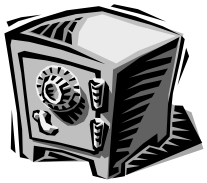
Безопасность базы данных в СУБД Oracle



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

Леонардо да Винчи

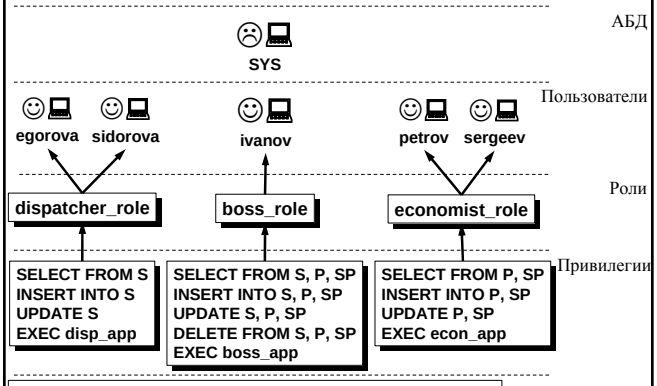
Содержание

- Понятие безопасности базы данных
- Средства безопасности базы данных данных

Безопасность базы данных

- *Безопасность базы данных (database security)* – защита базы данных от несанкционированного доступа.
- Безопасность *данных* обеспечивается средствами контроля и защиты базы данных *на уровне объектов схемы*: список пользователей, имеющих доступ к определенным объектам схемы, и разрешенные данным пользователям операции.
- *Системная* безопасность обеспечивается средствами контроля и защиты базы данных *на системном уровне*: имена и пароли учетных записей, ограничение размера дискового пространства для хранения объектов схемы пользователя и др.

Средства безопасности данных



Администратор базы данных

- *Администратор базы данных* – наиболее привилегированный пользователь, управляющий базой данных.
- Основные обязанности АБД:
  - установка и обновление Oracle Server и прикладных программных продуктов;
  - заведение и консультации пользователей;
  - поддержка безопасности и целостности данных;
  - управление физической и логической структурой базы данных;
  - планирование и осуществление резервного копирования и поддержание архивных данных;
  - восстановление базы данных после сбоев;
  - оптимизация производительности базы данных.

Пользователи и схемы

- 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 создает в своей схеме различные объекты и имеет к ним полный доступ. Пользователь может дать права доступа к объектам своей схемы другим пользователям.
- Создание пользователя:

```
CREATE USER ivanov
        IDENTIFIED BY thisispassword
        DEFAULT TABLESPACE dbms
        PROFILE BOSS_PROFILE;
GRANT CONNECT TO ivanov;
```

Привилегии

- *Привилегия (privilege)* – это право пользователя выполнять определенный тип предложений SQL (создать сессию, создать таблицу в своей схеме, выбрать строки таблицы из чужой схемы и др.).
- *Системная привилегия* позволяет пользователю выполнять конкретное действие на уровне системы, или конкретное действие над конкретным типом объектов схемы (подключиться к базе данных, удалить строки любой таблицы, создать табличное пространство, создать привилегию и др.). Всеми системными привилегиями обладает только АБД.
- *Объектная привилегия* позволяет пользователю выполнять конкретные действия над конкретным объектом схемы (удалить строки в указанной таблице и др.). Пользователь получает объектные привилегии от АБД или других пользователей.

Корпоративные системы баз данных © М.Л. Цымблер 7

Пример: назначение и отмена системных привилегий

```
GRANT create database link TO petrov;
GRANT create snapshot TO ivanov;
GRANT create, drop, alter role TO ivanov, petrov;
GRANT create, delete, backup, insert,
      update, lock, select any table TO admin
      WITH GRANT OPTION;
REVOKE create snapshot FROM ivanov;
```

Корпоративные системы баз данных © М.Л. Цымблер 8

Пример: назначение и отмена объектных привилегий

```
-- Пользователь admin
GRANT select, insert, delete, update
      ON s, p, sp
      TO ivanov, petrov;
REVOKE delete
      ON s, p, sp
      FROM petrov;
-- Пользователь ivanov
SELECT *
FROM admin.s;
```

Корпоративные системы баз данных © М.Л. Цымблер 9

Роли

- *Роль (role)* – именованная совокупность объектных или/и системных привилегий, которые можно назначить пользователям, приложениям базы данных или другим ролям.
- Получателю роли может быть присвоено *несколько* ролей.
- Роль может быть создана с *паролем*.
- Роль *приложения* получает все привилегии, необходимые для его работы. При запуске приложение активизирует нужную роль. В силу этого пользователь приложения не обязан знать пароль роли приложения.

Пример: назначение и отмена привилегий с помощью ролей

```
CREATE ROLE boss_role;
CREATE ROLE econ_role;
CREATE ROLE admin_role IDENTIFIED BY thisispassword;
GRANT insert, delete, update ON s, p, sp
        TO economist_role, boss_role;
GRANT all ON s, p, sp TO admin_role
        WITH GRANT OPTION;
REVOKE delete ON s, p, sp FROM econ_role;
GRANT execute ON change_rating TO boss_role;
GRANT boss_role TO ivanov;
GRANT economist_role TO petrov;
```


Средства системной безопасности

- АБД использует следующие средства системной безопасности:
  - Дисковые квоты
  - Профили пользователей
  - Аудит пользователей

Дисковые квоты

- АБД может ограничить размер дискового пространства для конкретного пользователя базы данных.
  - Квота на объем объектов схемы, хранящихся в табличном пространстве DEFAULT.
  - Квота на объем временных данных, создаваемых при выполнении запросов в табличном пространстве TEMPORARY.

Пример: назначение дисковых квот

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


Профили пользователей

- *Профиль (profile)* – именованная совокупность ограничений на доступные пользователю системные ресурсы:
  - число одновременных сессий
  - время процессора (доступное сессии или запросу пользователя)
  - число дисковых операций (доступное сессии или запросу пользователя)
  - время простоя
  - время сессии
  - парольные ограничения (число неудачных попыток регистрации, срок действия, возможность повторного использования, простота пароля).

Пример: создание профиля

```
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;
```


Аудит пользователей

- *Аудит (audit)* – регистрация действий пользователей для выявления попыток несанкционированного использования базы данных.
- *Аудит запросов SQL* – регистрация действий над определенными типами объектов схем (например, таблицами).
- *Аудит системных привилегий* – регистрация определенных действий над определенными типами объектов схем (например, создание таблиц).
- *Аудит объектов схемы* – регистрация определенных действий над определенными объектами схем (например, выборка из конкретной таблицы).

Журнал аудита

- Информация об аудите пользователей сохраняется в *журнале аудита (audit trial)*, который представляет собой таблицу SYS.AUD$.
- АБД создает ряд представлений журнала аудита для словаря базы данных.

```
SELECT user_name, obj_name, action_name
FROM DBA_AUDIT_OBJECTS;
```