БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

Глаза и уши, охочие до чужих секретов, всегда найдутся.

Л. да Винчи

Технологии баз данных

Содержание

2

- Понятие безопасности базы данных
- Средства обеспечения безопасности базы данных

Безопасность базы данных

3

- *Безопасность базы данных (database security)* – защита базы данных от несанкционированного доступа.
- Различные проблемы безопасности:
  - Правовые, этические аспекты
  - Организационно-административные вопросы
  - Аппаратные и программные средства защиты
  - **Средства защиты данных непосредственно в самой СУБД**

Средства безопасности в СУБД

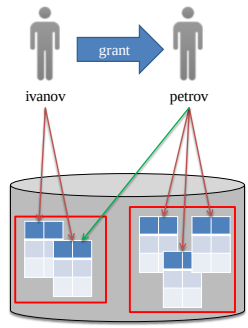
4

- Концептуальные средства
  - Концепция владельца данных
  - Концепция администратора базы данных
  - Привилегии
  - Роли
- Системные средства
  - Шифрование
  - Квоты
  - Аудит

Схема данных и владение данными

5

- База данных имеет *список имен* зарегистрированных пользователей.
  - При подключении к базе данных пользователь вводит свое *имя* и *пароль*.
- С каждым именем пользователя ассоциирована одноименная *схема*.
  - Пользователь может создавать различные объекты только в своей схеме;
  - Пользователь имеет полный доступ к объектам своей схемы.
  - Пользователь может дать права доступа к объектам своей схемы другим пользователям.



Администратор базы данных

6

- *Администратор базы данных (АБД)* – наиболее привилегированный пользователь, управляющий другими пользователями и базой данных.
- Основные обязанности АБД:
  - установка и обновление СУБД и прикладных программных продуктов
  - заведение и консультации пользователей
  - поддержка безопасности и целостности данных
  - управление базой данных на физическом и концептуальном уровне
  - планирование и осуществление резервного копирования и поддержание архивных данных;
  - восстановление базы данных после сбоев
  - оптимизация производительности базы данных.

Привилегии

7

- *Привилегия (privilege)* – это право пользователя выполнять определенный тип команд SQL.
- *Системная привилегия* позволяет выполнять конкретное действие на уровне СУБД, или конкретное действие над конкретным типом объектов схемы. Пользователь получает системные привилегии от АБД, который обладает всеми системными привилегиями.
  - подключиться к базе данных
  - удалить записи из таблицы
  - создать привилегию
  - …
- *Объектная привилегия* позволяет выполнять конкретные действия над конкретным объектом схемы. Пользователь получает объектные привилегии от АБД или других пользователей.
  - выбрать/обновить/удалить записи указанной таблицы
  - создать/удалить/изменить указанную таблицу
  - выполнить указанную хранимую процедуру

Назначение привилегий

8

- Назначение системных привилегий
  - SYSTEM> **grant** create session **to** ivanov;
  - SYSTEM> **grant** create, drop, alter, insert, select, update table **to** petrov;
- Назначение объектных привилегий
  - ivanov> **grant** select, insert, update, delete **on** S, P **to** petrov;
    ivanov> **grant** select **on** S, P **to** sidorov;
    petrov> insert into ivanov.S values ('S007', 'Bond', 'NY', 7);
    sidorov> select * from ivanov.S;
- В: Как пользователь может узнать, к каким объектам он имеет доступ?
  О: Из словаря базы данных.
  - -- Oracle PL/SQL
    select owner, object_name, object_type from all_objects;

Назначение привилегий

9

- Назначение привилегий *с правом их передачи*
  - ivanov> **grant** select, insert, update, delete **on** S, P **to** petrov **with grant option**;
    petrov> insert into ivanov.S values ('S007', 'Bond', 'NY', 7);
    petrov> **grant** select **on** S, P **to** sidorov **with grant option**;
    sidorov> select * from ivanov.S;
    sidorov> **grant** select **on** S, P **to** egorov;
    egorov> select * from ivanov.S;
- Назначение привилегий *на часть объекта схемы*
  - ivanov> **grant** select**(**SID, Name**) on** S **to** petrov;
    petrov> select SID, Name, Rating from ivanov.S;
    Ошибка! Недостаточно привилегий.

Отмена привилегий

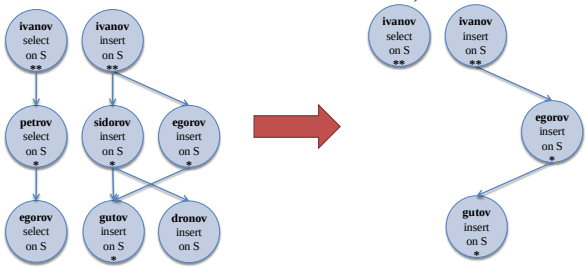
10

- Отмена привилегий, выданных без права их передачи
  - ivanov> **revoke** insert, update, delete on S, P from petrov;
    petrov> insert into ivanov.S values ('S007', 'Bond', 'NY', 7);
    Ошибка! Недостаточно привилегий.
- Отмена права передачи привилегии без отмены самой привилегии
  - ivanov> grant select, insert, update, delete on S, P to petrov with grant option;
    ivanov> **revoke grant option for** insert, update, delete **on** S **from** petrov;
    petrov> grant delete on S to sidorov;
    Ошибка! Недостаточно привилегий.

Отмена привилегий, выданных с правом передачи

11

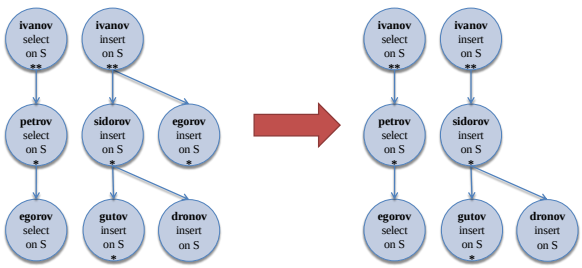
- Каскадная отмена
  - ivanov> **revoke** select **on** S **from** petrov **cascade**;
  - ivanov> **revoke** insert **on** S **from** sidorov **cascade**;



Отмена привилегий, выданных с правом передачи

12

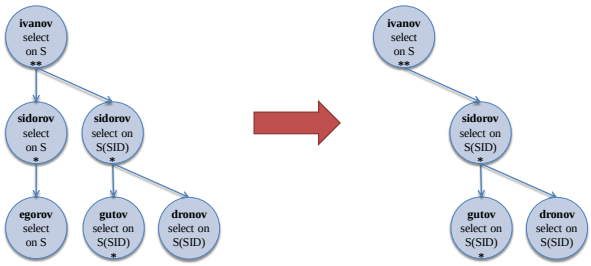
- Запрет отмены
  - ivanov> **revoke** select **on** S **from** petrov **restrict**;
  - ivanov> **revoke** insert **on** S **from** sidorov **restrict**;



Отмена привилегий, выданных с правом передачи

13

- Отмена привилегии не отменяет ее частный случай
  - ivanov> **revoke** select **on** S **from** sidorov **cascade**;



Отмена привилегий, выданных с правом передачи

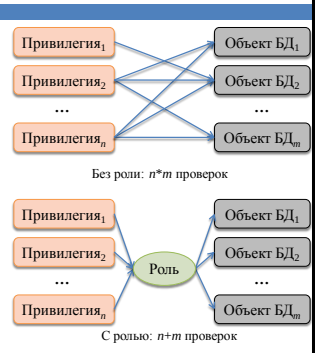
14

- Отмена права передачи привилегии не отменяет саму привилегию
  - ivanov> grant select on S to sidorov with grant option;
    sidorov> grant select on S to egorov;
    ivanov> **revoke grant option for** select on S **from** sidorov **cascade**;

Роли

15

- *Роль (role)* – именованная совокупность объектных или/и системных привилегий, которые можно назначить пользователям или другим ролям.
- Получателю роли может быть присвоено *несколько* ролей.
- Роли упрощают контроль безопасности данных.



Роли

16

- Создание роли
  - **create role** boss_role;
  - **create role** clerk_role;
- Наделение роли привилегиями
  - **grant** select, insert, update, delete **on** S, P, SP **to** boss_role;
  - **grant** select **on** S, P, SP **to** clerk_role;
- Назначение ролей пользователям
  - **grant** boss_role **to** ivanov;
  - **grant** clerk_role **to** petrov, sidorov, egorov;
- Отмена роли пользователя
  - **revoke** clerk_role **from** egorov;

Системные средства безопасности базы данных

17

- *Шифрование* данных в базе данных на основе различных алгоритмов.
- *Квоты* – предельные значения аппаратных ресурсов, выделяемых пользователям.
- *Аудит* – регистрация действий пользователей базы для выявления попыток несанкционированного использования данных.

Пример: назначение квот

18

```
CREATE USER admin_user
        IDENTIFIED BY password123
        DEFAULT TABLESPACE dbms
        TEMPORARY TABLESPACE temp
        QUOTA UNLIMITED ON dbms
        QUOTA 10M ON temp
        QUOTA 5M ON system
        PROFILE admin_profile;
```

Пример: создание профиля

19

```
CREATE PROFILE admin_profile
        LIMIT   SESSIONS_PER_USER UNLIMITED
        CPU_PER_SESSION UNLIMITED
        CPU_PER_CALL 3000
        CONNECT_TIME 45
        LOGICAL_READS_PER_SESSION DEFAULT
        LOGICAL_READS_PER_CALL 1000
        FAILED_LOGIN_ATTEMPTS 5
        PASSWORD_LIFE_TIME 60
        PASSWORD_REUSE_TIME 60
        PASSWORD_REUSE_MAX UNLIMITED
        PASSWORD_VERIFY_FUNCTION verify_function
        PASSWORD_LOCK_TIME 1/24
        PASSWORD_GRACE_TIME 10;
```


Заключение

20

- Безопасность базы данных – защита базы данных от несанкционированного доступа.
- Средства обеспечения безопасности данных в СУБД:
  - концепция владения данными (пользователь может создавать в данные только в собственной схеме и имеет к ним полный доступ)
  - концепция АБД (наиболее привилегированный пользователь)
  - привилегии – права на выполнение определенных команд SQL
  - роли – именованные совокупности привилегий.