Laboratorio di Basi di dati

Dr. Luca Tomassetti

Dipartimento di Fisica – Università di Ferrara

Tabella user (1)

- Host } Primary key
- user
- Password
- Select_priv
- Insert_priv
- Update_priv
- Delete_priv
- Create_prov
- Drop_priv
- Reload_Priv

- char(60)
- char(16)
- char(16)

enum('N','Y')

NOTE
Nessun campo ha 'null' come valore possibile

Tutti i _priv hanno 'N' come default

Tabella User (2)

- Shutdown_priv
- Process_priv
- File_priv
- Grant_priv
- References_priv
- Index_priv
- Alter_priv

Host e user possone essere stringa nulla; in questo caso valgono % (vengono trattati come se...)

Tabella User (3)

Host user	=> =>	Accettano valori con il carattere jolly % => anat%a comprende anatomia, anatolia, anatra
User	=>	Accetta nobody, che si comporta come un singolo %
Select, Insert,	=>	Possibilta' di eseguire i comandi SQL standard corrispondenti
Update, Delete	=>	
Create	=>	Possibilita' di eseguire il comando SQL CREATE, o di creare database

Tabella user (4)

- Drop => Possibilita' di cancellare db
- Reload => Ricaricare info sull'accesso mediante mysqladmin reload
- Shutdown => Fermare mysqld mediante mysqladmin shutdown
- Process => Possibilita' di gestire i thread del server mysqld
- File => Possibilita' di aprire e leggere file
  SELECT INTO DATA
  LOAD DATA INFILE

Tabella user (5)

- Grant => Possibilita' di assegnare a terzi al massimo i propri privilegi
- Index => Possibilita' di creare o distruggere indici
- Alter => Possibilita' di eseguire ALTER TABLE

Privilegi Amministrativi (2)

Sono concentrati nella tabella USER e non compaiono nelle altre tabelle del database mysql. A ciascuno di essi corrispondono uno o piu' privilegi/azioni

- Reload_priv => reload, refresh, flush-privileges, flush-host,flush-logs, flush-tables

- Shutdown_priv => shutdown

- Process_priv => processlist, kill

Privilegi Amministrativi (2)

INSERT INTO user (Host, User, Password, Select_priv, Insert_priv, Update_priv, Delete_priv)

VALUES ('%', 'boris', password('ciao'), 'Y', 'Y', 'Y', 'Y')

INSERT INTO user

(Host, User, Password, Select_priv)

VALUES('pcsegreteria_azienda.it', 'Luca', '', 'Y')

UTENTE AVANZATO
SEGRETARIA, OSPITE

Privilegi Amministrativi (3)

INSERT INTO user (Host,User,Password)
VALUES ('%', 'nobody', '')

INSERT INTO user (Host, User, Password, Select_priv, Insert_priv, Update_priv, Delete_priv, [..tutti...], Drop_priv)
VALUES ('dbadmin.azieda.it', ' ', 'ciao','Y', 'Y', 'Y', 'Y', [...Y..], 'N')

RESTO DEL MONDO

AMMINISTRATORE PRUDENTE => PARANOICO

Verifica Dati Sicurezza (1)

-La tabella 'user' e' ...una tabella=> i record sono NON ORDINATI

-Un utente invia al server mysqld una richiesta d'accesso che, ovviamente, e' nella forma

utente@macchina.spa.it

cioe' senza caratteri jolly

- il server confronta utente@macchina.spa.it con i campi "User" e "Host" della tabella user

- Poiche' nella tabella 'user' ci possono essere i '%', se utente@macchina.spa.it ha piu' di una corrispondenza, qual'e' il criterio?

Verifica Dati Sicurezza (2)

CRITERI CONFRONTO DATI UTENTE CON RECORD TABELLA USER

1) Prima gli host (le macchine) che NON contengono '%', poi quelli che contengono il jolly. I campi vuoti, al solito, valgono '%'

2) Se l'host (la macchina) e' la stessa, gli utenti SENZA '%' vengono prima di quelli col jolly. Campi vuoti = '%'

3) La prima corrispondenza e' l'unica considerata, ed il processo di autenticazione termina

Laboratorio di Basi di dati

Dr. Luca Tomassetti

Dipartimento di Fisica – Universita' di Ferrara

Tabella db (1)

- Host
- Db } Primary key
- user
- Select_priv
- Insert_priv
- Update_priv
- Delete_priv
- Create_prov
- Drop_priv

- char(60)
- char(32)
- char(16)

enum('N','Y')

NOTE

Nessun campo ha 'null' come valore possibile

Tutti i _priv hanno 'N' come default

Host e user e Db possone essere stringa nulla; in questo caso valgono % (vengono trattati come se...)

Tabella db (2)

- References_priv
- Index_priv
- Alter_priv

Tabella Host (1)

- Host
- Db

} Primary key

- Select_priv
- Insert_priv
- Update_priv
- Delete_priv
- Create_prov
- Drop_priv

- char(60)
- char(32)

enum('N','Y')

NOTE

Nessun campo ha 'null' come valore possibile

Tutti i _priv hanno 'N' come default

Tabella Host (2)

- References_priv
- Index_priv
- Alter_priv

Tabella Tables_priv

Host	=>	Primary Key	char (60)	NOTE:
Db	=>		char (64)	Il campo timestamp ammette null
User	=>		char (16)	
Table_name	=>		char (60)	
Table_priv	=>		set (i)	i= 'Select', 'Update', 'Delete', 'Create', 'Drop', 'Grant', 'References', ' Index', 'Alter'
Column_priv	=>		set(ii)	ii='Select', 'Insert', 'Update', 'References'
Timestamp			timestamp (14)	
Grant			char (77)	

Tabella Colums_priv

Host	=>	P	char (60)
Db	=>	r	char (64)
User	=>	i	char (16)
Table_name	=>	m	char (60)
Column_name	=>	a	char(64)
Column_priv	=>	r	set(i)
Timestamp		y K e y	timestamp (14)

NOTE:

Il campo timestamp ammette null

i='Select', 'Insert', 'Update', 'References'

Caratteri Jolly e Blank nelle tabelle MYSQL (1)

USER

- Host '%' consentito any host
  '-' consentito
  ' ' consentito verif. tabella host

- User '%' NON consentito ?
  '-' NON consentito
  ' ' consentito OK per ogni nome ma l'utente diventa 'nobody'

-Password '%' consentito inutile come jolly nel senso
'-' consentito che per mysql e' una pwd
' ' consentito NESSUNA pwd, non qualsiasi pwd

Caratteri Jolly e Blank nelle tabelle MYSQL (2)

Db

- Host '%' consentito any host
  '-' consentito
  ' ' consentito verif. tabella host

- Db '%' consentito any database
  '-' consentito
  ' ' consentito any database

-User '%' consentito non sono jolly
  '-' consentito non sono jolly
  ' ' consentito OK per ogni nome ma l'utente diventa 'nobody'

Caratteri Jolly e Blank nelle tabelle MYSQL (3)

Host

- Host '%' consentito any host
  '-' consentito
  ' ' consentito verif. tabella host

- Db '%' consentito any database
  '-' consentito
  ' ' consentito any database

Caratteri Jolly e Blank nelle tabelle MYSQL (4)

Tables_pivot

- Host '%' consentito any host
  '-' consentito
  ' ' consentito any host

- Db '%' NON consentito
  '-' NON consentito
  ' ' NON consentito

Caratteri Jolly e Blank nelle tabelle MYSQL (4/bis)

Tables_pivot

- Table_name '%' NON consentito
  '-' NON consentito
  ' ' NON consentito

- User '%' NON consentito
  '-' NON consentito
  ' ' consentito => 'utente nobody'

Caratteri Jolly e Blank nelle tabelle MYSQL (5)

Columns_priv

- Host '%' consentito any host
'-' consentito
' ' consentito any host

- Db '%' NON consentito
Table_name '-' NON consentito
Column_name ' ' NON consentito
Column_priv

Caratteri Jolly e Blank nelle tabelle MYSQL (5/bis)

Column_priv

- User '%' NON consentito
'-' NON consentito
' ' consentito => 'utente nobody'

Calcolo Logico Dei Privilegi

user privileges
OR
(db privileges AND host privileges)
OR
tables_priv privileges
OR
columns_priv privileges

I privilegi di amministratore sono limitati alla tabella user

Il Comando GRANT

```
GRANT    priv_type [(column_list)] [,priv_type[(column_list)]...]
          ON {tbl_name|*|**|db_name.*}
            TO  user_name [IDENTIFIED BY 'password'][user_name
                          [IDENTIFIED BY 'password']

                [WITH GRANT OPTION]
```

Il Comando REVOKE

REVOKE priv_type [(column_list)] [,priv_type[(column_list)]...]
ON {tbl_name||**|db_name.*}*
FROM user_name [, user_name....]

[WITH GRANT OPTION]

Note sui comandi GRANT e REVOKE

- *user_name va inteso nella forma user@host*
- *se user_name manca della seconda parte,ossia c'e' solo il nome, il server capisce user@% ossia "quell'utente da qualsiasi host"*
- *il comando GRANT crea l'user (sempre nel sensao user@host) se esso non esiste*
- *l'opzione * nella parte ON ha due significati diversi a seconda che si sia 'dentro' un database o no:*
  - *se si, significa "tutte le tabelle"*
  - *se no, significa " tutte le tabelle di tutti i database"!!!!!*

Esempi di comandi GRANT e REVOKE

GRANT USAGE ON db_test.* TO anon

Garantisce l'accesso senza alcun privilegio all'utente anon(da qualsiasi host)

GRANT SELECT ON agenda.* TO consult@%.ditta.it
Accesso con privilegio SELECT sul db agenda (tutte le tabelle) all'utente consult da qualsiasi macchina del dominio ditta.it

---

GRANT INSERT,UPDATE (Nome, Cognome, Tel) ON agenda.contatti to

segret@%.ditta.it
La segreteria puo' inserire record e/o modificare solo in parte nella tabella contatti del db agenda da qualsiasi host del dominio ditta.it