Securitatea bazelor de date

Utilizarea comenzilor GRANT si REVOKE pentru a controla accesul la baza de date.

Privilegiile si Functiile Sistemului

ORACLE utilizeaza un sistem de securitate descentralizat, unde utilizatorii sunt ei insisi responsabili pentru acordarea drepturilor de acces pentru obiectele pe care le detin celorlalti utilizatori. Un utilizator are nevoie de drepturile de conectare la o baza de date sau de creare de obiecte.

Cand Administratorul Bazelor de Date a creat un nou utilizator ORACLE, un grup de drepturi ii sunt atribuite. Se pot grupa combinatiile obisnuite de drepturi in roluri (roles). Rolurile corespunzatoare pot atunci fi atribuite utilizatorilor.

Privilegiile Sistemului

Sunt mai mult de 80 tipuri de drepturi ale sistemului disponibile pentru atribuite catre utilizatori si roluri. Unele din cele mai importante sunt:

Drept Sistem
: Operatii autorizate

CREATE SESSION
: Permite posesorului conectarea la baza de date.

CREATE TABLE
: Permite posesorului crearea de tabele. Utilizatorul trebuie de asemenea sa aiba o cota de "tablespace" (arie a bazei de date).

CREATE VIEW
: Permite crearea imaginilor.

CREATE USER
: Permite posesorului sa creeze alti utilizatori.

Roluri

Un rol este o colectie de drepturi sistem cu nume. Un utilizator poate avea acces la mai multe roluri, si mai multi utilizatori pot fi atribuiti aceluiasi rol, dandu-se flexibilitate sistemului de securitate.

Sunt cateva roluri predefinite, ca DBA (Administrator de Baza de Date) care include toate privilegiile sistemului; un DBA va crea de obicei roluri pentru cerintele sistemului.

Daca aveti atribuite mai multe roluri, puteti oscila intre ele prin comanda SET ROLE.

De exemplu, pentru a activa un rol care are parola "marigold" atasata:

```
SET ROLE gardener IDENTIFIED BY marigold;
```

Pentru a activa toate rolurile exeptand un singur rol pentru un utilizator:

```
SET ROLE ALL EXCEPT manager;
```

Pentru a dezactiva toate rolurile:

```
SET ROLE NONE;
```

La conectare, se activeaza toate rolurile acordate utilizatorului.

Schimbarea Parolei Utilizatorului

DBA atribuie utilizatorului o parola cand utilizatorul este creat (CREATE USER). Utilizatorul poate mai tarziu sa-si schimbe parola utilizand comanda ALTER USER. Sintaxa:

```
ALTER USER nume_utilizator IDENTIFIED BY parola
```

De exemplu :

```
ALTER USER glenn IDENTIFIED BY swordfish;
```

Comanda GRANT

Este utilizata pentru a atribui drepturile unui obiect catre

- un utilizator
- un rol

```
Atribuirea catre un utilizator:

GRANT priv1, priv2, ... ON nume_obiect
TO utilizator1, utilizator2, ... [ WITH GRANT OPTION ]

Atribuirea catre un rol :

GRANT  priv1, priv2, ... ON nume_obiect
TO rol1, rol2, ...
```

'nume_obiect' poate referi :

- o tabela
- o imagine (view)
- o secventa (sequence)
- un sinonim (synonym)
- o procedura

- o functie
- un pachet (package)

Privilegiile unui Obiect

Utilizatorul detine fiecare tabela, imagine, secventa si sinonim pe care il creeaza. Aceste obiecte mai pot fi accesate de DBA.

Pentru a permite accesul altor utilizatori la obiectele bazei de date, utilizati comanda GRANT:

```
GRANT   drepturi
ON      obiect
TO      utilizator;
```

Unele drepturi care pot fi acordate pentru tabele:

```
Drept           Obiect
-----           ------
SELECT          date
INSERT          linii
UPDATE          linii sau coloane specificate
DELETE          linii
ALTER           definitii de coloane
INDEX           indexare
ALL
```

Cel mai simplu fel de GRANT acorda un singur drept unui singur utilizator.

Pentru a acorda lui ADAMS dreptul de SELECT din tabela DEPT, introduceti :

```
GRANT           SELECT
ON              DEPT
TO              ADAMS;

Grant succeeded.
```

Pentru a acorda dreptul UPDATE pentru anumite coloane lui ADAMS, introduceti :

```
GRANT           UPDATE ( DNAME, LOC )
ON              DEPT
TO              ADAMS;
```

Pentru a acorda mai multe drepturi o data, introduceti toate drepturile separate prin virgule. Similar, pentru a acorda drepturi mai multor utilizatori, introduceti numele utilizatorilor separate prin virgule.

Pentru a acorda drepturile INSERT si UPDATE asupra DEPT lui ADAMS si JONES, introduceti:

```
GRANT           INSERT, UPDATE
ON              DEPT
TO              ADAMS, JONES;

Grant succeeded.
```

Pentru a acorda toate privilegiile asupra DEPT lui ADAMS, introduceti :

```
GRANT           ALL
ON              DEPT
TO              ADAMS;

Grant succeeded.
```

Transmiterea de Privilegii care au fost Acordate

Cand s-a acordat un drept de acces, utilizatorul care primeste dreptul, in mod normal nu primeste si autorizarea de a transmite acest drept si altora. Pentru a da unui utilizator dreptul de a transmite dreptul mai departe, utilizati clauza WITH GRANT OPTION.

Pentru a acorda dreptul SELECT asupra EMP lui ADAMS, cu autorizarea de a acorda acest drept si altora, introduceti:

```
GRANT           SELECT
ON              EMP
TO              ADAMS
WITH            GRANT OPTION;

Grant succeeded.
```

Dreptul Public

Permite detinatorului unei tabele sa acorde accesul tuturor utilizatorilor cu o singura comanda,

Acordarea da drept(uri) asupra unei tabele lui PUBLIC.

```
GRANT           SELECT
ON              EMP
TO              PUBLIC;
```

Violarea Drepturilor de Acces

Daca incercati sa executati o operatie neutorizata (de exemplu stergerea dintr-o tabela fara a avea dreptul DELETE), ORACLE nu va permite ca operatia sa aiba loc.

Daca primiti mesajul de eroare ORACLE ' table or view does not exist', aceasta poate insemna doua lucruri :

- aveti o tabela sau o imagine cu nume care nu exista
- ati incercat sa executati o operatie asupra acelei tabele sau imagini pentru care nu aveti drepturile corespunzatoare.

Comanda REVOKE

Pentru a retrage un drept acordat, utilizati comanda REVOKE.

```
REVOKE          drepturi
ON              tabela sau imagine
FROM            utilizatori;
```

Cand utlilzati comanda REVOKE, drepturile specificate sunt anulate utilizatorilor enumerati, si celorlalti utilizatori carora acestia le-au transmis aceste drepturi.

Pentru a anula toate drepturile asupra DEPT ale lui ADAMS, introduceti

```
REVOKE          ALL
ON              EMP
FROM            ADAMS;

Revoke succeeded.
```

Drepturile publice sunt retrase utilizand comanda REVOKE:

```
REVOKE          SELECT
ON              EMP
FROM            PUBLIC;
```

Crearea unui sinonim

Pentru a referi o tabela detinuta de un alt utilizator, trebuie sa prefixati numele tabelei cu numele utilizatorului care a creat-o urmat de punct (.).

Pentru a referi tabela EMP detinuta de SCOTT, introduceti:

```
SELECT          *
FROM            SCOTT.EMP;
```

Alternativa este de a crea un sinonim pentru tabela sau imaginea data.

Pentru a referi tabela EMP a lui SCOTT doar cu numele 'EMP', introduceti :

```
CREATE SYNONYM  EMP
FOR             SCOTT.EMP;
```

Acum, cand executati o cerere asupra tabelei EMP a lui Scott, doar introduceti:

```
SELECT          *
FROM            EMP;
```

Doar DBA poate crea sinonime PUBLICe la care toti utilizatorii sa aiba acces.

```
CREATE PUBLIC SYNONYM   nume_sinonim
for [proprietar.] nume_obiect;
```

Un sinonim public poate fi eliminat prin tastarea:

```
DROP [ PUBLIC ] SYNONYM nume_sinonim;
```

Sinonimele sunt utilizate din motive de securitate si comoditate, incluzand :

- pentru a referi o tabela, secventa sau imagine fara a specifica detinatorul obiectului
- pentru a furniza un alt nume pentru tabela.

Din motive de performanta, nu e recomandabila utilizarea de sinonime la referirea de tabele in aplicatii.