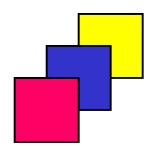
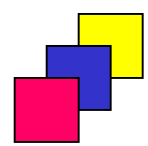
Rozdział 16
Uprawnienia, role, synonimy

Schemat, użytkownicy, autoryzacja użytkowników, uprawnienia systemowe i obiektowe, nadawanie i odbieranie uprawnień, tworzenie ról, przywileje, synonimy

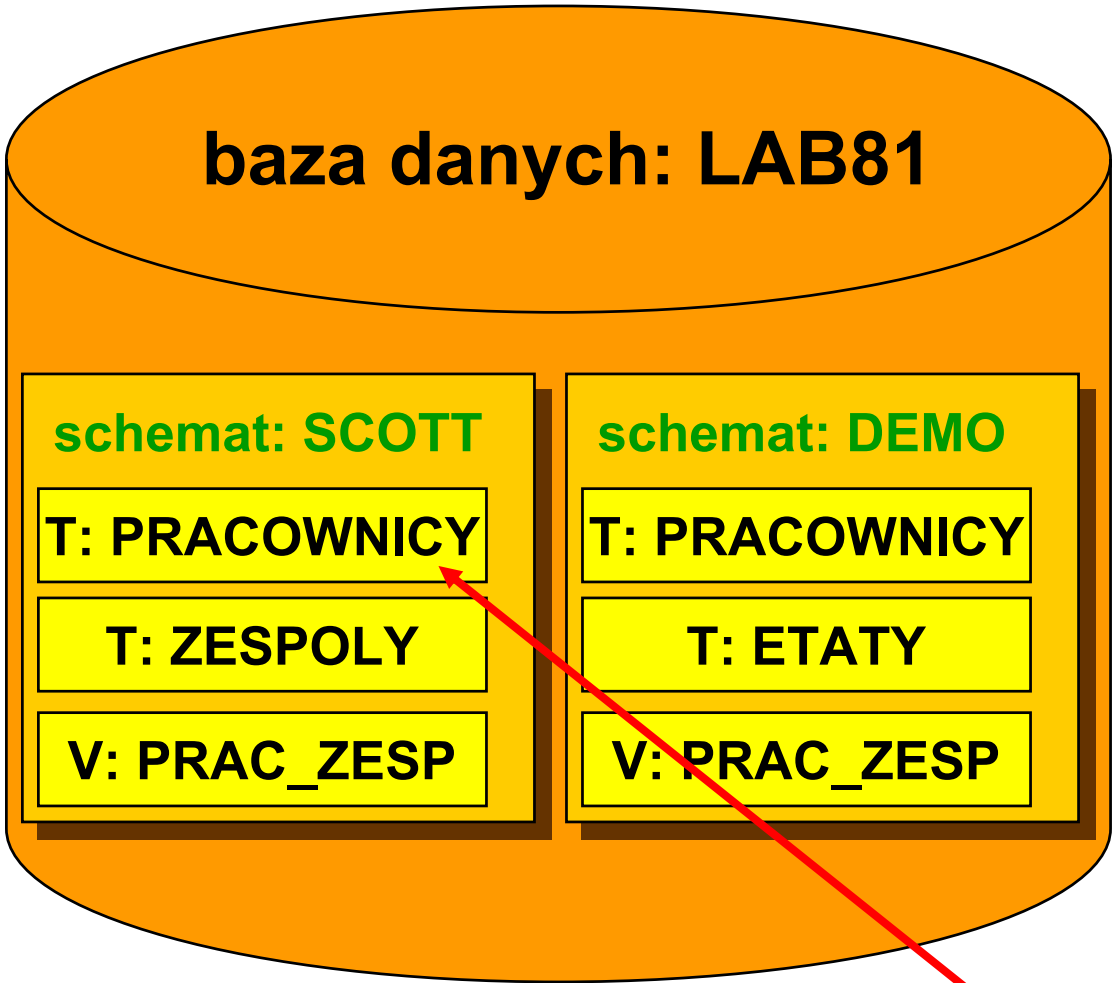


Schematy i użytkownicy

- Każda baza danych Oracle składa się ze schematów.
- Schemat jest zbiorem obiektów, takich jak: tabele, perspektywy, procedury PL/SQL, pakiety, należących do jednego użytkownika.
- W celu przyłączenia się do bazy danych, użytkownik musi podać swoją nazwę i hasło dostępu.
- Schematy tworzone są automatycznie dla każdego użytkownika. Nazwa schematu jest identyczna z nazwą użytkownika.
- Hasło dostępu może być zmieniane przez użytkownika
- Podczas instalacji bazy danych tworzonych jest dwóch wyróżnionych użytkowników: SYS i SYSTEM



Schematy i użytkownicy c.d.



użytkownik: DEMO

użytkownik: SCOTT

SCOTT.PRACOWNICY.NAZWISKO@LAB81

Informacje o użytkownikach

ALL_USERS	**Zawiera nazwy i daty utworzenia wszystkich użytkowników w bazie danych**
DBA_USERS	**Zawiera nazwę, identyfikator, zakodowane hasło, nazwę domyślnej przestrzeni tabel,nazwę tymczasowej przestrzeni tabel, datę utworzenia i profil każdego użytkownika bazy danych**
USER_USERS	**Zawiera nazwę, identyfikator, domyślną przestrzeń tabel, tymczasową przestrzeń tabel i datę utworzenia aktualnego użytkownika**
USER_TS_QUOTAS	**Zawiera nazwę przestrzeni tabel, liczbę bajtów użytych, wymiar kwoty w bajtach lub UNLIMITED, liczbę bloków użytych i wymiar kwoty użytkownika podany w blokach lub UNLIMITED**
DBA_TS_QUOTAS	**To samo co USER_TS_QUOTAS dla wszystkich użytkowników w bazie danych**

```
SELECT * FROM user_ts_quotas;
```

```
SELECT * FROM all_users;
```

Autoryzacja użytkowników

- **Autoryzacja przez bazę danych Oracle - w celu przyłączenia się do bazy danych wymagane jest wprowadzenie nazwy i hasła użytkownika Oracle**
- **Autoryzacja przez system operacyjny - użytkownicy przyłączają się do bazy danych bez wprowadzania swoich nazw i haseł, użytkownik jest identyfikowany na podstawie konta w systemie operacyjnym**
- **Autoryzacja za pomocą usługi sieciowej – DCE, Kerberos, SESAME**
- **Autoryzacja wielowarstwowa za pomocą serwera aplikacji (np. Oracle Wallet)**
- **Autoryzacja administratora bazy danych (przez system operacyjny albo za pomocą plików z hasłami)**

Uprawnienia (przywileje), role, profile

- **Uprawnienia systemowe zezwalają użytkownikowi na wykonywanie w bazie danych operacji określonego typu.**
- **Uprawnienia obiektowe zezwalają użytkownikowi na wykonanie określonych operacji na konkretnym obiekcie bazy danych.**
- **Uprawnienia mogą być kontrolowane przy pomocy ról, które stanowią nazwane zbiory uprawnień.**
- **Uprawnienia do wykorzystania konkretnych zasobów fizycznych systemu (procesor, pamięć, itp.) mogą być kontrolowane za pomocą profili.**

Uprawnienia systemowe - przykłady

CREATE TABLE	**zezwala użytkownikowi na tworzenie relacji w jego własnym schemacie**
DROP ANY VIEW	**zezwala użytkownikowi na usuwanie dowolnych perspektyw**
EXECUTE ANY PROCEDURE	**zezwala użytkownikowi na wykonywanie dowolnych procedur PL/SQL**
CREATE SESSION	**zezwala użytkownikowi na przyłączenie się do bazy danych**
ALTER SYSTEM	**zezwala użytkownikowi na wydawanie poleceń ALTER SYSTEM**

Informacje o aktualnych uprawnieniach systemowych

- **Perspektywy słownika bazy danych**
  - **USER_SYS_PRIVS**
  - **SESSION_PRIVS**

```
SQL> SELECT * FROM USER_SYS_PRIVS;

GRANTEE              PRIVILEGE                                ADM
-------------------- ---------------------------------------- ---------
SYS                  DELETE ANY TABLE                         NO
SYS                  INSERT ANY TABLE                         NO
SYS                  SELECT ANY TABLE                         YES
SYS                  UNLIMITED TABLESPACE                     YES
SYS                  UPDATE ANY TABLE                         NO
SYSTEM               UNLIMITED TABLESPACE                     YES
```

Typy uprawnień obiektowych

SELECT	**zezwala na wydawanie poleceń SELECT FROM dla obiektu (relacja, perspektywa, migawka, sekwencer)**
UPDATE	**zezwala na wydawanie poleceń UPDATE dla obiektu (relacja, perspektywa)**
INSERT	**zezwala na wydawanie poleceń INSERT dla obiektu (relacja, perspektywa)**
ALTER	**zezwala na wydawanie poleceń ALTER dla obiektu (relacja, perspektywa, sekwencer) i CREATE TRIGGER dla obiektu (relacja)**
DELETE	**zezwala na wydawanie poleceń DELETE FROM dla obiektu (relacja, perspektywa) lub TRUNCATE (relacja)**
EXECUTE	**zezwala na wydawanie poleceń EXECUTE dla obiektu (procedura, funkcja)**
INDEX	**zezwala na wydawanie poleceń CREATE INDEX dla obiektu (relacja)**
REFERENCES	**zezwala na wydawanie poleceń CREATE i ALTER TABLE definiujących klucz obcy dla obiektu (relacje)**
ALL	**wszystkie przywileje dla danego obiektu**

Nadawanie uprawnień obiektowych

- **Polecenie GRANT**

```
GRANT ALL [ PRIVILEGES ] | uprawnienie [ , uprawnienie, ... ]
ON obiekt
TO PUBLIC | rola [ , rola, ... ] | użytkownik [ , użytkownik, ... ]
[ WITH GRANT OPTION ];
```

```
GRANT SELECT ON pracownicy
TO DEMO, SCOTT;
```

```
GRANT INSERT(id_prac, nazwisko), UPDATE (placa_pod)
ON pracownicy
TO PUBLIC;
```

Informacje o aktualnych uprawnieniach

USER_TAB_PRIVS	**Uprawnienia obiektowe, których użytkownik jest właścicielem, nadającym lub uprawnionym**
USER_TAB_PRIVS_MADE	**Uprawnienia obiektowe do obiektów będących własnością użytkownika**
USER_TAB_PRIVS_RECD	**Uprawnienia obiektowe, które użytkownik otrzymał**
USER_COL_PRIVS	**Uprawnienia dla atrybutów, których użytkownik jest właścicielem, nadającym lub uprawnionym**
USER_COL_PRIVS_MADE	**Uprawnienia do atrybutów będących własnością użytkownika**
USER_COL_PRIVS_RECD	**Uprawnienia do atrybutów, które użytkownik otrzymał**

```
SELECT * FROM USER_TAB_PRIVS_MADE;
SELECT * FROM USER_TAB_PRIVS_RECD;
```

```
DESC USER_COL_PRIVS
```

Odbieranie uprawnień obiektowych

- **Polecenie REVOKE**

```
ALL [ PRIVILEGES ] | uprawnienie [ , uprawnienie, ... ]
ON obiekt
FROM PUBLIC | rola [ , rola, ... ] | użytkownik [ , użytkownik, ... ]
```

```
REVOKE SELECT ON pracownicy
FROM SCOTT;
```

```
REVOKE ALL ON pracownicy FROM PUBLIC;
```

- **Klauzula CASCADE CONSTRAINTS usuwa wszystkie ograniczenia integralnościowe, zdefiniowane przy pomocy odbieranego przywileju REFERENCES**

Role

- Rola jest nazwanym zbiorem uprawnień zarówno systemowych, jak i obiektowych.
- Role upraszczają zarządzanie uprawnieniami dla dużych zbiorów użytkowników o podobnej charakterystyce (np. pracownicy działu kadr, zarząd, dział marketingu).
- Zmieniając uprawnienia należące do roli, zmienia się uprawnienia wszystkich użytkowników do niej przypisanych.
- W bazie danych zdefiniowane są zawsze role standardowe: CONNECT, RESOURCE, DBA, EXP_FULL_DATABASE, IMP_FULL_DATABASE, SELECT_CATALOG_ROLE, DELETE_CATALOG_ROLE, EXECUTE_CATALOG_ROLE
- Praktycznie każdemu tworzonemu użytkownikowi przydziela się role CONNECT i RESOURCE.

Korzystanie z ról

- **Utworzenie roli**

```
CREATE ROLE nazwa_roli [ IDENTIFIED BY hasło ];
```

- **Włączenie i wyłączenie roli**

```
SET ROLE   nazwa_roli [ IDENTIFIED BY hasło ]
           ALL [ EXCEPT nazwa_roli, ... ]
           NONE;
```

- **Nadanie roli użytkownikowi**

```
GRANT nazwa_roli TO użytkownik [ WITH ADMIN OPTION ];
```

```
CREATE ROLE KIEROWNIK IDENTIFIED BY trudne_haslo;
GRANT ALL ON PRACOWNICY TO KIEROWNIK;
GRANT KIEROWNIK TO Kowalski WITH ADMIN OPTION;
```

Informacje o rolach i uprawnieniach

USER_ROLE_PRIVS	Role przyznane użytkownikowi
ROLE_ROLE_PRIVS	Role przyznane innym rolom
ROLE_SYS_PRIVS	Uprawnienia systemowe przyznane rolom
ROLE_TAB_PRIVS	Uprawnienia obiektowe przyznane rolom
SESSION_ROLES	Role użytkownika aktywowane w bieżącej sesji

```
SELECT ROLE, TABLE_NAME, PRIVILEGE
FROM ROLE_TAB_PRIVS;
```

```
SELECT * FROM SESSION_ROLES;
```

Profile

- **Profile są wykorzystywane do kontroli użytkowania zasobów systemowych i fizycznych.**
- **Zasobami systemowymi są: czas procesora, operacje I/O, czas bezczynności, czas trwania sesji, równoczesne sesje.**
- **Kiedy przekroczony zostanie limit zasobów określony przez profil, wtedy: aktualne polecenie jest wycofywane, dozwolone jest COMMIT i ROLLBACK, sesja zostaje zakończona.**
- **Profile służą również do zarządzania hasłami: pozwalają administratorowi na ustalanie czasu życia haseł, czasu blokowania konta, liczby nieudanych prób zalogowania przed zablokowaniem konta, itp.**

Synonimy

- **Synonim to alternatywna nazwa dla obiektu bazy danych**
  - **Synonimy prywatne - obowiązują tylko jednego użytkownika, mogą być tworzone przez każdego użytkownika.**
  - **Synonimy publiczne - obowiązują członków grupy PUBLIC, czyli wszystkich użytkowników. Tylko użytkownicy dysponujący odpowiednimi prawami mogą tworzyć synonimy publiczne.**

```
CREATE [ PUBLIC ] SYNONYM [ użytkownik ].nazwa_synonimu
FOR [ użytkownik ].nazwa_obiektu;
```

```
DROP [ PUBLIC ] SYNONYM [użytkownik].nazwa_synonimu;
```

```
CREATE SYNONYM EMP FOR SCOTT.EMP;
```