Gestionarea accesului

Sistemul de privelegii în MySQL

- Funcția principală este de a autentifica și autoriza utilizatorii conectați la server
- Autorizarea – permisiunea de a rula interogări precum SELECT, INSERT, UPDATE, DELETE, drepturi de administrare, de interacționare cu SO.
- Privelegiu – un drept al unui utilizator de a acționa într-un anumit fel asupra unui obiect al BD (tabele, cîmp, index etc.)

Utilizator și parole

- Există diferențe între sistemul de utilizatori și parole din MySQL și SO Unix sau Windows:
  - Numele de utilizatori MySQL pot avea 16 caractere semnificative, pe cînd în majoritatea implementările Unix – 8 caractere.
  - Numele utilizatorilor și parolele sunt păstrate separat de MySQL și nu au nimic comun cu cele din sistemul de operare.
  - MySQL crptează parolele folosind un algoritm diferit de cel utilizat de Unix sau Windows. Algoritmul de criptare este ireversibil.

Prinipiul – Minimum de privilegii necesare

- Sporește securitatea oricărui calculator (nu doar a serverului MySQL)
- Principiul:
  - Un utilizator (sau proces) trebuie să aibă cel mai scăzut nivel de privilegii, suficient pentru a putea executa sarcinile care i-au fost alocate.

Privilegii în MySQL

- Informațiile despre privilegii sunt stocate în BD mysql în tabelele:
  - user
  - db
  - host
  - tables_priv
  - columns_priv
- Sistemul citește datele din aceste tabele ori de cîte ori sistemul de privilegii trebuie să acționeze.

Privilegiu	Denumire coloana	Context	Semnificatie
select	Select_priv	tabele	permite selectarea (vizualizarea) datelor
insert	Insert_priv	tabele	permite adaugarea unor noi inregistrari
update	Update_priv	tabele	permite modificarea datelor
delete	Delete_priv	tabele	permite stergerea inregistrarilor
index	Index_priv	tabele	permite crearea/stergerea indecsilor
alter	Alter_priv	tabele	permite redenumire sau modificarea structurii tabelei
create	Create_priv	baza de date, tabele sau indecsi	permite crearea unei baze de date/tabele
drop	Drop_priv	baza de date, tabele	permite stergerea unei baze de date/tabele
grant	Grant_priv	baza de date, tabele	permite delegarea privilegiilor catre alt utilizator
shutdown	Shutdown_priv	administrare server	permite oprirea serverului din programul client
process	Process_priv	administrare server	permite vizualizarea/oprirea proceselor in executie
file	File_priv	acces la fisiere externe	permite schimbul de date intre tabele si fisiere

Privilegii

- Privilegiul grant permite utilizatorilor să dea mai departe privilegiile lor și altor utilizatori.
- Privilegiul alter poate fi folosit pentru a redenumi tabele, modificînd astfel baza de date și făcînd astfel inutilizabile programele altor utilizatori.
- Privilegiul file poate fi folosit pentru a citi informații sensibile de pe server.
- Privilegiul shutdowm dă posibilitatea opririi serverului de la distanță.
- Privilegiul process poate fi utilizat pentru a vedea conținutul interogărilor ce se execută în acel moment, inclusiv cele de setare a parolei.

Nu se acoperă

- Nu se poate specifica explicit că unui utilizator i se refuză dreptul de a se conecta.
- Nu se poate da dreptul unui utilizator pentru a crea și șterge tabele într-o bază de date, nu poate șterge nici BD.

Comanda Grant

- Permite utilizatorilor stabilirea și/sau modificarea privilegiilor acestora pe patru nivele de privilegii:
  - Global – se aplică tuturor BD existente pe un server
  - Database – se aplică tuturor tabelelor dintr-o BD
  - Table – se aplică tuturor coloanelor dintr-o tabelă
  - Column – se aplică doar coloanelor specificate explicit

Forma generală

GRANT privilegii [coloane]

ON componenta

TO nume_utilizator [IDENTIFIED BY ‘parola’]

[WITH GRANT OPTIONS]

PRIVILEGII

- Lista de privilegii desp[ríte prin virgul[
  - SELECT
  - INSERT
  - ALTER
  - …
  - ALL [PRIVILEGES]
  - USAGE – utilizator fără drepturi

COLOANE

- Listă de una sau mai multe coloane.
- Permite de a stabili privilegiile la nivel de coloane.
- Poate fi * pentru toate coloanele (novel Table)

COMPONENTA

- Numele BD sau tabele asupra cărora vor fi stabilite privilegiile
- Toate BD se specifică prin *.* (nivel Global)
- Baza de date curentă * (nivel Database)
- O anumită BD prin nume_bd.* (nivel Database)
- O tabelă prin nume_bd.nume_tabela (nivel Table)

UTILIZATOR

- Numele utilizatorului căruia i se atribuie privilegiile
- Poate conține și numele stației de pe care are dreptul să se conecteze
  - ionel@localhost
  - ionel@home.com
  - ionel@’%.md’ - orice utilizator ionel de la orice stație din domeniul .md
  - ionel@’%’ = ionel – de la orice stație

PAROLA

- Parola cu care utilizatorul se va conecta
- Dacă opțiunea IDENTIFIED BY lipsește, utilizatorul se va putea conecta fără parolă, ceea ce reprezintă o gravă lacună de securitate
- WITH GRANT OPTION – dă dreptul utilizatorului să dea privilegii echivalente cu ale sale altor utilizatori

Schimbarea parolei

- SET PASSWORD FOR nume_user = PASSWORD(”parolă_nouă”)

Vizualizarea privilegiilor

- SHOW GRANTS FOR nume_user

Retragerea privilegiilor

- Inversul lui GRANT este REVOKE

REVOKE privilegii[coloane]

ON componenta

FROM nume_user

Retragerea privilegiilor

- Pentru a retrage privilegiile oferite cu WITH GRANT OPTION se va utiliza:

REVOKE GRANT OPTIONS

ON componenta

FROM nume_user

Întrebări?