Bezpieczeństwo bazy danych

Wszystkie tabele, widoki, procedury są zabezpieczone przed niepowołanym dostępem już w momencie ich stworzenia. Tylko ich twórca (właściciel) może używać instrukcji **GRANT** do nadawania uprawnień innym użytkownikom, rolom lub procedurom. Tylko twórca procedury może ją wywoływać i tylko on może nadawać uprawnienia do wywoływań.

W Interbase/Firebird występuje również superużytkownik **SYSDBA**, który ma dostęp do wszystkich obiektów znajdujących się w bazie.

Możliwe uprawnienia:

ALL - Select, insert, update, delete i związek klucza głównego z obcym
SELECT – czytanie danych
INSERT – zapis nowych danych
UPDATE – modyfikacja danych
DELETE – usuwanie danych
EXECUTE PROCEDURE – wywołanie procedury
REFERENCES - związek klucza głównego z obcym
role – wszystkie uprawnienia związane z rolą

1. Nadawanie uprawnień

GRANT lista uprawnień ON { nazwa tabeli | nazwa widoku}
TO {obiekt | lista użytkowników | rola | PUBLIC };

Lista uprawnień może zawierać:
SELECT
| DELETE
| INSERT
| UPDATE [(lista kolumn)]
| REFERENCES [(lista kolumn)]

Obiektem może być:
PROCEDURE procname
| TRIGGER trigname
| VIEW viewname
| PUBLIC

Lista użytkowników może zawierać:
[USER] username| rolename

Przykłady:

GRANT SELECT ON FILM TO EMIL;
GRANT REFERENCES ON FILM(id_filmu) TO EMIL;
GRANT UPDATE (imie, nazwisko) ON OSOBA TO PUBLIC;
GRANT INSERT ON FILM TO PROCEDURE WSTAW_FILM;
GRANT INSERT, UPDATE ON FILM TO LIZA;
GRANT INSERT, UPDATE ON FILM TO PROCEDURE WYLICZ_BUDZET;
GRANT ALL ON OSOBA TO LIZA;
GRANT INSERT, UPDATE ON OSOBA TO MAKS, LENA, KAMIL;

GRANT SELECT, INSERT, UPDATE ON DEPARTMENT TO PUBLIC;
(PUBLIC - tylko dla użytkowników, nie dla procedur, widoków itp.)

Rola – mechanizm pozwalający na zarządzanie uprawnieniami dla grupy użytkowników.

Schemat postępowania:
tworzy się rolę, nadaje jej uprawnienia, nadaje się rolę użytkownikom

1. CREATE ROLE rolename;

2. GRANT lista uprawnień TO rolename;

3. GRANT rolename ON tabela|widok TO lista użytkowników;

GRANT lista ról TO {PUBLIC | lista użytkowników}[WITH ADMIN OPTION];

Przykłady:

CREATE ROLE SEKRETARZ;
GRANT ALL ON OSOBA TO SEKRETARZ;
GRANT SEKRETARZ TO LIZA;

Uwaga.
Użycie **WITH GRANT OPTION** pozwala użytkownikowi na przekazywanie uprawnień roli dalej.

2. Odbieranie uprawnień:

REVOKE lista uprawnień ON { nazwa tabeli | nazwa widoku}
FROM { obiekt | lista użytkowników};

Przykłady:

REVOKE SELECT ON FILM FROM EMIL;
REVOKE INSERT ON FILM FROM PROCEDURE WSTAW_FILM;
REVOKE EXECUTE ON PROCEDURE WYLICZ_BUDZET FROM PROCEDURE WSTAW_FILM;
REVOKE ALL ON OSOBA FROM LIZA;

REVOKE lista uprawnień ON tabela|widok FROM lista ról;

REVOKE rola FROM {PUBLIC | lista użytkowników};

REVOKE SEKRETARZ FROM LIZA;

Można zablokować możliwość przekazywania uprawnień:

REVOKE GRANT OPTION FOR lista uprawnień ON tabela FROM użytkownik;

REVOKE GRANT OPTION FOR SELECT ON OSOBA FROM EMIL;