UCB: Universitatea Constantin Brâncuși din Târgu-Jiu
Automatică și Informatică Aplicată

Baze de date

Limbajul SQL

Adrian Runceanu

THE INFORMATION COMPANY

Curs 11

Controlul accesului utilizatorilor

Cuprins

Controlul accesului utilizatorilor

Într-un mediu multi-user, vrem sa mentinem securitatea utilizarii si accesarii bazei de date. Securitatea bazei de date de pe *serverul Oracle* ne permite urmatoarele:

- Controlul accesului la baza de date
- Acordarea accesului la obiecte specifice din baza de date
- Confirmarea privilegiilor date si primite cu ajutorul dictionarului de date Oracle
- Crearea de sinonime pentru obiectele bazei de date

tt

Securitatea bazei de date poate fi clasificata în doua categorii:

1) securitatea sistemului

2) securitatea datelor

tt

1) Securitatea sistemului acopera accesarea si utilizarea bazei de date la nivelul sistemului, cum ar fi: numele utilizatorului si parola, spatiul pe disc alocat utilizatorilor, si operatiile de sistem permise utilizatorilor.

https://www.scnsoft.com/blog/database-security-best-practices

tt

2) Securitatea bazei de date acopera accesarea si utilizarea obiectelor bazei de date si actiunile pe care acesti utilizatori le pot efectua asupra obiectelor.

https://www.opensourceforu.com/2020/09/a-comprehensive-look-at-opensource-database-security-concerns/

Privilegii

Administratorul bazei de date este un utilizator de nivel înalt ce are posibilitatea de a acorda accesul utilizatorilor la baza de date si la obiectele sale.
Utilizatorii necesita *privilegii de sistem* pentru a dobândi acces la baza de date si *privilegii de obiect* pentru a putea manipula continutul obiectelor în baza de date.
Utilizatorilor li se poate da de asemeni privilegiul de a acorda privilegii aditionale altor utilizatori sau unor *roluri*, cum sunt numite *grupurile de privilegii adiacente*.

Scheme

O schema este o colectie de obiecte, cum ar fi:

- ✓ tabele
- ✓ indecsi
- ✓ vizualizari
- ✓ secvente

Schema este detinuta de un utilizator al bazei de date si are acelasi nume cu utilizatorul.

tt

Privilegii de sistem

Sunt disponibile mai mult de 80 de *privilegii de sistem* pentru utilizatori si pentru roluri.

Privilegiile de sistem sunt setate de catre administratorul bazei de date.

Privilegiile caracteristice ale DBA

Privilegii de sistem	Operatii autorizate
Creare de utilizatori	Permite crearea unui alt utilizator Oracle (privilegiu cerut pentru rolul de DBA)
Stergerea de utilizatori	Permite stergerea altui utilizator
Stergerea oricarei tabele	Permite stergerea unei tabele în orice schema
Recuperarea oricarei tabele	Recuperarea oricarei tabele în orice schema cu utilitare de export

Crearea de utilizatori

DBA creeaza utilizatori cu ajutorul declaratiei CREATE USER.

CREATE USER ***user***
IDENTIFIED BY ***password;***

Exemplu:
CREATE USER scott
IDENTIFIED BY tiger;

Crearea unui utilizator

- DBA creeaza un utilizator prin executia declaratiei **CREATE USER**.
- Utilizatorul nu are nici un fel de privilegiu în acest moment.
- *DBA poate da apoi un numar de privilegii acestui utilizator.*
- Aceste privilegii determina drepturile utilizatorului la nivelul bazei de date.

tt

În sintaxa:

user este numele utilizatorului ce este creat.

password specifica faptul ca acest utilizator trebuie sa se conecteze cu parola.

Privilegiile de sistem ale utilizatorului

Odata ce un user este creat, DBA îi poate acorda acestuia privilegii de sistem specifice.

GRANT privilege [, privilege…]
TO user [, user…];

În sintaxa:

privilege este privilegiul de sistem ce va fi acordat.

user este numele utilizatorului.

tt

Persoana care creaza o aplicatie trebuie sa aiba urmatoarele *privilegii de sistem*:

- Crearea de sesiuni
- Crearea de tabele
- Crearea de secvente
- Crearea de imagini
- Crearea de proceduri

Privilegii de utilizator caracteristice

Dupa ce DBA a creat un utilizator, el poate atribui privilegii acelui utilizator.

Privilegii de sistem	Operatii autorizate
Crearea de sesiuni	Conectarea la o baza de date
Crearea de tabele	Creaza tabele în schema utilizatoruluii
Crearea de secvente	Creaza o secventa în schema utilizatorului
Crearea de imagini	Creaza o imagine în schema utilizatorului
Crearea de proceduri	Creaza o procedura, functie sau o transpune în schema utilizatorului

Acordarea privilegiilor de sistem

DBA poate acorda unui utilizator *privilegii de sistem specifice*.

Exemplu:

GRANT create table, create sequence, create view

TO scott;

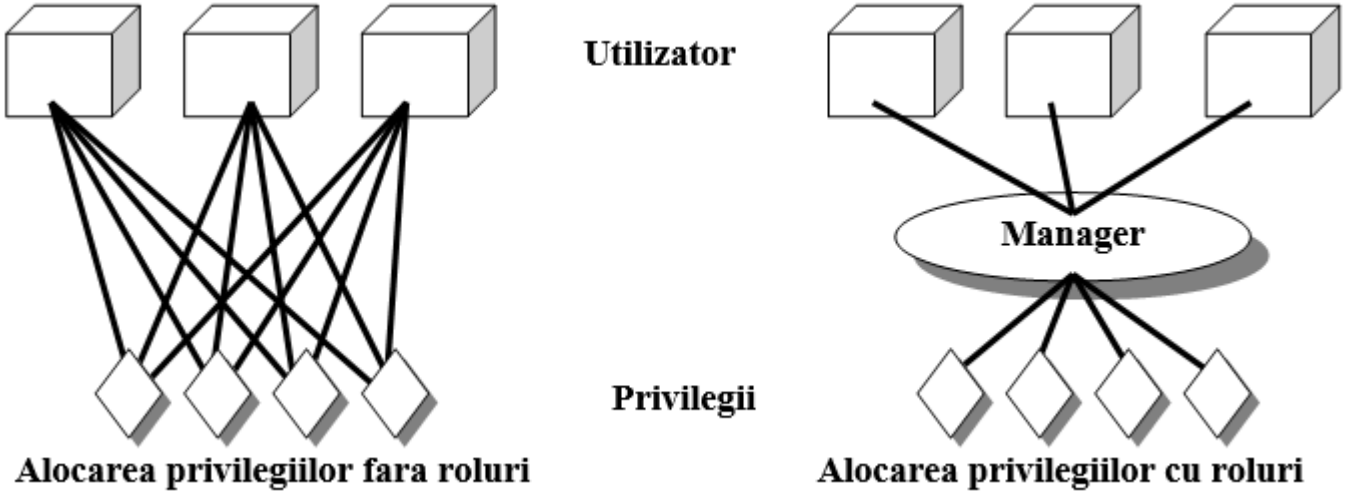
Acordarea privilegiilor de sistem

- DBA foloseste declaratia GRANT pentru a aloca privilegii de sistem unui utilizator.
- Odata ce un utilizator a obtinut aceste privilegii, poate imediat beneficia de ele.
- În exemplul anterior, utilizatorul Scott a primit dreptul de a crea tabele, secvente si imagini.

Ce este un rol?

Un **rol** este *un grup de privilegii adiacente ce pot fi acordate unui utilizator*.

Aceasta metoda face ca acordarea si revocarea de privilegii sa fie mai usor de facut si urmarit.



Crearea si atribuirea unui rol

Mai întâi DBA trebuie sa creeze un rol.
Apoi DBA poate atribui privilegii acelui rol si utilizatori acelui rol.
Sintaxa

CREATE ROLE role;

unde: role este numele rolului ce se creaza.
Dupa ce rolul a fost creat, DBA poate utiliza declaratia GRANT pentru a aloca utilizatori rolului, sau pentru a atribui privilegii rolului.

Crearea si acordarea de privilegii unui rol

Exemplu:

```
CREATE ROLE   manager;
Role created.

GRANT create table, create view
to manager;

GRANT manager to BLAKE, CLARK;
```

Crearea unui rol

- Exemplul anterior creaza un rol numit „manager” si apoi permite „managerilor” sa creeze tabele si vizualizari.
- Apoi se atribuie lui Blake si lui Clarke rolul de „manager”.
- Acum Blake si Clark pot crea tabele si vizualizari.

Schimbarea parolei

Fiecare utilizator are o parola care este initiata de DBA atunci când utilizatorul este creat.
Parola se poate schimba prin folosirea declaratiei **ALTER USER**.
Sintaxa

ALTER USER user IDENTIFIED BY password;

unde: user este numele utilizatorului.
password specifica noua parola.

tt

Exemplu:

```
ALTER USER scott
IDENTIFIED BY lion;
```

- Desi aceasta declaratie poate fi folosita pentru schimbarea parolei, exista multe alte optiuni.

- Pentru a putea schimba oricare alta optiune trebuie sa avem privilegiul ALTER USER.

Privilegii de obiect

Privilegiu de obiect	Tabela	Vizualizare	Secventa	Procedura
ALTER	V		V	
DELETE	V	V		
EXECUTE				V
INDEX	V			
INSERT	V	V		
REFERENCES	V			
SELECT	V	V	V	
UPDATE	V	V		

Privilegii de obiect

- Un *privilegiu de obiect* este un privilegiu ce permite utilizatorului sa efectueze o actiune particulara într-o tabela, vizualizare, secventa sau procedura specifica.
- Fiecare obiect are un set de privilegii alocate.
- Tabela anterioara prezinta o serie de privilegii pentru diferite obiecte.
- De notat ca singurele privilegii ce se aplica unei secvente sunt SELECT si ALTER.

Privilegii de obiect

- UPDATE, REFERENCE si INSERT pot fi restrictionate prin specificarea unui set de coloane ce pot fi modificate.
- Un SELECT poate fi restrictionat prin crearea unei imagini cu un subset de coloane si acordarea privilegiului SELECT asupra imaginii.
- O alocare asupra unui sinonim este convertita ca o alocare asupra tabelei de baza ce este referita de sinonim.

Acordarea privilegiilor de obiect

- Diferite privilegii de obiect sunt disponibile pentru diferite tipuri de obiecte de schema.
- Un utilizator are automat privilegii de obiect asupra obiectelor de schema continute în schema sa.
- Un utilizator poate acorda orice privilegiu de obiect asupra oricarei scheme de obiect pe care o detine unui alt utilizator sau unui rol.

Acordarea privilegiilor de obiect

- Daca alocarea include si declaratia GRANT OPTION, cel ce a primit privilegiul poate la rândul sau sa acorde privilegii asupra acelui obiect mai departe altor utilizatori, în caz contrar el având dreptul de a folosi privilegiul, dar neavând posibilitatea de a-l transmite mai departe.

Acordarea privilegiilor de obiect

```
GRANT  object_priv  [ (columns) ]
ON         object
TO         { user | role |  PUBLIC }
[WITH GRANT OPTION];
```

Acordarea privilegiilor de obiect

În sintaxa:

object_priv este un privilegiu de obiect ce va fi acordat.

ALL toate privilegiile de obiect.

columns specifica coloana dintr-o tabela sau o imagine în care privilegiile sunt acordate.

ON object este obiectul asupra caruia privilegiile sunt acordate.

TO identifica cui îi este acordat privilegiul.

PUBLIC acorda privilegii de obiect tuturor utilizatorilor.

WITH GRANT OPTION da dreptul detinatorului sa acorde mai departe privilegii de obiect altor utilizatori sau roluri.

Acordarea privilegiilor de obiect

Exemplu:
Acordarea privilegiilor de interogare în tabela EMP.

```
GRANT     select
ON        emp
TO        sue, rich;

Grant succeeded.
```

Acordarea privilegiilor de obiect

Exemplu:
Acordarea privilegiilor de actualizare a anumitor coloane utilizatorilor si rolurilor.

```
GRANT   update (dname, loc)
ON      dept
TO      scott, manager;
```

Grant succeeded.

Acordarea privilegiilor de obiect

În primul exemplu de mai sus se acorda utilizatorilor Sue si Rich privilegiul de a interoga tabela EMP.
În al doilea exemplu se acorda privilegii de actualizare a anumitor coloane în tabela DEPT utilizatorului Scott si rolului de „manager”.
Nota: DBA acorda în general privilegii de sistem; orice utilizator ce detine un obiect poate acorda privilegii de obiect.

Acordarea privilegiilor de obiect

Precizari

- Pentru a putea acorda privilegii asupra unui obiect, cel ce vrea sa acorde privilegii trebuie sa detina obiectul în schema sa sau trebuie sa detina privilegii de obiect WITH GRANT OPTION.
- Un proprietar de obiect poate acorda orice privilegii de obiect asupra obiectului sau oricarui utilizator sau rol din baza de date.
- Proprietarul unui obiect câstiga automat toate privilegiile de obiect asupra acestuia.

tt

- Folosirea cuvintelor cheie **WITH GRANT OPTION** si **PUBLIC**
- Acordarea dreptului de a acorda mai departe privilegiile altui utilizator.

Exemplu:

```
GRANT   select, insert
ON          dept
TO          scott
WITH GRANT OPTION;
```

Grant succeeded.

Cuvântul cheie WITH GRANT OPTION

- Un privilegiu ce este acordat WITH GRANT OPTION poate fi transmis mai departe altor utilizatori, de catre cel ce are acest privilegiu.
- Privilegiile de obiect acordate WITH GRANT OPTION sunt retrase când privilegiul de a putea acorda privilegii este retras.
- În exemplul anterior se acorda dreptul utilizatorului Scott de a accesa tabela DEPT cu privilegiul de a adauga acesteia noi rânduri.
- De asemenea se acorda dreptul lui Scott de a acorda mai departe aceste privilegii.

tt

- Acordarea tuturor utilizatorilor din sistem a dreptului de a interoga datele din tabela DEPT a lui Alice.

Exemplu:

```
GRANT   select
ON          alice.dept
TO          PUBLIC;
Grant succeeded.
```

Cuvântul cheie PUBLIC

- Detinatorul unei tabele poate acorda accesul la ea tuturor utilizatorilor prin folosirea cuvântului cheie PUBLIC.

- În exemplul anterior se permite tuturor utilizatorilor din sistem sa acceseze datele din tabele DEPT ce este detinuta de Alice.

Confirmarea privilegiilor acordate

Tabela datelor din dictionar	Descriere
ROLE_SYS_PRIVS	Privilegii de sistem acordate rolurilor
ROLE_TABS_PRIVS	Privilegii de tabela acordate rolurilor
USER_ROLE_PRIVS	Roluri accesibile utilizatorului
USER_TAB_PRIVS_MADE	Privilegii de obiect acordate obiectelor utilizatorului
USER_TAB_PRIVS_RECD	Privilegii de obiect acordate utilizatorului
USER_COL_PRIVS_MADE	Privilegii de obiect acordate asupra coloanelor obiectelor utilizatorului
USER_COL_PRIVS_RECD	Privilegii de obiect acordate utilizatorului în diferite coloane

Confirmarea privilegiilor acordate

- Daca se încearca sa se efectueze o operatie neautorizata – de exemplu stergerea unui rând dintr-o tabela asupra careia nu avem privilegiul DELETE – serverul Oracle nu va permite ca operatia sa fie efectuata.

Confirmarea privilegiilor acordate

Daca se primeste de la serverul Oracle mesajul de eroare "tabela sau imagine inexistenta" trebuie sa fie luate în calcul urmatoarele doua posibilitati:

1. Tabela sau imaginea respectiva nu exista
2. S-a încercat sa se efectueze o operatie asupra unei tabele sau imagini asupra careia nu exista acel privilegiu

Se poate accesa dictionarul de date pentru a putea vedea ce privilegii se detin.

Tabela anterioara descrie diferite tabele din dictionarul de date.

Cum sa retragem privilegiile de obiect

- Se foloseste declaratia REVOKE pentru a retrage privilegiile acordate altui utilizator.

- Si privilegiile acordate altui utilizator cu declaratia WITH GRANT OPTION vor fi de asemenea retractate.

Cum sa retragem privilegiile de obiect

REVOKE { privilege [, privilege …] | ALL
ON object
FROM {user [, user …] | role | Public }
[CASCADE CONSRAINTS];

Retragerea privilegiilor de obiect

- Privilegiile acordate altor utilizatori se retrag folosind declaratia **REVOKE**.
- Când se foloseste declaratia **REVOKE**, privilegiile pe care le vom specifica vor fi retrase de la utilizatori pe care i-am numit si de la toti utilizatorii carora aceste privilegii au fost acordate.

În sintaxa:

CASCADE CONSTRAINTS este cerut pentru a retrage orice constrângeri de integritate referentiale aplicate obiectului prin privilegiul **REFERENCES**.

Retragerea privilegiilor de obiect

Cum retrage utilizatorul Alice privilegiile **SELECT** si **INSERT** acordate utilizatorului Scott asupra tabelei DEPT.

Exemplu:

```
REVOKE   select, insert
    2    ON          dept
    3    FROM        scott;
Revoke succeeded.
```

Retragerea privilegiilor de obiect

În exemplul anterior se retrag privilegiile **INSERT** si **SELECT** acordate utilizatorului Scott asupra tabelei DEPT.

Nota:

Daca un utilizator primeste un privilegiu cu optiunea **WITH GRANT OPTION**, acel utilizator poate acorda la rândul sau privilegiul cu optiunea WITH GRANT OPTION, astfel încât un lung sir de acordari în lant este posibil, dar nu sunt permise acordarile circulare.

Retragerea privilegiilor de obiect

- Daca un detinator retrage un privilegiu unui utilizator ce a acordat acel privilegiu altor utilizatori, declaratia **REVOKE** va actiona în cascada , retragând acele privilegii si celorlalti utilizatori.

Retragerea privilegiilor de obiect

- De exemplu, daca un utilizator A acorda privilegiu **SELECT** asupra unei tabele unui utilizator B incluzând si optiunea **WITH GRANT OPTION**, utilizatorul B poate acorda privilegiul **SELECT** unui utilizator C cu optiunea **WITH GRANT OPTION**, care la rândul sau poate acorda acest privilegiu unui utilizator D.

- Daca utilizatorul A retrage privilegiul utilizatorului B, atunci privilegiile acordate utilizatorilor C si D sunt de asemenea revocate.

Sumar

CREATE USER	Permite DBA sa creeze un utilizator
GRANT	Permite unui utilizator sa acorde privilegii de acces altor utilizatori la obiectele pe care le detine
CREATE ROLE	Permite DBA sa creeze o colectie de privilegii
ALTER USER	Permite utilizatorilor sa-si schimbe parola
REVOKE	Retrage privilegiile acordate asupra unui obiect utilizatorilor

Concluzii

DBA stabileste initial securitatea bazei de date pentru utilizatori, prin acordarea de privilegii acestora.

- DBA creaza utilizatori care trebuie sa aiba o parola. DBA este de asemenea responsabil pentru stabilirea privilegiilor de sistem initiale pentru un utilizator.
- Odata ce un utilizator a creat un obiect, el poate sa transmita mai departe oricare din privilegiile de obiect disponibile unor utilizatori, sau tuturor utilizatorilor, prin folosirea declaratiei **GRANT**.

Concluzii

- Un DBA poate crea roluri cu ajutorul declaratiei **CREATE ROLE**, putând astfel transmite mai departe un set de privilegii de sistem sau obiect mai multor utilizatori. Rolurile fac ca acordarea si retragerea de privilegii sa fie mai usor de efectuat.
- Utilizatorii îsi pot schimba parola cu ajutorul declaratiei **ALTER USER**.
- Privilegiile se pot retrage de la utilizatori cu ajutorul declaratiei **REVOKE**.
- Imaginile din dictionarul de date permit utilizatorilor sa vada privilegiile acordate lor si celor ce au acces la obiectele lor.

Întrebări?