1 Uživatele

1.1 Databázová bezpečnost teorie

1.1.1 Rozlišení práv

Co není povoleno, je zakázáno

- Přiřadit mu práva pro celý server
- Přiřadit mu práva pro jednu nebo více databází (z mnoha existujících)
- Přiřadit mu práva pro jednu nebo více tabulek v databázi (z mnoha existujících)
- Přiřadit mu práva pro jeden sloupec v tabulce
- Přiřadit mu práva vytvářet a používat **pohledy** (jen MySQL 5.x)
- Přiřadit mu práva vytvářet, měnit nebo spouštět uložené **procedury** (jen MySQL 5.x)

- Prohlížet (používat SELECT)
- Vkládat (používat INSERT)
- Upravovat (používat UPDATE)
- Odstraňovat (používat DELETE)
- …

Zvláštní práva:

- Měnit práva uživatelů
- Nastavovat systém

1.2 Tabulky nad databází MySQL

- **user**
- **db**
- **host**
- **func**
- **columns_priv**
- **tables_priv**

1.2.1 tabulka user

V databázi mysql v tabulce **user** jsou uložena oprávnění pro uživatele, která platí na **úrovni celé databáze**, proto dávejte pozor, co zde komu dovolíte.

- **host** - IP adresa, nebo název počítače, odkud se uživatel může připojit, pokud je vám to jedno, použijte znak **%** jako zástupný symbol pro cokoliv.
- **User** - Jméno uživatele.
- **Password** - Heslo zahashované funkcí PASSWORD().
- Následující položky můžou nabývat hodnot **Y** a **N**, jako výchozí hodnota je nastaveno **N**.
- **Select_priv** - Vypisování řádků z tabulky.
- **Insert_priv** - Vkládání řádků do tabulky.
- **Update_priv** - Update řádků v tabulce.
- **Delete_priv** - Odstraňování řádků z tabulky.
- **Create_priv** - Vytváření databází a tabulek.
- **Drop_priv** - Mazání databází a tabulek.
- **Reload_priv** - Znovunačtení tabulky přístupových oprávnění.
- **Shutdown_priv** - Vypínaní serveru.

- **Process_priv** - Prohlížení informací o vláknech serveru
- **File_priv** - Přístup k souborům na serveru, číst můžete jen soubory čitelné všemi a vytvářet jen nové soubory tzn. že nemůžete přepsat existující soubor.
- **Grant_priv** - Udělovaní oprávnění jiným účtům.
- **References_priv** - Rezervováno pro budoucí použití.
- **Index_priv** - Vytváření/odstraňování indexů.
- **Alter_priv** - Změny struktury tabulky.
- **Show_db_priv** - Zobrazovat informace o databázích *(SHOW DATABASES)*
- **Super_priv** - Superuživatelské operace, práce s vlákny apd...
- **Create_tmp_table_priv** - Vytváření dočasných tabulek
- **Execute_priv** - Spouštění uživatelských procedur *(zatím se nepoužívá, kdyžtak mě opravte ;-)*
- **Lock_tables_priv** - Povolí nastavení zámku proti čtení/zápisu.
- **Pár dalších** (dle verze) - další položky, ale ty se nevztahují k přímo k přístupovým právům.

1.2.2 Tabulka DB

Zde jsou uložena oprávnění k jednotlivým databázím.

1.2.3 Tabulka tables_priv

Práva pro jednotlivé tabulky.

1.2.4 Tabulka columns_priv

Práva pro jednotlivé sloupce tabulek.

1.3 Různá oprávnění

Zzde je malý výpis oprávnění, která můžete použít

- ***ADMINISTRATORSKA***
  - ALL PRIVILEGES- jak jsme předvedli výše – MySQL uživatel má přístup do všech databází (kromě systémových databází)
  - GRANT OPTION- povolí uživateli přiřazovat, nebo odstraňovat oprávnění
- UŽIVATELSKÁ
  - CREATE TEMPORARY TABLES – Vytvářet dočasné tabulky
  - FILE - Práce se soubory na serveru
  - LOCK TABLES - Povoluje explicitní použití příkazu LOCK TABLES
  - PROCESS - Získávání informací o vláknech.
  - RELOAD - Znovunačítání přístupových oprávnění apd.
  - SHOW DATABASES - Povoluje prohlížet si všechny databáze.
  - SHUTDOWN - Ukončovat práci serveru
  - SUPER – Ukončovat vlákna

Právo	Vztahuje se na	Popis
SELECT	tabulky, sloupce	Povoluje vybírat záznamy z tabulek.
INSERT	tabulky, sloupce	Povoluje vkládat nové řádky do tabulky.
UPDATE	tabulky, sloupce	Povoluje obnovovat hodnoty záznamů v tabulkách.
DELETE	Tabulky	Povoluje odstraňovat záznamy (řádky) z tabulek.
INDEX	Tabulky	Povoluje vytvářet a odstraňovat indexy z tabulek.
ALTER	Tabulky	Povoluje měnit strukturu stávajících tabulek (přejmenovávat nebo přidávat sloupce, měnit datové typy sloupců).
CREATE	databáze, tabulky	Povoluje vytvářet nové databáze a tabulky.

DROP databáze, tabulky Povoluje odstranit databáze a tabulky.

1.4 Prohlídnout uživatelé a práva

1.4.1 Uživatelé

1.4.2 Oprávnění GRANT

```
show grants;
```

1.5 Vytvořit uživatele

Co měnit a neměnit

1.5.1 Uživatel pod local host

```
CREATE USER
```

1.6 Přiřadit práva GRANT

1.6.1 GRANT syntaxe

```
GRANT práva [sloupce]
ON položka_kde
TO uživatel [IDENTIFIED BY 'heslo' ]
[REQUIRE volby_ssl]
[WITH [GRANT OPTION | volby_omezení] ]
```

Pro připomenutí:

- **ALL** - Může všechno.
- **ALTER** - Měnit strukturu tabulky.
- **CREATE** - Vytvářet tabulky a databáze.
- **DELETE** - Mazat záznamy z tabulek.
- **DROP** - Mazat tabulky a databáze.
- **FILE** - Práce se soubory na serveru.
- **INDEX** - Vytvářet a odstraňovat indexy.
- **INSERT** - Vkládat řádky do tabulek.
- **PROCESS** - Získávání informací o vláknech.
- **REFERENCES** - Nepoužívá se.
- **RELOAD** - Znovunačítání přístupových oprávnění apd.
- **SELECT** - Vybírat záznamy z tabulek.
- **SHUTDOWN** - Ukončovat práci serveru.
- **UPDATE** - Aktualizování řádků v tabulce.
- **USAGE** - Nemá žádná oprávnění.

1.6.2 Přidat jim práva –prakticky

```
GRANT ALL PRIVILEGES ON jmeno_databaze.* TO 'uzivatel'@'localhost'
```

1.7 Změnit práva uživatele

Nejrychlejší smazat a vytvořit znova

```
ALTER USER
```

1.8 Smazat uživatele

```
DROP USER 'uživatel'@'localhost';
```

1.9 Obnovení

```
FLUSH PRIVILEGES;
```