

# SQL jogosultság-kezelés

Privilégiumok

Grant és Revoke

Grant Diagrammok

# Jogosultság-kezelés

- Egy fájlrendszer általában jogosultságokat rendel az általa kezelt objektumokhoz.
  - Tipikusan olvasható, írható, végrehajtási jogosultságokról van szó.
- Ugyanakkor bizonyos „résztvevőkhöz” sorolja ezeket a jogosultságokat.
  - Például rendszergazda, egy korlátozott jogosultságokkal rendelkező felhasználó stb.

## Jogosultságok – (1)

- Az SQL-ben több fajta jogosultság és adatobjektum (pl. relációs táblák) létezik, mint egy tipikus fájlrendszerben.
- Összességében 9 jogosultság, ezek némelyike egy reláció egyetlen attribútumára is megadható.

## Jogosultságok – (2)

- Néhány relációra vonatkozó jogosultság:
  1. **SELECT** = a reláció lekérdezésének joga.
    - Lehet, hogy egyetlen attribútumra vonatkozik.
  2. **INSERT** = sorok beszúrásának joga.
    - ♦ Lehet, hogy egyetlen attribútumra vonatkozik.
  3. **DELETE** = sorok törlésének joga.
  4. **UPDATE** = sorok módosításának a joga.
    - ♦ Szintén lehet, hogy egy attribútumra vonatkozik.

## Példa: jogosultságok

- Az alábbi utasítás esetében:

INSERT INTO sörök(név)

SELECT sör FROM felszolgál

WHERE NOT EXISTS

(SELECT \* FROM sörök  
WHERE név = sör);

azok a sörök, amelyek még nincsenek benne a sörök táblában. A beszúrás után a gyártó értéke NULL.

- Az utasítás végrehajtásához szükséges: SELECT jogosultság a felszolgál és sörök táblába és INSERT jog a sörök tábla név attribútumára vonatkozóan.

# Adatbázis objektumok

- Jogosultságokat nézetekre és materializált nézetekre vonatkozóan is megadhatunk.
- Egy másik fajta jogosultság lehet pl. adatbázis objektumok létrehozásának a joga: pl. táblák, nézetek, triggererek.
- A nézettáblák segítségével tovább finomíthatjuk az adatokhoz való hozzáférést.

## Példa: nézettáblák és jogosultságok

- Tegyük fel, hogy nem szeretnénk SELECT jogosultságot adni az **Dolgozók(név, cím, fizetés)** táblában.
- Viszont a BiztDolg nézettáblán már igen:  

```
CREATE VIEW BiztDolg AS  
  SELECT név, cím FROM Dolgozók;
```
- A BiztDolg nézettáblára vonatkozó kérdésekhez nem kell SELECT jog a Dolgozók táblán, csak a BiztDolg nézettáblán.

## Jogosultsági azonosítók

- A felhasználókat egy *jogosultsági azonosító* (*authorization ID*) alapján azonosítjuk, általában ez a bejelentkezési név.
- Külön jogosultsági azonosító a PUBLIC.
  - A PUBLIC jogosultság minden felhasználó számára biztosítja az adott jogot.



## Jogosultságok megadása

- A magunk készítette objektumok esetében az összes jogosultsággal rendelkezünk.
- Másoknak is megadhatunk jogosultságokat, például a PUBLIC jogosultsági azonosítót is használhatjuk.
- A WITH GRANT OPTION utasításrész lehetővé teszi, hogy aki megkapta a jogosultságot, tovább is adhassa azt.

## A GRANT utasítás

- Jogosultságok megadásának szintaktikája:

GRANT <jogosultságok listája>

ON <reláció vagy másféle objektum>

TO <jogosultsági azonosítók listája>;

- Ehhez hozzáadható:

WITH GRANT OPTION

## Példa: GRANT

- `GRANT SELECT, UPDATE (ár)  
ON Felszolgal  
TO sally;`
- Ez után Sally kérdéseket adhat meg a Felszolgal táblára vonatkozóan és módosíthatja az ár attribútumot.

## Példa: Grant Option

```
GRANT UPDATE ON Felszolgal TO sally  
WITH GRANT OPTION;
```

- Ez után Sally módosíthatja a Felszolgal táblát és tovább is adhatja ezt a jogosultságot.
  - Az UPDATE jogosultságot korlátozottan is továbbadhatja: UPDATE (ár) ON Felszolgal.

# Jogosultságok visszavonása

REVOKE <jogosultságok listája>

ON <reláció vagy más objektum>

FROM <jogosultsági azonosítók listája>;

- Az általunk kiadott jogosultságok ez által visszavonódnak.
  - De ha máshonnan is megkapták ugyanazt a jogosultságot, akkor az még megmarad.

# REVOKE opciói

- A REVOKE utasításhoz a két opció közül valamelyiket még hozzá kell adnunk:
  1. **CASCADE**. Azok a jogosultságok, melyeket az adott ki a visszavonandó jogosultságon keresztül, akitől éppen visszavonjuk az adott jogosultságot, szintén visszavonódnak.
  2. **RESTRICT**. A visszavonás nem hajtódik végre, amíg a visszavonandó jogosultságtól függő jogosultságok is vannak. Először ezeket kell megszüntetni.

# Grant diagrammok

- Pontok = felhasználó/jogosultság/grant option?/tulajdonos-e?
  - UPDATE ON R, UPDATE(a) ON R, és UPDATE(b) ON R három különböző pontot adnak.
  - SELECT ON R és SELECT ON R WITH GRANT OPTION szintén.
- Az  $X \rightarrow Y$  él jelentése: az  $X$  pontot használtuk az  $Y$  pont jogosultságának megadására.

Hogy néznek ki a pontok?

- Az  $AP$  pont az  $A$  felhasználói azonosítójú felhasználó  $P$  jogát jelenti.
  - $P^* = P$  jogosultság grant option opcióval.
  - $P^{**} = a$   $P$  jog tulajdonosi viszonyból származik.
    - $A^{**}$  jelölésből a grant option opció is következik.



## Élek kezelése – (1)

- Amikor  $A$  megadja a  $P$  jogot  $B$ -nek,  $AP^*$  vagy  $AP^{**}$ -ből húzunk egy élt  $BP$ -be.
  - Vagy  $BP^*$  ha grant option is szerepel.
- Ha  $A$  a  $P$  jogosultságnak egy részét adja meg, legyen ez  $Q$  [például UPDATE(a) on R, ahol  $P$  : UPDATE ON R], akkor az él  $BQ$  vagy  $BQ^*$  pontba lesz.

## Élek kezelése – (2)

- **Alapvető szabály:** a  $C$  felhasználó rendelkezik a  $Q$  jogosultsággal egészen addig, amíg létezik út az  $XP^{**}$  pontból  $CQ$ ,  $CQ^*$  vagy  $CQ^{**}$ -ba és  $P$  egy  $Q$ -t magában foglaló jogosultság.
  - Itt  $P$  lehet  $Q$  és  $X$  lehet  $C$ .

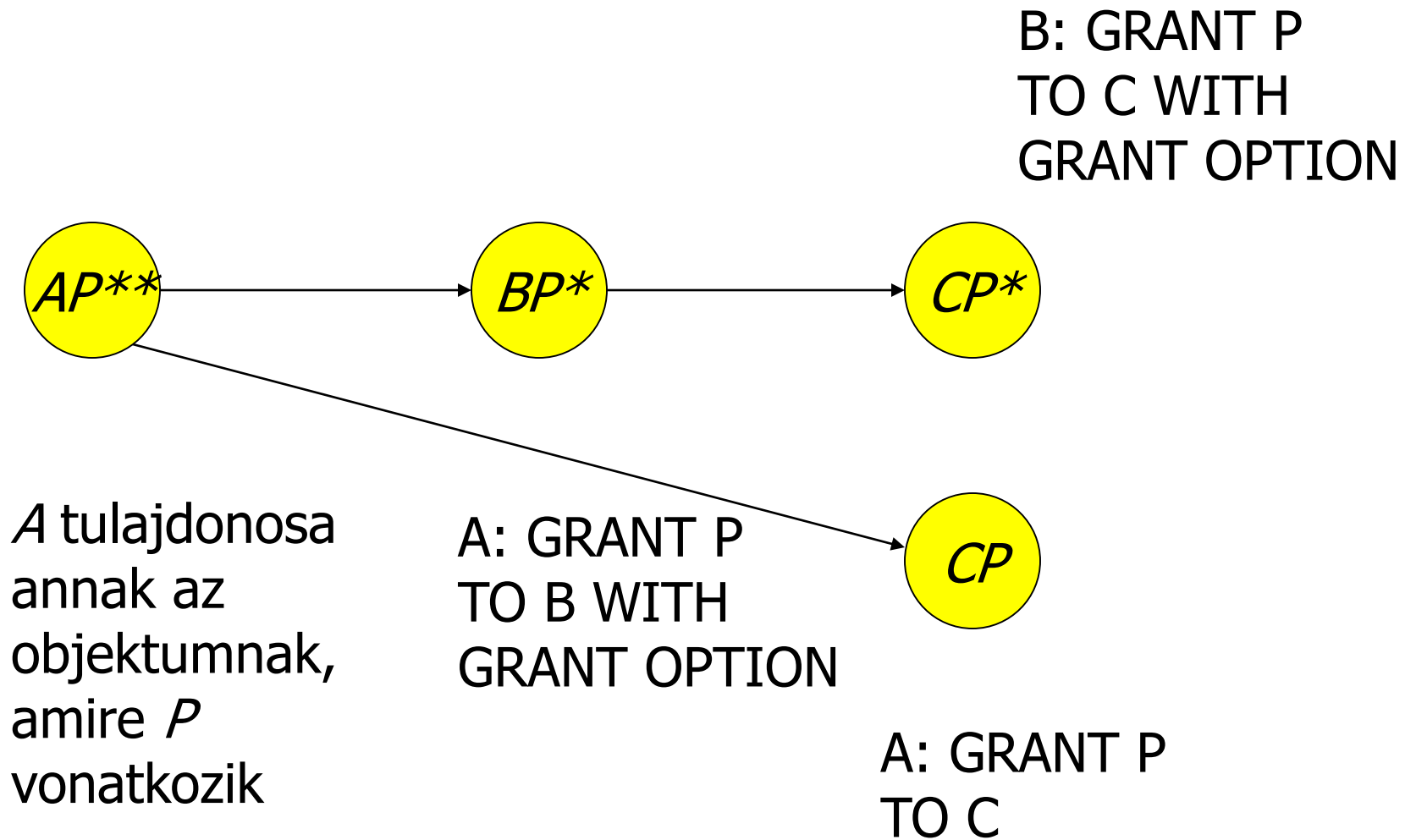
## Élek kezelése – (3)

- Ha  $A$  visszavonja a  $P$  jogot  $B$ -től a CASCADE opcióval, ki kell törölni az  $AP - BP$  élt.
- De, ha  $A$  RESTRICT opciót használ és a  $BP$  pontból indul ki él, akkor vissza kell utasítani a kérést a gráfot változatlanul hagyva.

## Élek kezelése – (4)

- A gráf frissítésekor, minden pontra meg kell nézni, hogy elérhető-e egy \*\* pontból.
- Ha nincs ilyen út, az adott pont egy visszavont jogosultságot reprezentál, és ki kell törölni.

## Példa: Grant diagram



## Példa: Grant Diagram

