**Erőforrás korlátok, jogosultságok**

A profile erőforrás korlátozások egy halmaza. Minden felhasználóhoz hozzá van rendelve egy profile, amit a felhasználó létrehozásakor lehet megadni (CREATE USER) vagy később megváltoztatni (ALTER USER). Van egy DEFAULT nevű profile is.

CREATE PROFILE prof1 LIMIT

 SESSIONS\_PER\_USER UNLIMITED

 CPU\_PER\_SESSION UNLIMITED

 CPU\_PER\_CALL 3000

 CONNECT\_TIME 45

 LOGICAL\_READS\_PER\_SESSION DEFAULT

 LOGICAL\_READS\_PER\_CALL 1000

 PRIVATE\_SGA 15K

 COMPOSITE\_LIMIT 5000000;

CREATE USER user1 PROFILE prof1;

Az adatbázisbeli profile-ok, és a foganatosított korlátozások a dba\_profiles nevű adatszótárban (katalógusban) vannak tárolva. A korlátozások köre nem bővíthető, csak azokra adható korlátozás, amit az adott verzió ismer.

Egy profile-ban beállított értékek

PASSWORD\_LOCK\_TIME

Egy fiók zároltságának ideje; letelte után automatikusan ismét használható lesz

PASSWORD\_LIFE\_TIME

Jelszó lejárati idő; eltelte után kötelező azt megváltoztatni

Mikor jár le -> DBA\_USERS.expiry\_date

**SELECT username, expiry\_date FROM DBA\_USERS WHERE username=user;**

A lejárt, illetve zárolt fiók nem ugyanazt jelenti -> DBA\_USERS.lock\_date

A zárolt fiók nem használható (csak a zároltság feloldása után), a lejárt fióknak csak a jelszavát kötelező legközelebb megváltoztatni.

CREATE USER (vagy ALTER USER) <user> password expire

-> Első bejelentkezés után kötelező a jelszóváltoztatás

**Jogosultságok**

Rendszer szintű jogosultságok, lásd -> system\_privilege\_map nevű adatszótár

Ebből nem lehet újabbat létrehozni, annyi rendszer jogosultság van, amennyit az adott oracle verzió ismer. Jogosultság adása egy felhasználónak, vagy mindenkinek:

GRANT SELECT ANY DICTIONARY TO bubu;

GRANT CREATE TABLE TO PUBLIC;

A fenti utasításokban a ’bubu’ egy adatbázis felhasználó neve, a ’PUBLIC’ pedig egy speciális kulcsszó, amelynek megadása esetén az adott jogosultságot minden felhasználó megkapja. Az adatbázis felhasználóit a dba\_users nevű adatszótár tartalmazza.

Objektum szintű jogosultságok, lásd -> table\_privilege\_map nevű adatszótár

Ebből sem lehet újabbat létrehozni.

GRANT INSERT ON emp TO bubu;

GRANT SELECT ON emp TO PUBLIC;

Szerepkörök, melyikhez van jelszó megadva? -> dba\_roles nevű adatszótár

Újabb szerepköröket tetszés szerint hozhatunk létre. Egy szerepkör lehet jelszóval védett, vagy anélküli, valamilyen külső szolgáltatás által védett (pl. az op. rendszer védi, lásd lejjebb), globális (ami több adatbázisra vonatkozik és egy Directory Service-ben tárolódik) vagy egy package által védett.

CREATE ROLE role1;

CREATE ROLE role2 IDENTIFIED BY jelszó;

CREATE ROLE role3 IDENTIFIED EXTERNALLY;

CREATE ROLE role4 IDENTIFIED GLOBALLY;

CREATE ROLE role5 IDENTIFIED USING <package>;

Milyen rendszer szintű jogokat kaptak az egyes role-ok es user-ek?

-> dba\_sys\_privs

Role-nak is adhatunk jogot, sőt role-t is, vagyis a jogosultság adás több lépcsős is lehet.

GRANT CREATE TABLE TO role1;

GRANT role1 TO role2;

GRANT role2 TO bubu;

Milyen objektum szintű jogokat kaptak az egyes role-ok es user-ek?

-> dba\_tab\_privs

A rendszer jogosultságokhoz hasonlóan ezt is lehet role-okon keresztül adni.

Milyen role jogokat kaptak az egyes role-ok es user-ek? Mely role-ok vannak

tovább engedélyezve más role-ok és user-ek számára? Melyek egy felhasználó

automatikusan megkapott (default) role-jai?

-> dba\_role\_privs

Ha egy role-t valaki megkapott (GRANT), az még nem biztos, hogy rendelkezik a role jogaival, csak akkor, ha „felveszi” a role-t. Ehhez lehet, hogy jelszóra van szüksége, vagy valamilyen más szolgáltatás ellenőrzi, hogy felveheti-e a szerepkört. A felhasználónak megadott role-ok közül megadható, hogy melyek legyenek az ő default role-jai. Ezeket a bejelentkezéskor automatikusan megkapja, nem kell semmit tennie. A többit fel kell vennie.

ALTER USER bubu DEFAULT ROLE ALL EXCEPT role1;

Az adott pillanatban rendelkezésre álló jogosultságok körének megváltoztatása

a SET ROLE utasítással történik. Pl.

SET ROLE NONE;

SET ROLE ALL;

SET ROLE ALL EXCEPT role1;

SET ROLE role2 IDENTIFIED BY jelszó;

Mely role-ok vannak egy adott pillanatban engedélyezve a session számára?

-> session\_roles

Milyen rendszer szintű jogosultságok vannak engedélyezve egy adott pillanatban

a session számára? -> session\_privs

További lehetőségek:

GRANT update (o1, o2) ON <tábla> TO <user> (update korlátozása oszlopokra)

GRANT <jog> TO <user|role> WITH ADMIN OPTION (továbbadást engedélyezi)

GRANT **<role>** TO <user|role> WITH ADMIN OPTION (módosítást, törlést is enged)

GRANT <jog> ON <obj> TO <user|role> WITH GRANT OPTION (továbbadást engedélyezi)

Ha visszavonjuk, az is elveszti a jogot, aki az illetőtől kapta.

CREATE ROLE role\_nev IDENTIFIED EXTERNALLY (-> init.ora-ban OS\_ROLES=TRUE)

A szerepkört az op. r. ellenőrzi. Unixban általában az /etc/group állományba kerül egy ilyen sor:

ora\_<sid>\_role\_nev\_da:NONE:1:user1, user2

(\_d: default role, \_a: admin option)