Бази даних та інформаційні системи

Тема 19. Адміністрування БД.

СумДУ, каф. КН

2020

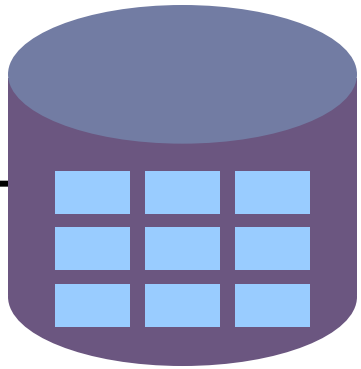
Зміст

- Після завершення заняття ви повинні вміти і знати наступне:
  - Як призначати дозволи (привілеї) на різні об'єкти БД;
  - Як створити користувача;
  - Що таке ролі та як їх передавати.

Контроль прав доступу до БД

Адміністратор БД

Ім’я та пароль
Привілеї



Користувачі

Дозволи

- Безпека БД:
  - Системні дозволи;
  - Дозволи доступу до даних;
- Системні дозволи: дозволи на дії всередині бази даних;
- Об'єктні дозволи: дозволи на дії з даними бази даних;
- Схема: набір об'єктів, таких як таблиці, представлення, об'єкти

Системні дозволи

- Більше 100 типів дозволів.
- Приклади основних дозволів:
  - створити користувача;
  - видалити користувача;
  - видалити таблицю;
  - архівувати таблицю.

Створення користувача

DBA може створити нового користувача за допомогою команди **CREATE USER**

```
CREATE USER user
IDENTIFIED BY   password;
```

```
CREATE USER  demo
IDENTIFIED BY demo;
```

Призначення привілеїв

Після того, як користувач створений, йому можна дати певні дозволи:

```
GRANT privilege [, privilege...]
TO user [, user| role, PUBLIC...];
```

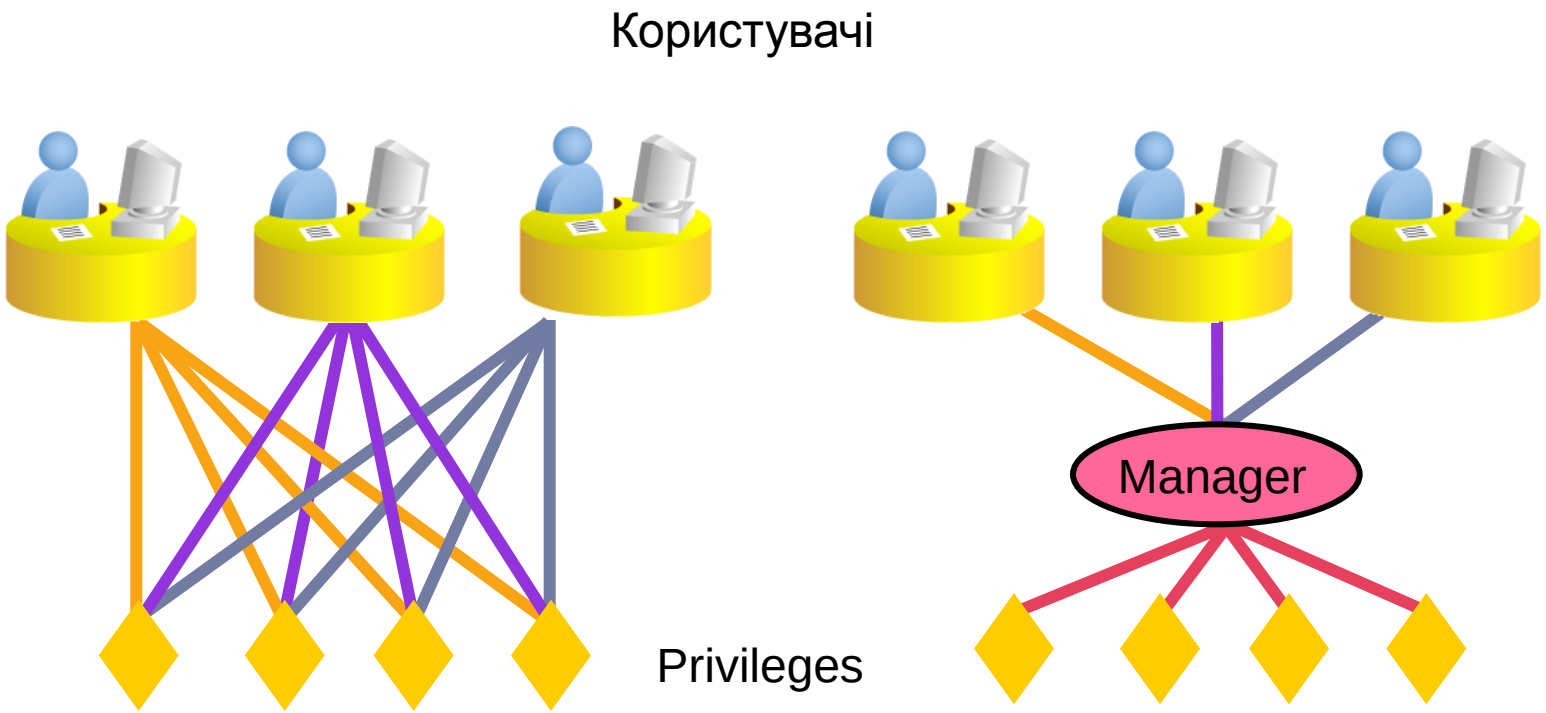
- **CREATE SESSION**
- **CREATE TABLE**
- **CREATE SEQUENCE**
- **CREATE VIEW**
- **CREATE PROCEDURE**

Приклад

DBA надає користувачу **demo** привілеї на створення деяких об'єктів:

```
GRANT   create session, create table,
        create sequence, create view
TO      demo;
```

Використання ролей



Використання ролей

Створення ролі:

```
CREATE ROLE manager;
```

Надання дозволу ролі:

```
GRANT create table, create view
TO manager;
```

Зв'язування ролі і користувача;

```
GRANT manager TO BELL, KOCHHAR;
```

Зміна пароля користувача

DBA створює користувачів і задає їм паролі.

Змінити пароль можна використовуючи **ALTER USER**:

```
ALTER USER demo
IDENTIFIED BY employ;
```

Дозволи та об'єкти БД

Дія	Таблиця	Представлення	Послідовність
ALTER	√		√
DELETE	√	√	
INDEX	√		
INSERT	√	√	
REFERENCES	√		
SELECT	√	√	√
UPDATE	√	√	

Дозволи на рівні об'єктів

- Для різних об'єктів можна призначити різні дозволи.
- Власник об'єкта має всі дозволи по відношенню до об'єкта.
- Власник може встановлювати дозволи доступу до об'єкта для інших користувачів.

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

Приклад передачі дозволів

- Призначення дозволу на читання :

```
GRANT   select
ON      emp
TO      demo;
```

- Призначення дозволів на окремі стовпці певним користувачам і ролям:

```
GRANT   update (department_name, location_id)
ON      departments
TO      demo, manager;
```

Передача дозволів

- Установка дозволів з можливістю їх передачі:

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

- Передача дозволів на читання з псевдонімів таблиці:

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

Як перевірити дозволи

Представлення	Опис
ROLE_SYS_PRIVS	Системні дозволи передані ролі
ROLE_TAB_PRIVS	Дозволи на рівні таблиць, передані ролі
USER_ROLE_PRIVS	Яким ролям належить користувач
USER_SYS_PRIVS	Системні дозволи передані користувачу
USER_TAB_PRIVS_MADE	Об'єктні дозволи на об'єкти користувача
USER_TAB_PRIVS_RECD	Об'єктні дозволи на користувача
USER_COL_PRIVS_MADE	Об'єктні дозволи на стовпці об'єктів користувача
USER_COL_PRIVS_RECD	Об'єктні дозволи на стовпці для користувача

Відкликати привілеї

- Щоб відкликати привілеї використовуйте **REVOKE**.
- Так само можна відкликати привілеї **WITH GRANT OPTION**.

```
REVOKE {privilege [, privilege...]|ALL}
ON     object
FROM   {user[, user...]|role|PUBLIC}
[CASCADE CONSTRAINTS];
```

Приклад

Відкликати привілеї на додавання та читання даних користувачу **demo** з таблиці **DEPT**.

```
REVOKE   select, insert
ON       dept
FROM     demo;
```

Питання

Які з тверджень справедливі?

1. Після того, як користувач створений, йому можуть бути передані будь-які дозволи з використанням GRANT.
2. Користувач може створити роль використовуючи CREATE ROLE і передати через роль всі свої системні і об'єктні дозволи іншому користувачу.
3. Користувачі можуть змінювати свої паролі.
4. Користувач може переглядати свої дозволи і дозволи на свої об'єкти.

Висновки

Привілеї бувають системні та об'єктні.

Привілеї можна передавати.

Речення	Дія
`CREATE USER`	Створити користувача (DBA)
`GRANT`	Дати дозвіл
`CREATE ROLE`	Створити роль (DBA)
`ALTER USER`	Змінити пароль користувача
`REVOKE`	Відкликати дозвіл

Домашнє читання

- Лекція з дисциплини "Администрирование баз данных *и* приложений"