

Praktikum 3: Kasutajate haldamine

Teemad

Kasutajate ja rollide loomine.

Õiguste lisamine rollidele.

Kasutajale rollide määramine.

Profiili loomine ja redigeerimine.

Pärast selle praktikumi läbimist üliõpilane oskab luua ja hallata kasutajaid, profiile ja rolle Oracle andmebaasis.

Profiilid

Profiilid määravad piirangud andmebaasi ressurssidele. Kui kasutajale on seatud profiil, siis see kasutaja ei saa ületada profiilis määratud piiranguid. Igal kasutajal võib olla ainult üks profiil. Profiili kustutamisel seatakse seda profiili omavale kasutajale vastavusse profiil *default*.

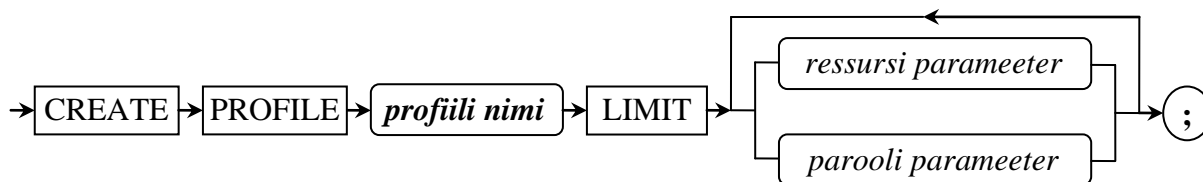
Piiranguid saab jagada kahte ossa:

1. Tuuma ressursside piirangud, mille alla kuuluvad:
 - a. IDLE_TIME – tühjakäigulise sessiooni kestvus, enne kui see suletakse;
 - b. SESSIONS_PER_USER – mitu samaaegselt jooksvat sessiooni on lubatud kasutajale luua;
 - c. ...Selleks, et tuuma ressursside piirangud rakenduksid, on vaja seada initsialiseerimise parameeter RESOURCE_LIMIT tõseks (TRUE).
2. Parooli ressursside piirangud:
 - a. FAILED_LOGIN_ATTEMPTS – lubatud ebaõnnestunud sisselogimise katsete arv, enne kui kasutaja konto lukustatakse;
 - b. PASSWORD_LIFE_TIME – päevade arv, mille möödumisel tuleb parool vahetada;
 - c. PASSWORD_LOCK_TIME – päevade arv, milleks lukustatakse kasutaja konto, pärast seda, kui ületati FAILED_LOGIN_ATTEMPTS parameetriga määratud sisselogimise katsete arv;
 - d. PASSWORD_VERIFY_FUNCTION – PL/SQLis kirjutatud funktsioon kasutaja parooli turvanõuete kontrollimiseks;

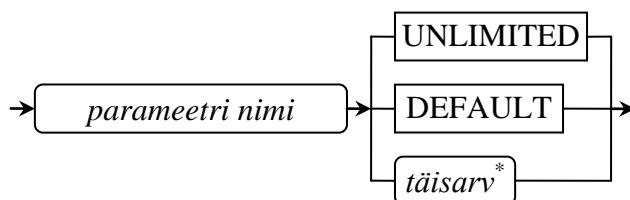
Andmebaasi vaade, mis on seotud profiilidega:

- *dba_profiles* – väljastab kõik profiilid ja nende piirangud;

Profiili loomise süntaks:



Ressursi parameeterlausendil on järgmine kuju:

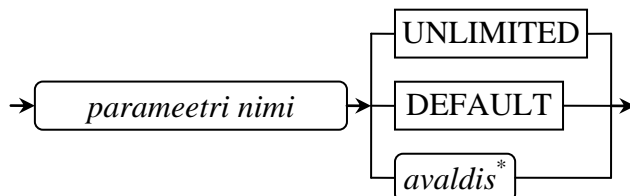


Tuuma ressursside parameetrite nimesid saab vaadata järgmise päringuga:

```
SQL> SELECT resource_name
1 FROM dba_profiles
2 WHERE profile = 'DEFAULT'
3 AND resource_type = 'KERNEL';
```

**PRIVATE_SGA* parameetri puhul kasutatakse täisarvu asemel suuruse lausendit.

Parooli parameeterlausend:

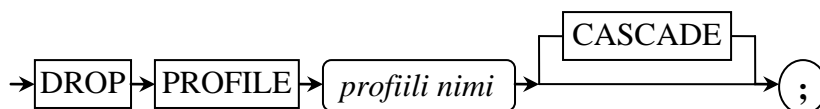


Parooli parameetreid saab vaadata järgmise päringuga:

```
SQL> SELECT resource_name
1 FROM dba_profiles
2 WHERE profile = 'DEFAULT'
3 AND resource_type = 'PASSWORD';
```

**PASSWORD_VERIFY_FUNCTION* parameetri puhul kasutatakse avaldise asemel funktsiooni nime.

Profiili kustutamise süntaks:



Juhul, kui kustutatav profiil on määratud mingile kasutajale, siis profiili ei saa kustutada ilma võtmesõnata CASCADE. Viimane võtab profiili maha kõikidelt kasutajatelt, kellele ta on kustutamise hetkel määratud.

Profiili loomise päringu näidis:

```
SQL> CREATE PROFILE näidis LIMIT
  1 SESSIONS_PER_USER 1
  2 FAILED_LOGIN_ATTEMPTS 3
  3 PASSWORD_LOCK_TIME 1
  4 PASSWORD_LIFE_TIME 7;
```

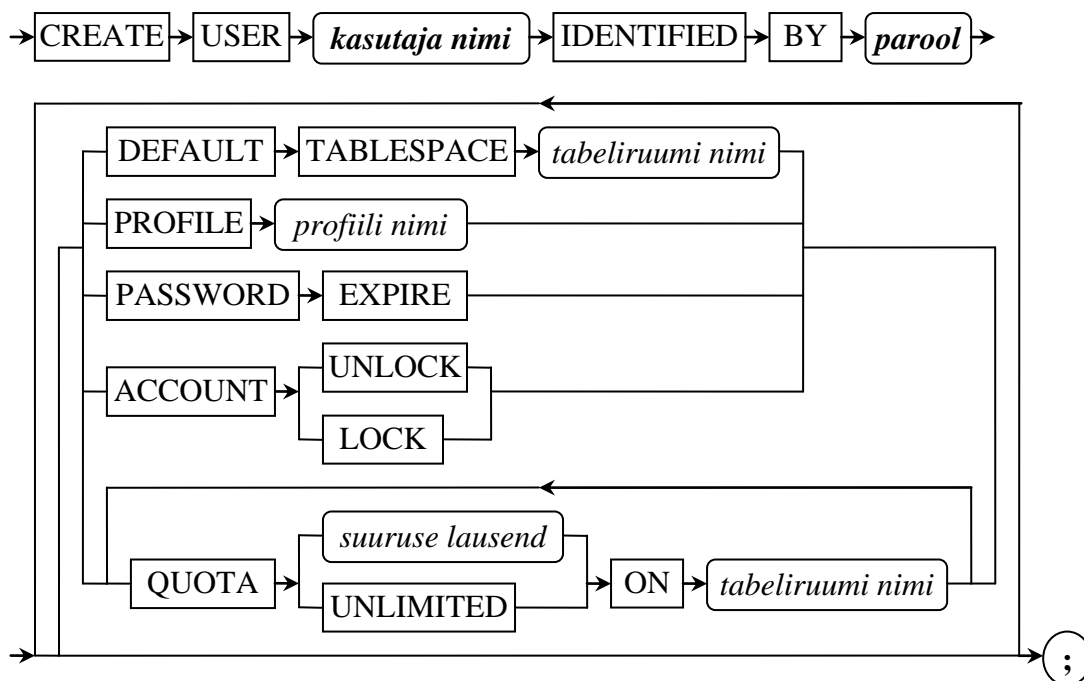
Kasutajad

Kasutajad – on kontod, mille kaudu saab juurdepääsu andmebaasile. Andmebaasi sisse logimiseks peab kasutajal olema CREATE SESSION süsteemiõigus. Kasutajate SYS või SYSTEM kustutamine toob kaasa andmebaasi kahjustuse.

Andmebaasi vaade, mis on seotud andmebaasi kasutajatega:

- *dba_users* – sisaldab informatsiooni kõikide andmebaasi kasutajate kohta.

Kasutaja loomise süntaks



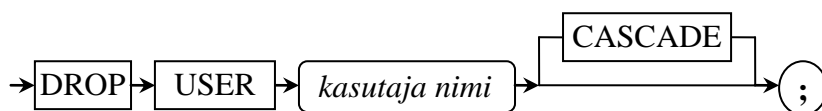
DEFAULT TABLESPACE – määrab kasutaja vaikimisi tabeliruumi;

PASSWORD EXPIRE – sunnib kasutajat järgmisel sisse logimisel parooli vahetama;

ACCOUNT LOCK/UNLOCK – lukustab või võtab kasutaja kontolt lukustuse maha;

QUOTA ... ON ... – võimaldab määrata tabeliruumi kvooti.

Kasutaja kustutamise süntaks:



Võtmesõna **CASCADE** kasutamisel kustutatakse andmebaasist ka kõik kasutajale kuuluvad objektid.

Kasutaja lisamise näidis:

```
SQL> CREATE USER näidis_kasutaja IDENTIFIED BY muuda_sisselogimisel  
 1 DEFAULT TABLESPACE USERS PROFILE näidis  
 2 PASSWORD EXPIRE ACCOUNT UNLOCK QUOTA 3M ON USERS;
```

Rollid

Roll – õiguste kogum, mida saab määrata kasutajatele või teistele rollidele. Roll sisaldab kõiki õigusi, mis on talle antud ja kõik teiste rollide õigused, mis on määratud antud rollile. Uus roll on vaikimisi ilma õigusteta.

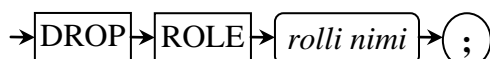
Andmebaasi vaated, mis on seotud rollidega:

- *dba_roles* – kirjeldab kõiki rolle, mis eksisteerivad andmebaasis;
- *dba_role_privs* – rollid, mis on määratud teistele kasutajatele või rollidele.

Rolli loomine süntaks:



Rolli kustutamise süntaks:



Õigused

Oracle õiguste poliitika on järgmine – see mis pole lubatud on keelatud. Õigused võivad olla kahte tüüpi:

1. Süsteemsed – objektide loomine, muutmine, kustutamine:
 - a. **CREATE SESSION**
 - b. **CREATE [ANY] TABLE/SEQUENCE/TRIGGER**
 - c. **DROP USER**
 - d. ...

2. Objektipõhilised – nt. tabeli kirjete selekteerimine, lisamine, kustutamine:

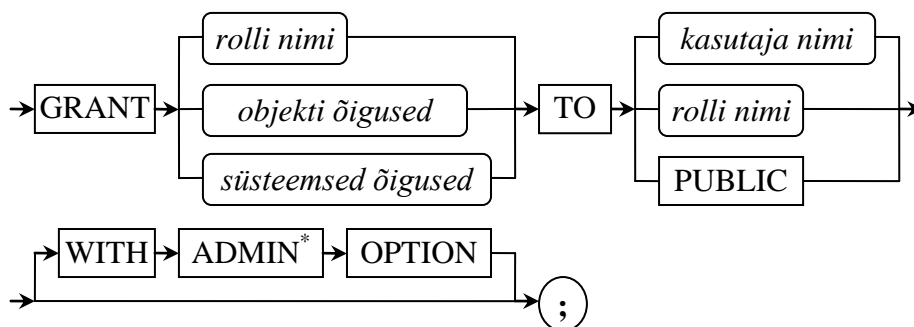
- a. SELECT, UPDATE, INSERT, DELETE
- b. ...

NB! Üksiku veeru uuendamise õiguse tagasivõtmine pole võimalik, selleks tuleb võtta tagasi muutmise õigus tervelt tabelilt. Oracle XE 10.2.0.1.0 ei toeta veergude selektiivset õigust, selle asemel tuleb luua vaade vajalike veergudega ja anda sellele selektiivne õigus kasutajale või rollile.

Andmebaasi vaated, mis on seotud süsteemsete ja objektipõhiliste õigustega:

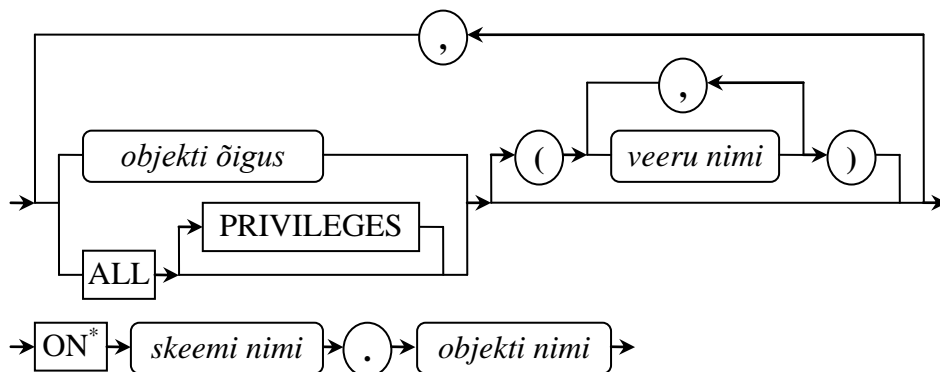
- a) *dba_sys_privs* – kirjeldab süsteemseid õigusi, mis on määratud kasutajatele ja rollidele;
- b) *dba_tab_privs* – kirjeldab kõiki andmebaasi objektipõhiseid õigusi;
- c) *dba_col_privs* – kirjeldab kõiki veergudega seotud objektipõhiseid õigusi andmebaasis;

Õiguste omistamise süntaks:

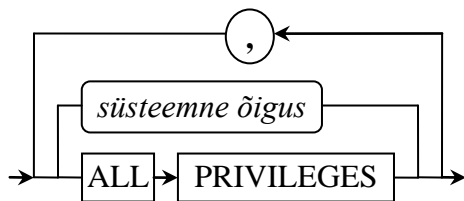


*Objektipõhiste õiguste puhul kasutatakse võtmesõna ADMIN asemel võtmesõna GRANT; GRANT/ADMIN võimaldab kasutajal delegeerida õigust teisele kasutajale;

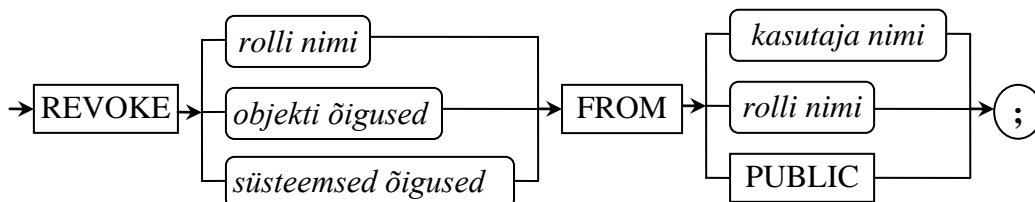
Objektipõhiste õiguste lausend:



Süsteemsed õigused:



Õiguste tagasivõtmise süntaks



Õiguste andmise päringute näidised:

```
SQL> GRANT ALTER ON
  1 skeemi_nimi.tabeli_nimi TO kasutaja_või_rolli_nimi;
```

```
SQL> GRANT UPDATE (veerg_1, veerg_2, ...) ON
  2 skeemi_nimi.tabeli_nimi TO kasutaja_või_rolli_nimi;
```

Päringud, mis on seotud kasutajate haldamisega:

Päring kasutajate rollide ja nendele määratud süsteemsete õiguste vaatamiseks:

```
SQL> SELECT LPAD(' ', (LEVEL-1)*2) || granted_role AS "Rollid ja õigused"
  1 FROM(
  2 SELECT NULL AS grantee, username AS granted_role
  3 FROM dba_users
  4 UNION
  5 SELECT grantee, granted_role
  6 FROM dba_role_privs
  7 UNION
  8 SELECT grantee, privilege
  9 FROM dba_sys_privs)
 10 START WITH grantee IS NULL
 11 CONNECT BY grantee = PRIOR granted_role;
```

Päring kasutajate objekti(tabeli) õiguste vaatamiseks:

```
SQL> SELECT LPAD(' ', (LEVEL-1)*2) || granted_role AS "Rollid ja õigused"
  1 FROM(
  2 SELECT NULL AS grantee, username AS granted_role
  3 FROM dba_users
  4 UNION
  5 SELECT grantee, granted_role
  6 FROM dba_role_privs
  7 UNION
  8 SELECT grantee, privilege || ' on ' || table_name
  9 FROM dba_tab_privs)
 10 START WITH grantee IS NULL
 11 CONNECT BY grantee = PRIOR granted_role;
```

Ülesanded

1. Kasutades programmi SQL*Plus, logige sisse kasutajana *sys*.
2. Seada initsialiseerimise parameeter RESOURCE_LIMIT tõseks (TRUE).
`SQL> ALTER SYSTEM SET RESOURCE_LIMIT=TRUE SCOPE=BOTH;`
3. Looge uus profiil *redaktor* järgmiste piirangutega:
 - a. IDLE_TIME = 15 (min.);
 - b. SESSIONS_PER_USER = 1.
4. Looge uus profiil *veebi_kasutaja* veebiliidese kasutaja jaoks.
5. Looge uus konto *k_raamat* järgmiste parameetritega:
 - a. Vaikimisi tabeliruum – USERS;
 - b. Tabeliruumi USERS kvoot – 1MB;
 - c. Konto suletud;
6. Käivitage skript *praktikum_n3.sql*.
7. Looge uus roll *kulastajad* järgmiste õigustega:
 - a. Selekteerimine kasutaja *k_raamat* tabelist *kommentaaride_tabel*;
 - b. Ridade lisamine kasutaja *k_raamat* tabelisse *kommentaaride_tabel*.
8. Looge uus konto *veebi_kasutaja* järgmiste parameetritega:
 - a. parool – *www*;
 - b. konto avatud (*unlock*);
 - c. vaikimisi tabeliruum – ei ole;
 - d. profiil – *veebi_kasutaja*.
9. Andke kasutajale *veebi_kasutaja* järgmised õigused/rollid:
 - a. CREATE SESSION (õigus);
 - b. Roll - *kulastajad*.
10. Looge uus roll *tsensuur* järgmiste õigustega:
 - a. Kasutaja *k_raamat* tabeli *kommentaaride_tabel* kirjete kustutamine;
 - b. Kasutaja *k_raamat* tabeli *kommentaaride_tabel* kirjete uuendamine.
11. Looge uus konto *redaktor* järgmiste parameetritega:
 - a. Parool – *redaktor*;
 - b. Konto avatud;
 - c. Profiil – *redaktor*;
 - d. Vaikimisi tabeliruum – ei ole.
12. Määrake rollile *tsensuur* – roll *kulastajad*.

13. Andke kasutajale *redaktor*:
 - a. Õigus CREATE SESSION;
 - b. Roll – *tsensuur*.
14. Veenduge, et rakendatud õigused toimivad:
 - a. *veebi_kasutaja* saab lisada ridu ja vaadata tabeli sisu;
 - b. *tsensuur* saab teha kõike (lisada, uuendada, kustutada ja vaadata).
15. Looge uus kasutaja *sybase* järgmiste parameetritega:
 - a. Parool – *sybase*;
 - b. Konto avatud;
 - c. Vaikimisi tabeliruum *sybase*;
 - d. Tabeliruumi *sybase* kvoot – piiramatu.
16. Andke kasutajale *sybase* järgmised õigused/rollid:
 - a. CREATE SYNONYM;
 - b. CREATE TABLE;
 - c. CREATE SEQUENCE;
 - d. CREATE TRIGGER;
 - e. CREATE ANY INDEX;
 - f. CONNECT.