_POLICY (object_schema => 'rrhh',object_name => 'emp', policy_name => 'mypolicy1');

DBMS_FGA.ENABLE_POLICY (object_schema => 'rrhh',object_name => 'emp',
                        policy_name => 'mypolicy1', enable => TRUE/FALSE  );

DBMS_FGA.DROP_POLICY (object_schema => 'rrhh',object_name => 'emp', policy_name => 'mypolicy1');
```

XML o DB

Auditoria de grau fi. FGA Fine Grained Auditing

La auditoria de grau fi, fa server les vistes del DD

DD-Regles
DBA_AUDIT_POLICIES
DBA_AUDIT_POLICY_COLUMNS

DD-Accions guardades
SYS.FGA_LOG$

DD-Configuracions
DBA_FGA_AUDIT_TRAIL
CDB_FGA_AUDIT_TRAIL

Auditoria unificada

El registre d'auditoria unificat, que resideix en una taula de només lectura, fa que aquesta informació estiga disponible en un format uniforme en una vista del diccionari de dades i està disponible tant en entorns d'instància única com en Oracle Database Real Application Clústers.
A més de l'usuari SYS, els usuaris als quals se'ls han atorgat els rols AUDIT_ADMIN i AUDIT_VIEWER poden gestionar/consultar aquestes vistes

L'Auditoria Unificada està present des de la versió 12c

L'Auditoria tradicional, conviu amb la Unificada. Es poden fer servir les dos

L'Auditoria tradicional està 'obsoleta' en la versió 21c, però encara pot ser utilitzada

Per defecte, esta actiu el model ***Mixed Mode Auditing***

En la versió 23, l'Auditoria tradicional ja no podrà ser utilitzada. Sols la Unificada

Auditoria unificada

AUDIT POLICY (Unified Auditing)

```
CREATE AUDIT POLICY dml_pol
  ACTIONS DELETE on hr.employees,
          INSERT on hr.employees,
          UPDATE on hr.employees,
          ALL on hr.departments;

AUDIT POLICY dml_pol;

NOAUDIT POLICY dml_pol;

ALTER AUDIT POLICY dml_pol ......;

DROP AUDIT POLICY dml_pol;
```

Exemples

```
CREATE AUDIT POLICY table_pol
  PRIVILEGES CREATE ANY TABLE, DROP ANY TABLE;

CREATE AUDIT POLICY read_dir_pol
  ACTIONS READ ON DIRECTORY bfile_dir;

CREATE AUDIT POLICY read_dir_pol ACTIONS ALL;

CREATE AUDIT POLICY dp_actions_pol
  ACTIONS COMPONENT = datapump IMPORT;

CREATE AUDIT POLICY local_table_pol
  PRIVILEGES CREATE ANY TABLE, DROP ANY TABLE
  CONTAINER = CURRENT;

CREATE AUDIT POLICY common_role1_pol
  ROLES c##role1    CONTAINER = ALL;
```

Auditoria Unificada (Exemple)

-Mixed Mode Auditing
-Pure Unified Auditing

(1) Des de SYS en una PDB amb SQL Developer

```
SQL> CREATE AUDIT POLICY table_pol2 PRIVILEGES CREATE ANY TABLE, DROP ANY TABLE;
SQL> AUDIT POLICY table_pol2;
Select * from AUDIT_UNIFIED_POLICIES where oracle_supplied='NO';
```

DD-Regles
AUDIT_UNIFIED_POLICIES;

(2) Des de SYSTEM en una PDB amb SQL Developer

```
SQL> create table prueba10
     (id number primary key, nom varchar2(30) ) ;
```

Des de USUARI1 en una PDB amb SQL Developer

```
SQL> create table prueba20
     (id number primary key, nom varchar2(30) ) ;
```

(3) Des de SYS en una PDB amb SQL Developer

```
SQL> select * from unified_audit_trail;
SQL> select dbusername,oject_schema,sql_text,unified_audit_policies
     from unified_audit_trail order by event_timestamp desc;
```

DD-Accions guardades
unified_audit_trail

Auditoria Unificada (Exemple)

-Mixed Mode Auditing
-Pure Unified Auditing

(1) Des de SYS en una PDB amb SQL Developer

```
SQL> CREATE AUDIT POLICY table_pol3 ACTIONS CHANGE PASSWORD;
SQL> AUDIT POLICY table_pol3;

Select * from AUDIT_UNIFIED_POLICIES where oracle_supplied='NO';
```

DD-Regles
AUDIT_UNIFIED_POLICIES;

(2) Des d'usuari prova1 en una PDB amb SQL Developer
password (Ctrl + Enter)
-- canviem password, vella per nova.

Prova-ho en SQL Developer
Observa com funciona

(3) Des de SYS en una PDB amb SQL Developer

```
SQL> select * from unified_audit_trail;
SQL> select dbusername,oject_schema,sql_text,unified_audit_policies
     from unified_audit_trail order by event_timestamp desc;
```

DD-Accions guardades
unified_audit_trail

Autenticitat
No repudi
+
Autorització
Comptabilitat

Confidencialitat
Encriptació
Auditoria

Integritat
Restriccions
Transaccions

Disponibilitat
Copies de seguretat
Recuperació

+

Normativa vigent en matèria de dades personals

LOPDGDD - RPGD (GDPR)

RI – Restriccions d'Integritat

Les restriccions d'integritat proporcionen un mitjà d'assegurar que les modificacions fetes a la base de dades pels usuaris autoritzats no provoquen la pèrdua de la consistència de les dades. Per tant, les restriccions d'integritat protegeixen la base de dades contra els danys accidentals

En el context de les bases de dades, les "restriccions d'integritat" es refereixen a regles específiques que s'implementen per a garantir la precisió i coherència de les dades dins d'una base de dades relacional

RI – Restriccions d'Integritat

RI de Clau primaria:	PRIMARY KEY
RI de Clau aliena:	FOREING KEY
RI d'unicitat:	UNIQUE
RI de nul·litat:	NOT NULL
RI de domini:	DEFAULT valor CHECK condició +DISPARADORS
RI d'entitat	(implícit, no hi ha dos registres iguals)

```
ALTER TABLE nomtaula DISABLE CONSTRAINT nom_restr ;
ALTER TABLE nomtaula ENABLE CONSTRAINT nom_restr ;
```

RI – Restriccions d'Integritat

(1) Des d'USUARI1 en una PDB amb SQL Developer

```
SQL> create table prueba09
       (id number primary key, nom varchar2(30) not null,
         valor number check (valor>100) ) ;
```

```
user_constraints
dba_constraints
dba_cons_columns
dba_objects
```

(2) Des d'USUARI1 en una PDB amb SQL Developer

```
SQL> insert into prueba09 (id,nom) values (100,'valor1');
SQL> insert into prueba09 (id,nom) values (100,'valor2');
SQL> insert into prueba09 (id,nom) values (200,null);
```

→ Error de RI !!

(3) Des d'USUARI1 en una PDB amb SQL Developer

```
SQL> select table_name,constraint_type,search_condition,status
        from user_constraints;
```

Prova-ho en SQL Developer
Observa com funciona

Control de concurrència - Transaccions

ORACLE
TCL Commands

Una transacció és un conjunt de sentències SQL que s'executen en una base de dades com una **única operació**, confirmant-se o desfent-se tot el conjunt de sentències SQL. La transacció pot quedar finalitzada (amb les sentències apropiades) o implícitament (acabant la sessió).

ORACLE és un sistema de base de dades purament transaccional, de tal forma, que la instrucció BEGIN TRANSACTION no existeix.

En una transacció les dades modificades no són visibles per la resta d'usuaris fins que es confirme la transacció.

Control de concurrència - Transaccions

ORACLE
TCL Commands

Les sentències de finalització de transacció són:

COMMIT; la transacció acaba correctament, es bolquen les dades al tablespace original.
ROLLBACK; es rebutja la transacció. Qualsevol canvi realitzat des que es va iniciar la transacció es desfà, quedant la base de dades en el mateix estat que abans d'iniciar-se la transacció.

Es poden definir punts de control => `SAVEPOINT Nom_punt_control;`
I posteriorment fer

```
COMMIT TO nom_punt_control;
ROLLBACK TO nom_punt_control;
```

Control de concurrència - Transaccions

ORACLE
TCL Commands

DML: Aquestes sentències no executen un COMMIT implícit. +CALL, LOCK TABLE i altres

DDL: Oracle Server executa un COMMIT implícit abans i després de cada instrucció DDL, per la qual cosa es confirma la transacció actual +Establir opcions d'auditoria i agregar comentaris al Diccionari de Dades

DCL: Oracle Server executa un COMMIT implícit abans i després de cada sentència DCL

ALTER SESSION i ALTER SYSTEM: Aquestes sentències no executen un COMMIT implícit

Cridades a procediments: Aquestes sentències no executen un COMMIT implícit

Control de concurrència - Transaccions

ORACLE
TCL Commands

Exemple

Obrim 2 sessions (**en SQL*PLUS**) amb usuari1 (dos cmd diferents)

En la primera sessió (1er CMD)

```
SQL> insert into prueba10  (id, nom) values (1000,'valor1 ');
1 row created.
```

En la segon sessió (2on CMD)

```
SQL> select count(*) from prueba10;
COUNT(*)
----------
         0
```

En la primera sessió (1er CMD)

```
SQL> commit;
```

En la segon sessió (2on CMD)

```
SQL> select count(*) from prueba10;
COUNT(*)
----------
         1
```

Prova-ho en SQL Developer
Observa com funciona

Autenticitat
No repudi
+
Autorització
Comptabilitat

Confidencialitat

Encriptació
Auditoria

Integritat

Restriccions
Transaccions

Disponibilitat

Copies de seguretat
Recuperació

+

Normativa vigent en matèria de dades personals

LOPDGDD - RPGD (GDPR)

Recuperació

Eines bàsiques:

- Copies de seguretat
- Diari de transaccions o quadern de bitàcola

✅ És bona idea guardar aquestes eines en discos físics separats dels discos que alberguen les dades de treball.

Còpies de Seguretat

Gestió de CS
- Backup
- Restore
- Recovery (sistema, sgbd)

Tasques del dba
- Definir polítiques de CS
- Definir procediment de recuperació
- Planificar i gestionar simulacres de recuperació

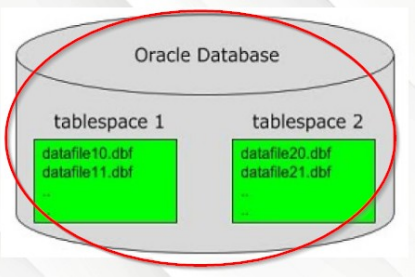
Còpies de Seguretat

Tipus de CS
- Totals o parcials
- Lògica o física
- Completa o incremental
- Online o Offline

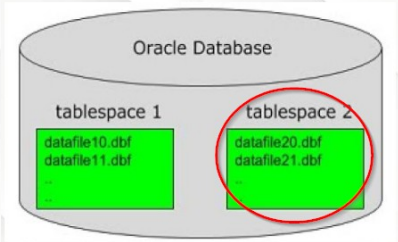
Mecanismes d'ORACLE
- Exportació (exp / imp) (la còpia lògica es guarda en l'equip client)
- Datapump (expdp / impdp) (la còpia lògica es guarda en l'equip servidor)
- RMAN (la còpia física o incremental es guarda en l'equip servidor)

Còpies de Seguretat

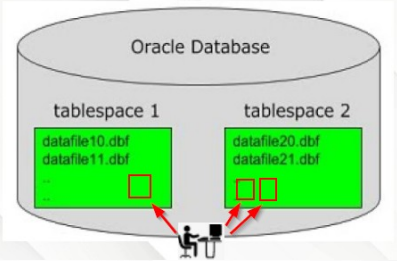
Mode : FULL=Y



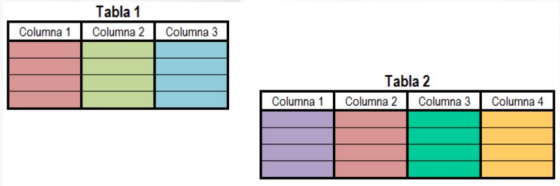
Mode : TABLESPACES= tb1 [,...]



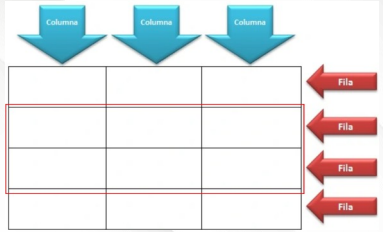
Mode : SCHEMAS= usuari1 [,...]



Mode : TABLE= taula1 [,...]



Mode : QUERY [usuari.taula:] WHERE ....



Còpies de Seguretat

ORACLE DATABASE

En una PDB qualsevol ..

Existeixen en instal·lar

* SYSTEM
* SYSAUX
* UNDO
* TEMP
* USERS

* +Altres TableSpaces creats pels usuaris (+dades)

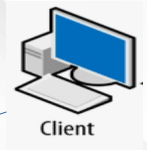
TABLESPACE SYSTEM
Conté:
Usuaris
Privilegis
Rols
Perfils
DD
....

TABLESPACE: USERS
Conté:
Dades -> Taules

Còpies de Seguretat

Exportació (exp / imp) Oracle l'anomena 'Original Export'

- Des de la línia de comandos/terminal
- la còpia lògica es guarda en l'equip client
- Modes: full, user (esquema), tablespace, table, query
- Es pot usar un fitxer de paràmetres `parfile=`



Exemples

```
exp username/password@ipAddress:portNumber/serviceName file=/recovery_area/export/prueba_export.dmp full=yes buffer=1000000
exp scott/tiger@localhost/pdb1 file=orasitescott.dmp tables=(emp,dept) buffer=1000000
exp scott/tiger@localhost/pdb1 file=c:\orasitempleados.dmp tables=emp query=\"where deptno=10\"
exp system/manager@localhost/pdb1 owner='production' file='/oracle10/production.dmp' log='/oracle10/production.log'
```

Si volem fer un **exp** total (full=yes), l'usuari que l'execute necessita el rol EXP_FULL_DATABASE

Per cridar amb sys
exp \'username/password@instance AS SYSDBA\' *parametres*

Còpies de Seguretat

DataPump (expdp / impdp)

- Des de la linea de comandos/terminal (però la còpia s'executa en el servidor)
- Des de dins de l'SGBD amb el paquet DBMS_DATAPUMP
- Des de Enterprise Manager (EM) (deprecated)
- La còpia lògica es guarda en l'equip servidor
- Més ràpid, més rendiment, diversos fils en paral·lel
- Modes: full=Y, eschemas=esquema_1[, esquema_N], tablespaces=, tables=
- QUERY=
- Es pot usar un fitxer de paràmetres `parfile=`

Exemples

```
SQL> create or repace directory dumpdir as 'c:\oracle\dumpdir' ;
SQL> grant read,write on directory dumpdir to username ;

$ expdp username/password@ipAddress:portNumber/serviceName directory=dumpdir dumpfile=export.dmp logfile=fichero.log
$ expdp username/password@.......serviceName directory=dumpdir dumpfile=export.dmp encryption_password=''clave segura''
$ expdp username/password@ipAddress:portNumber/serviceName parfile=parametros.txt
```

Abans.....
S'ha de crear el DIRECTORY en oracle

Còpies de Seguretat

DataPump (expdp / impdp)

- L'usuari que connecta ha de tindre permisos d'accés a **les dades** per fer còpies
- Els fitxers destí no deuen existir
-
- Parameters Available in Data Pump Export Command-Line Mode

Exemples de parfile

```
SCHEMAS=usuari1
DUMPFILE=exp.dmp
DIRECTORY=dirpump
LOGFILE=exp.log
```

```
TABLESPACES=users
DUMPFILE=exp2.dmp
DIRECTORY=dirdump
LOGFILE=exp2.log
```

```
TABLES=usuari1.festius,usuari1.llibres
DUMPFILE=exp3.dmp
DIRECTORY=dirdump
LOGFILE=exp3.log
```

```
QUERY=usuari1.festius:"where data>'1/6/23'"
DUMPFILE=exp4.dmp
DIRECTORY=dirdump
LOGFILE=exp4.log
```

- Per fer una còpia completa es necessita un permís (ROL) concret =>

```
DATAPUMP_EXP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE
```

Còpies de Seguretat

Crear DIRECTORY en oracle

CREATE [OR REPLACE] DIRECTORY directory_name AS 'path_name';

e.g.
En Linux
```
CREATE OR REPLACE DIRECTORY g_vid_lib AS '/video/library/g_rated';
```

En Windows:
```
CREATE OR REPLACE DIRECTORY dircopies AS 'D:\oracle\copseg';
```

Crear un objecte DIRECTORY en oracle

La carpeta ha d'existir !!

You must have the **CREATE ANY DIRECTORY** system privilege to create directories.
When you create a directory, you are automatically granted the READ, WRITE, and EXECUTE object privileges on the directory, and you can grant these privileges to other users and roles. The DBA can also grant these privileges to other users and roles.

Còpies de Seguretat

DataPump (expdp / impdp)

Exemple d'us del paquet DBMS_DATAPUMP


```
declare
      handle number;
begin
      handle:=dbms_datapump.open('EXPORT','SCHEMA');
      dbms_datapump.add_file(handle,'VENTAS.DMP','DUMPDIR');
      dbms_datapump.metadata_filter(handle,'SCHEMA_EXPR','IN (''CLIENT01'')');
      dbms_datapump.set_parallel(handle,4);
      dbms_datapump.start_job(handle);
      dbms_datapump.detach(handle);
end;
```

Procediment anònim

Açò ho vorem millor en la unitat 04 (part procediments)

Còpies de Seguretat

RMAN (Oracle Database Recovery Manager)

- Des de la ferramenta especial RMAN
- Des de dins de l'SGBD amb el paquet DBMS_RCVMAN i DBMS_BACKUP_RESTORE
- La còpia és física i incremental, a nivell de blocs
- Utilitza Servidor de backup
- RMAN necessita el ARCHIVELOG activat
- RMAN necessita privilegi de SYSDBA

Exemples

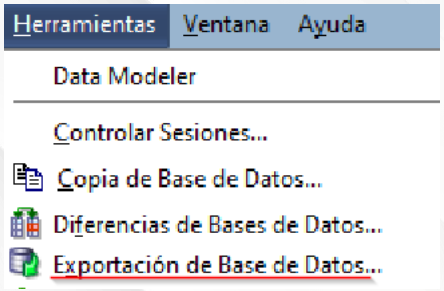
```
$ rman target /
RMAN> show all;
RMAN> backup incremental level 0 tag 'INC_L0' database ;                        //nivell 0 es complet
RMAN> backup incremental level 1 for recover of copy tag 'INC_L0' database ;    // nivell 1 es incremental
RMAN> recover copy of database with tag 'INC_L0' ;
RMAN> backup recovery area ;
```

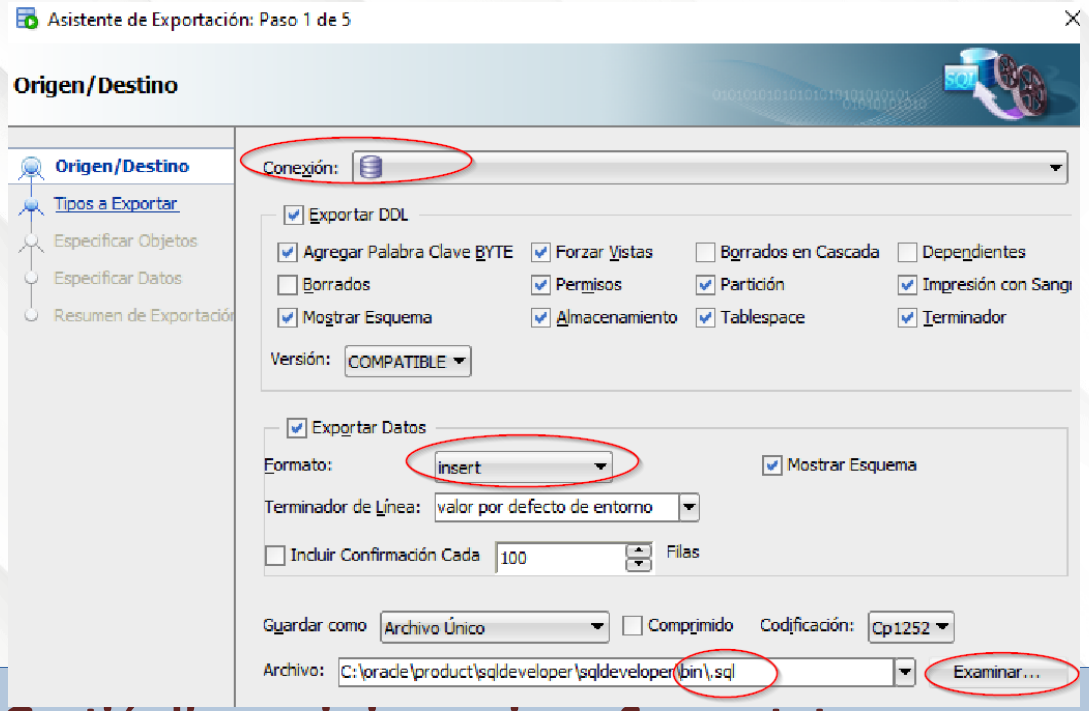
Còpies de Seguretat (oracle)

Aplicació	Total / Parcial	Completa / Incremental	Online / Offline	Lògica / Física
exp / imp	Ambdues	Completes	Ambdues	Lògica
Data Pump	Ambdues	Completes	Ambdues	Lògica
RMAN	Ambdues	Ambdues	Ambdues	Física

Còpies de Seguretat (oracle)

Exportar dades en SQL Developer





Còpies de Seguretat (oracle)

SQL*Loader

SQL*Loader és una utilitat que permet la inserció de dades des d'un arxiu pla a una o més bases de dades.

Durant una sola de les seves execucions és possible omplir múltiples taules amb dades de múltiples arxius, manejar registres d'ample variable o fix, manipular les dades entrants per a tractar amb valors nuls, delimitadors i espais en blanc, obviar registres o encapçalats i reaccionar enfront de fallades del procés de carregat

Autenticitat
No repudi
+
Autorització
Comptabilitat

Confidencialitat
Encriptació
Auditoria

Integritat
Restriccions
Transaccions

Disponibilitat
Copies de seguretat
Recuperació

+

Normativa vigent en matèria de dades personals

LOPDGDD - RPGD (GDPR)

Normativa vigent en matèria de dades personals
LOPDGDD - RPGD (GDPR)

Reglament Europeu (UE) 27 abril 2016
Llei Orgànica 3/2018, 5 de desembre

Drets ARCO
- Accés
- Rectificació
- Cancel·lació
- Oposició

Classificar informació
- Nivell bàsic
- Nivell mig
- Nivell alt

- Document de seguretat actualitzat
- Notificar a AEPD

Normativa vigent en matèria de dades personals
LOPDGDD - RPGD (GDPR)

Paper del SGBD

- Gestió d'usuaris i permisos
- Sistemes de recuperació
- RI
- Encriptació (informació sensible)
- Auditoria

Els procediments han d'estar documentats i supervisats per poder garantir el compliment de la normativa i la llei.

“

Activitat

Investiga que relació té la LOPDGDD amb la GDPR

Que és cadascuna d’elles ?

”