

# Capitolul 6

## Gestiune utilizatori, profiluri, privilegii, roluri - Partea 1 -

# Setari pentru useri

- ☐ Cota pe diverse tablespace-uri ✓
- ☐ Tablespace implicit (default)
- ☐ Tablespace temporar
- ☐ Blocare cont
- ☐ Creare / modificare user
- ☐ Limitari de resurse (profiluri)
- ☐ Privilegii user
- ☐ Roluri

# Mecanismul de autentificare

- Autentificarea userului se poate face in mai multe feluri:
  1. De catre serverul de BD (**database authentication**) – pe baza unui username si a unei parole (cum lucrati de obicei la laborator).
  2. Prin sistemul de operare (**operating system authentication**) – Oracle foloseste informatiile despre user aflate in sistemul de operare si il autentifica, nemaifiind necesara introducerea unui username si a unei parole.
  3. Prin retea (**network authentication**) – folosind servicii de autentificare third-party.

# Cota pe diverse tablespace-uri

- ❑ La crearea unui nou user se poate specifica spatiul pe care acel user il poate 'consuma' din diversele tablespace-uri care exista la acel moment in sistem.
- ❑ Nu se pot asocia cote pe tablespace-urile temporare
- ❑ Implicit userii nu au cote asociate cu nici un tablespace

```
SQL>
SQL>
SQL>
SQL> select * from DBA_TS_QUOTAS;
```

TABLESPACE_NAME	USERNAME	BYTES	MAX_BYTES	BLOCKS	MAX_BLOCKS	DRO
BD_DATA	STUD1	196608	10485760	24	1280	NO
BD_DATA	UBD1	196608	10485760	24	1280	NO
BD_DATA	UBD2	196608	10485760	24	1280	NO
SYSAUX	APPQOSSYS	0	-1	0	-1	NO
SYSAUX	FLows_FILES	0	-1	0	-1	NO
SYSAUX	SYSMAN	95092736	-1	11608	-1	NO
SYSAUX	OLAPSYS	7667712	-1	936	-1	NO
BD_DATA	DMUSER	0	10485760	0	1280	NO
BD_DATA	STUD2	196608	10485760	24	1280	NO

```
9 tnregistrari selectate.
```

```
SQL> _
```

SQL>  
SQL>  
SQL>  
SQL>  
SQL>  
SQL>  
SQL>  
SQL>  
SQL>

SQL> CONNECT STUD1/student

Conectat.

SQL> SELECT \* FROM USER\_TS\_QUOTAS;

TABLESPACE_NAME	BYTES	MAX_BYTES	BLOCKS	MAX_BLOCKS	DRO
USERS	0	0	0	0	NO
BD_DATA	196608	10485760	24	1280	NO

SQL>

# Cota - cont

- ❑ Asignarea unei cote pentru un user intr-un tablespace are urmatoarele efecte:
  - Userii care au privilegiul de a crea obiecte pot crea acele obiecte in tablespace-ul respectiv.
  - Oracle limiteaza spatiul pe care acele obiecte il pot ocupa in tablespace-ul specificat la cat spune cota alocata.
- ❑ Se poate inhiba pentru un user posibilitatea de creare de noi obiecte intr-un anumit tablespace prin setarea unei cote egale cu 0

# Cota - cont

- Cand cota unui user este modificata la o valoare mai mica decat spatiul ocupat la acel moment de acel user in acel tablespace (inclusiv la setarea unei cote egala cu 0) obiectele existente nu se sterg dar:
  - Nu se mai pot crea noi obiecte
  - Obiectele existente nu mai pot creste in dimensiune (dar pot scadea)



# Setari pentru useri

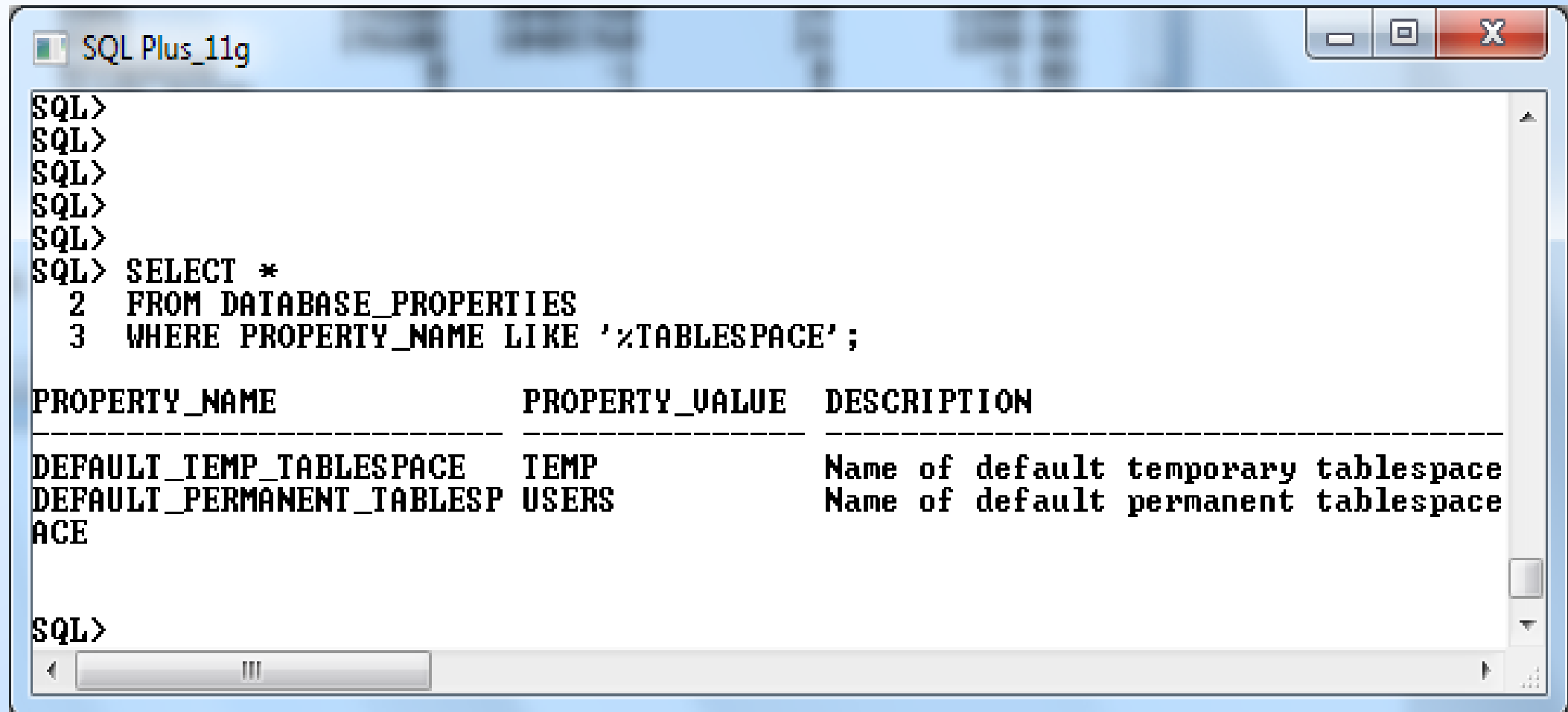
- ☐ Cota pe diverse tablespace-uri ✓
- ☐ Tablespace implicit (default) ✓
- ☐ Tablespace temporar
- ☐ Blocare cont
- ☐ Creare / modificare user
- ☐ Limitari de resurse (profiluri)
- ☐ Privilegii user
- ☐ Roluri

# Tablespace implicit (default)

- ❑ Orice user are un tablespace implicit (default).
- ❑ Acest tablespace definește locația unde sunt create obiectele (segmentele) userului în absența specificării unui tablespace în momentul creării acelui obiect.
- ❑ La crearea unui nou user se poate opțional specifica tablespace-ul implicit al userului (cel permanent și cel temporar).
- ❑ Dacă nu se specifică aceste informații userul va moșteni valorile implicite ale bazei de date.

# Tablespace implicit (default)

- ❑ Aflarea tablespace-urilor implicite se poate face din DATABASE\_PROPERTIES:



```
SQL>
SQL>
SQL>
SQL>
SQL>
SQL> SELECT *
      2  FROM DATABASE_PROPERTIES
      3  WHERE PROPERTY_NAME LIKE '%TABLESPACE';
```

PROPERTY_NAME	PROPERTY_VALUE	DESCRIPTION
DEFAULT_TEMP_TABLESPACE	TEMP	Name of default temporary tablespace
DEFAULT_PERMANENT_TABLESPACE	USERS	Name of default permanent tablespace

```
SQL>
```

# Tablespace implicit (default)

- ❑ In Oracle valoarea de default este tablespace-ul SYSTEM, ceea ce nu este foarte bine in cazul in care userul creaza noi obiecte.
- ❑ Este bine sa se creeze un tablespace permanent si unul temporar iar userii uzuali sa le aiba pe acestea ca implicite.
- ❑ Userii de sistem (SYS, SYSTEM) trebuie insa sa ramana cu tablespace implicit SYSTEM.
- ❑ Tablespace-urile default ale unui user se pot schimba si dupa crearea userului, cu ALTER USER.

# Setari pentru useri

- ☐ Cota pe diverse tablespace-uri ✓
- ☐ Tablespace implicit (default) ✓
- ☐ Tablespace temporar ✓
- ☐ Blocare cont
- ☐ Creare / modificare user
- ☐ Limitari de resurse (profiluri)
- ☐ Privilegii user
- ☐ Roluri

# Tablespace temporar

- ❑ In cazul in care sunt folosite segmente temporare (de exemplu sunt executate cereri care implica sortari de date voluminoase), acestea sunt stocate:
  - In tablespace-ul implicit (default) daca nu s-a specificat un tablespace temporar la crearea userului
  - In tablespace-ul temporar daca acesta a fost specificat
- ❑ Si acest tablespace se poate specifica si ulterior, prin **ALTER USER**

# Aflarea valorilor implicite

- Pentru a afla valorile implicite ale unui user existent se poate interoga si vederea DBA\_USERS:

```
SQL> select USERNAME, DEFAULT_TABLESPACE,  
        TEMPORARY_TABLESPACE  
from DBA_USERS  
where USERNAME='stud1' ;
```

USERNAME	DEFAULT_TABLESPACE	TEMPORARY_TABLESPACE
stud1	USERS	TEMP

```
SQL>
```

# Setari pentru useri

- ☐ Cota pe diverse tablespace-uri ✓
- ☐ Tablespace implicit (default) ✓
- ☐ Tablespace temporar ✓
- ☐ Blocare cont ✓
- ☐ Creare / modificare user
- ☐ Limitari de resurse (profiluri)
- ☐ Privilegii user
- ☐ Roluri



# Blocare cont

- ❑ Un cont poate fi configurat sa se blocheze dupa un anumit numar de incercari de intrare fara succes.
- ❑ Contul se poate debloca dupa un anumit interval de timp, specificat, sau de catre administratorul bazei de date.
- ❑ De asemenea, parola de la creare se poate seta ca expirata, fortand astfel schimbarea parolei (de user sau de administratorul bazei de date) inainte de a putea intra in sistem.

# Obiectele unui user

- ❑ Ele formeaza 'schema' acelui user
- ❑ Pot fi:
  - ❑ Tabele (cu declansatori si constrangeri asociate)
  - ❑ Indecsi
  - ❑ Vederi
  - ❑ Secvente
  - ❑ Subprograme stocate
  - ❑ Sinonime
  - ❑ Tipuri definite de user
  - ❑ Legaturi (database links – prin ele se pot accesa obiecte din alte baze de date)

# Setari pentru useri

- ☐ Cota pe diverse tablespace-uri ✓
- ☐ Tablespace implicit (default) ✓
- ☐ Tablespace temporar ✓
- ☐ Blocare cont ✓
- ☐ Creare / modificare user ✓
- ☐ Limitari de resurse (profiluri)
- ☐ Privilegii user
- ☐ Roluri

# Crearea unui nou user

- ❑ La crearea unui nou user se stabilesc mai intai urmatoarele:
  - Numele, parola si metoda de autentificare pentru acel user
  - Tablespace-urile care pot fi utilizate de catre acesta
  - Cota alocata userului pentru fiecare tablespace
  - Tablespace-ul implicit si cel temporar
- ❑ Se emite comanda CREATE USER care foloseste informatiile de mai sus
- ❑ Se adauga apoi privilegii si roluri pentru user.

# Sintaxa

```
CREATE USER username
IDENTIFIED {BY password
           | EXTERNALLY
           | GLOBALLY AS 'external_name' }
[ DEFAULT TABLESPACE tablespace ]
[ TEMPORARY TABLESPACE tablespace ]
[ QUOTA int {K | M} ON tablespace ]
[ QUOTA UNLIMITED ON tablespace ]
[ PROFILE { profile_name | DEFAULT } ]
[ PASSWORD EXPIRE ]
[ ACCOUNT {LOCK|UNLOCK} ]
```

# Detalii

```
IDENTIFIED {BY password  
            | EXTERNALLY ...  
            | GLOBALLY ...}
```

- ❑ Aceasta clauza spune modul de autentificare pentru acest user:
- ❑ BY password arata ca este un user local care trebuie sa specifice username si parola la login,
- ❑ EXTERNALLY indica un user extern, autentificat fie prin sistemul de operare fie prin servicii third party
- ❑ GLOBALLY arata ca este un user global, autentificat prin 'directory services'

# Detalii

[ **DEFAULT TABLESPACE** *tablespace* ]

- ❑ Aceasta clauza specifica tablespace-ul default (implicit)

[ **TEMPORARY TABLESPACE** *tablespace* ]

- ❑ Aceasta clauza specifica tablespace-ul pentru segmente temporare

[ **QUOTA** *int* {**K** | **M**} **ON** *tablespace* ]

- ❑ Aceasta clauza specifica valoarea cotei pe un anumit tablespace in bytes / KB / MB.

[ **QUOTA UNLIMITED** **ON** *tablespace* ]

- ❑ Aceasta clauza specifica faptul ca nu este fixata o limita superioara pentru cota pe acel tablespace (bineinteles segmentele userului nu pot depasi spatiul existent acolo)

# Detalii

[ **PROFILE** { *profile\_name* | **DEFAULT** } ]

- ❑ Specifica profilul asociat cu acel user, acesta aratand limitările privind resursele pe care le poate consuma userul. Dacă nu se specifica, va fi asociat un profil implicit (numit **DEFAULT**).

[ **PASSWORD EXPIRE** ]

- ❑ Specifica faptul ca parola este 'pre-expirata', deci DBA sau userul trebuie sa o schimbe inainte de a putea intra in acel cont

[ **ACCOUNT** { **LOCK** | **UNLOCK** } ]

- ❑ Specifica faptul ca acel cont este blocat (**LOCK**), deci necesita deblocare inainte de a fi utilizat. Implicit contul este deblocat (**UNLOCK**) si se poate lucra.



# Exemplu

## ❑ User autentificat prin parola:

```
CREATE USER mihai341C5  
IDENTIFIED BY ec004  
DEFAULT TABLESPACE users  
QUOTA 100M ON test  
QUOTA 500K ON users  
TEMPORARY TABLESPACE temp  
PROFILE clerk;
```

## ❑ Se adauga si niste privilegii:

```
GRANT create session TO mihai341C5;
```

# Restrictii pentru parola

- ❑ In cazul in care autentificarea se face prin parola, aceasta trebuie sa verifice restrictiile de nume Oracle:
  1. Maximum 30 de caractere (pana in versiunea 11g este case-insensitive.)
  2. Incepe cu o litera
  3. Contine litere, cifre sau caracterele speciale:  
# \_ \$

Motivatia acestor restrictii tine de sintaxa comenzii de creare a unui user cu specificarea parolei sau a modificarii parolei sale - aceasta nu se pune intre apostrofi deci trebuie sa respecte regulile pe care le respecta si numele de obiecte.

Exemplu: `CREATE USER U1 IDENTIFIED BY PAROLA_MEA`

# Restrictii pentru parola

❑ Incepand cu versiunea 11g se pot seta parole 'case sensitive':

Exemplu: creare user test2 cu parola Test2

```
CONN / AS SYSDBA
```

```
ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON = TRUE;
```

```
CREATE USER TEST2 IDENTIFIED BY Test2;
```

```
GRANT CONNECT TO test2
```

```
-- autentificare
```

```
SQL> CONNECT TEST2/Test2
```

```
Connected.
```

```
SQL> CONNECT TEST2/test2
```

```
ERROR:
```

```
ORA-01017: invalid username/password; logon denied
```

# Restrictii pentru parola

In cazul in care se seteaza SEC\_CASE\_SENSITIVE\_LOGON pe FALSE literele mari vor fi la fel cu cele mari.

Exemplu: pentru userul anterior:

```
CONN / AS SYSDBA
```

```
ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON = FALSE;
```

```
SQL> CONN TEST2/Test2
```

```
Connected.
```

```
SQL> CONN TEST2/test2
```

```
Connected.
```

```
SQL>
```

# Modificare date user

- ❑ Datele privind autentificarea userului:

```
ALTER USER username  
IDENTIFIED {BY password  
            | EXTERNALLY ...  
            | GLOBALLY ...}  
[ PASSWORD EXPIRE ]  
[ ACCOUNT {LOCK|UNLOCK} ]
```

- ❑ In momentul blocarii unui cont (LOCK), daca userul e logat la acel moment nu va fi afectat. Modificarile date de comanda de mai sus sunt valabile **incepand cu urmatoarea sesiune** de lucru.

```
SQL>
SQL> CONNECT UBD1 AS SYSDBA
Introduce■i parola:
Conectat.
SQL> ALTER USER STUD1 ACCOUNT LOCK;
```

Utilizator modificat.

```
SQL> CONNECT STUD1
Introduce■i parola:
ERROR:
ORA-28000: the account is locked
```

Aten■ie: Nu mai sunte■i conectat la ORACLE.

```
SQL> CONNECT UBD1 AS SYSDBA
Introduce■i parola:
Conectat.
SQL> ALTER USER STUD1 ACCOUNT UNLOCK;
```

Utilizator modificat.

```
SQL> CONNECT STUD1
Introduce■i parola:
Conectat.
SQL> _
```

# Modificare date user - cont

- Datele privind tablespace si cote:

```
ALTER USER username
```

```
[ DEFAULT TABLESPACE tablespace ]
```

```
[ TEMPORARY TABLESPACE tablespace ]
```

```
[ QUOTA int {K | M} ON tablespace ]
```

```
[ QUOTA UNLIMITED ON tablespace ]
```

- La trecerea pe 0 a cotei nu se mai pot crea obiecte si cele existente nu mai pot creste. Exemplu:

```
ALTER USER mihai341c5
```

```
QUOTA 0 ON users;
```

# Modificare date user - cont

- ❑ Observatie: trecerea pe 0 a cotei nu are efect daca userul are asignat rolul (colectia de privilegii) **RESOURCE** deoarece aceasta implica o cota nelimitata.



# Exemplu: stud1 are rolul RESOURCE

SQL Plus\_11g

```
SQL>
SQL> connect stud1/student
Conectat.
SQL> create table t(a number);

Tabelul creat.

SQL> connect ubd1/ubd1
Conectat.
SQL> alter user stud1 quota 0 on USERS;

Utilizator modificat.

SQL> connect stud1/student
Conectat.
SQL> create table t1(b number);

Tabelul creat.

SQL>
```

# Stergere user

- ❑ Stergerea unui user se face cu comanda DROP USER:

**DROP USER nume [CASCADE]**

- ❑ Optiunea CASCADE sterge intai toate obiectele din schema userului respectiv (altfel se obtine un mesaj de eroare).
- ❑ Fara CASCADE se pot sterge doar useri care nu detin nici un obiect in schema proprie.

```
SQL>
SQL>
SQL>
SQL>
SQL>
SQL>
SQL>
SQL> CONNECT UBD1/ubd1
Conectat.
SQL> DROP USER STUD1;
DROP USER STUD1
*
EROARE la linia 1:
ORA-01922: CASCADE trebuie specificat pentru a elimina 'STUD1'
```

```
SQL>
```

# Vederi care se pot utiliza

View	Description
DBA_USERS	Describes all users of the database.
ALL_USERS	Lists users visible to the current user, but does not describe them.
USER_USERS	Describes only the current user.
DBA_TS_QUOTAS , USER_TS_QUOTAS	Describes tablespace quotas for users.
USER_PASSWORD_LIMITS	Describes the password profile parameters that are assigned to the user (vezi partea despre profiluri din curs).
USER_RESOURCE_LIMITS	Displays the resource limits for the current user (vezi partea despre profiluri din curs).
DBA_PROFILES	Displays all profiles and their limits.
RESOURCE_COST	Lists the cost for each resource.
V\$SESSION	Lists session information for each current session. Includes user name.
V\$SESSTAT	Lists user session statistics.
V\$STATNAME	Displays decoded statistic names for the statistics shown in the V\$SESSTAT view.
PROXY_USERS	Describes users who can assume the identity of other users.

# Exemplu

```
SELECT TABLESPACE_NAME, BLOCKS, MAX_BLOCKS, BYTES,  
       MAX_BYTES  
FROM DBA_TS_QUOTAS  
WHERE USERNAME = 'SCOTT';
```

- ❑ Se obtine un rezultat care contine date despre cota userului:

TABLESPACE_NAME	BLOCKS	MAX_BLOCKS	BYTES	MAX_BYTES
DATE	10	-1	20480	-1

- ❑ Valoarea -1 reprezinta cota nelimitata. Restul valorilor reprezinta spatiul ocupat la acel moment.

# Alt exemplu

```
SELECT USERNAME, ACCOUNT_STATUS,  
       TEMPORARY_TABLESPACE  
FROM DBA_USERS
```

□ Se obtine o lista cu starea fiecarui cont (si alte date):

USERNAME	ACCOUNT_STATUS	TEMPORARY_TABLESPACE
-----	-----	-----
SYS	OPEN	TEMP
SYSTEM	OPEN	TEMP
DBSNMP	OPEN	TEMP
SCOTT	OPEN	TEMP

# Setari pentru useri

- ☐ Cota pe diverse tablespace-uri ✓
- ☐ Tablespace implicit (default) ✓
- ☐ Tablespace temporar ✓
- ☐ Blocare cont ✓
- ☐ Creare / modificare user ✓
- ☐ Limitari de resurse (profiluri) ✓
- ☐ Privilegii user
- ☐ Roluri

# PROFIL

- ❑ Profilurile sunt o modalitate prin care se pot limita resursele care pot fi utilizate de un utilizator.
- ❑ Un profil se creaza cu CREATE PROFILE si se asigneaza userului la creare sau ulterior prin comanda ALTER USER.
- ❑ Exista un profil DEFAULT care se asociaza implicit la userii pentru care la creare nu s-a specificat un profil.



# Resurse ale sistemului

Pentru ca aceste limitari de sistem sa fie active trebuie ca parametrul de initializare RESOURCE\_LIMIT sa fie setat pe TRUE – se poate modifica folosind ALTER SYSTEM

- ❑ Numarul maxim de sesiuni concurente pentru user (**SESSIONS\_PER\_USER**)
- ❑ Timp CPU per sesiune (**CPU\_PER\_SESSION**) – masurat in sutimi de secunda.
- ❑ Timp CPU per operatie (**CPU\_PER\_CALL**) – masurat in sutimi de secunda. O operatie este un ciclu parse, execute, fetch.

# Resurse ale sistemului

- ❑ Timpul maxim de conectare masurat in minute (**CONNECT\_TIME**).  
Sesiunile userului sunt inchise de Oracle dupa expirarea acestui timp.
- ❑ Timp maxim de asteptare (**IDLE\_TIME**) – masurat in minute  
- sesiunile vor fi inchise de Oracle dupa expirarea perioadei specificate daca in sesiunea respectiva nu s-a facut nimic (e 'idle'). Atentie: cererile a caror executie este lunga nu intra in aceasta categorie!

# Resurse ale sistemului

- ❑ Numar maxim de blocuri citite per sesiune. Este vorba aici de numarul de blocuri citite de pe disc ***sau*** din memorie. Acest parametru este gandit pentru a limita cererile care fac citiri intensive (**LOGICAL\_READS\_PER\_SESSION**).
- ❑ Numarul maxim de blocuri citite per operatie (call) (**LOGICAL\_READS\_PER\_CALL**).
- ❑ Dimensiunea maxima de memorie ocupata in shared pool – parte a SGA - de o sesiune de lucru – in bytes (**PRIVATE\_SGA**).

# Resurse legate de parola

- ❑ Numarul maxim de incercari eronate de login (**FAILED\_LOGIN\_ATTEMPTS**)
- ❑ Timpul maxim (in zile) cat parola este valida (**PASSWORD\_LIFE\_TIME**)
- ❑ Numarul minim de parole diferite utilizate pana cand o parola poate fi reutilizata (**PASSWORD\_REUSE\_MAX**)
- ❑ Numarul minim de zile dupa care o parola poate fi reutilizata (**PASSWORD\_REUSE\_TIME**)

# Resurse legate de parola

Mai exista si:

- ❑ **PASSWORD\_LOCK\_TIME** : Cate zile se blocheaza contul dupa incercari repetate de login esuate
- ❑ **PASSWORD\_GRACE\_TIME** : Cate zile sunt disponibile pentru a schimba o parola dupa expirarea acesteia
- ❑ **PASSWORD\_VERIFY\_FUNCTION**: bloc (program) PL/SQL utilizat pentru verificarea parolei
- ❑ **SEC\_CASE\_SENSITIVE\_LOGON** : literele mari si cele mici sunt considerate identice sau nu intr-o parola.

# Alte informatii

- ❑ Lista de mai sus nu este exhaustiva.
- ❑ Am dat numele parametrilor pentru ca fiecare in parte se poate modifica ulterior prin comenzi ALTER PROFILE.

# Limitari

- ❑ Daca este atinsa o limita la nivel de sesiune atunci:
  - Fie se afiseaza un mesaj de eroare (de exemplu cand se incearca deschiderea unei noi sesiuni si se depaseste sessions\_per\_user)
  - Fie Oracle deconecteaza userul (sesiunea), de exemplu cand s-a atins durata ei maxima.

# Limitari

□ Daca este atinsa o limita la nivel de operatie (call) atunci:

- Procesarea cererii curente este oprita
- Cererea curenta este revocata (rollback)
- Efectul cererilor anterioare persista
- Userul ramane conectat.



# Lecturi obligatorii

1. Oracle Database Security Guide (v19c) – Capitolele despre gestiune utilizatori, privilegii, profiluri, roluri

<https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/database-security-guide.pdf>

# Sfârșit partea 1