

Управление доступом пользователей

Защита информации в БД

Темы

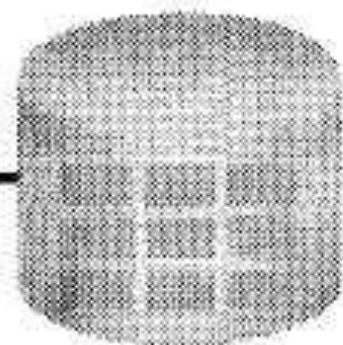
- **Создание пользователей**
- **Создание ролей для упрощения реализации и сопровождения модели безопасности базы данных.**
- **Предоставление и отмена объектных привилегий с помощью команд GRANT и REVOKE**

Управление доступом пользователей

Администратор
базы данных



Имя пользователя и пароль
Привилегии



Пользователи



Привилегии

- **Безопасность базы данных**
- **Безопасность системы**
- **Безопасность данных**
- **Системные привилегии: получение доступа к базе данных**
- **Объектные привилегии: манипулирование содержимым объектов базы данных**
- **Схема: совокупность таких объектов, как таблицы, представления и последовательности, владельцем которых является конкретный пользователь.**

Системные привилегии

- **Имеется более 80 привилегий.**
- **Администратор базы данных (АБД) имеет системные привилегии высокого уровня.**
 - **Создание новых пользователей**
 - **Удаление пользователей**
 - **Удаление таблиц**
 - **Резервное копирование таблиц**

Создание пользователей: синтаксис

Администратор базы данных создает пользователей с помощью команды **CREATE USER**.

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

```
SQL> CREATE    USER    scott  
  2  IDENTIFIED BY tiger;  
User created.
```

Системные привилегии пользователя

- Сразу после создания пользователя АБД может предоставить ему конкретные системные привилегии.

```
GRANT privilege [, privilege...]  
TO user [, user...];
```

- Разработчик приложения может иметь следующие системные привилегии:
 - CREATE SESSION
 - CREATE TABLE
 - CREATE SEQUENCE
 - CREATE VIEW
 - CREATE PROCEDURE

Предоставление системных привилегий: пример

Администратор базы данных может предоставить пользователю конкретные системные привилегии

```
SQL> GRANT create table, create sequence, create view  
2 TO scott;  
Grant succeeded.
```


Что такое роль?



Пользователи

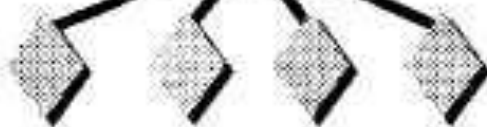


Предоставление
привилегий без роли



Менеджер

Привилегии



Предоставление
привилегий с ролью

Создание роли и предоставление ей привилегий: пример

```
SQL> CREATE ROLE manager;  
Role created.
```

```
SQL> GRANT create table, create view  
2 to manager;  
Grant succeeded.
```

```
SQL> GRANT manager to BLAKE, CLARK;  
Grant succeeded.
```

Изменение пароля

- Пароль инициализируется при создании пользователя.
- Пользователи могут менять свои пароли с помощью команды **ALTER USER**.

```
SQL> ALTER USER scott  
2 IDENTIFIED BY lion;  
User altered.
```

Объектные привилегии

Привилегии на объект	Таблица	Представление	Последовательность	Процедура
ALTER	√		√	
DELETE	√	√		
EXECUTE				√
INDEX	√			
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

Объектные привилегии: синтаксис

- Объектные привилегии варьируются от объекта к объекту.
- Владелец объекта имеет все привилегии на этот объект.
- Владелец может предоставлять конкретные привилегии на принадлежащий ему объект.

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

Предоставление объектных привилегий: пример

- Предоставление привилегии на выполнение запроса к таблице EMP.

```
SQL> GRANT  select
      2  ON    emp
      3  TO    sue, rich;
Grant succeeded.
```

- Предоставление привилегий пользователям и ролям на обновление конкретных столбцов.

```
SQL> GRANT  update (dname, loc)
      2  ON    dept
      3  TO    scott, manager;
Grant succeeded.
```

ИСПОЛЬЗОВАНИЕ КЛЮЧЕВЫХ СЛОВ WITH GRANT OPTION и PUBLIC

- Предоставление полномочий пользователю на передачу привилегий.

```
SQL> GRANT    select, insert
  2  ON        dept
  3  TO        scott
  4  WITH GRANT OPTION;
Grant succeeded.
```

- Предоставление разрешения всем пользователям системы на выборку данных из таблицы DEPT, принадлежащей пользователю Алисе (ALICE).

```
SQL> GRANT    select
  2  ON        alice.dept
  3  TO        PUBLIC;
Grant succeeded.
```

Проверка предоставленных привилегий

Таблица базы данных	Описание
ROLE_SYS_PRIVS	Системные привилегии, предоставленные ролям
ROLE_TAB_PRIVS	Привилегии на таблицы, предоставленные ролям
USER_ROLE_PRIVS	Роли, доступные пользователю
USER_TAB_PRIVS_MADE	Объектные привилегии, предоставленные пользователем на его объекты
USER_TAB_PRIVS_RECD	Объектные привилегии, предоставленные пользователю
USER_COL_PRIVS_MADE	Привилегии, предоставленные пользователем на столбцы его объектов
USER_COL_PRIVS_RECD	Привилегии на столбцы чужих объектов, предоставленные пользователю

Отмена объектных привилегий: СИНТАКСИС

- Для отмены привилегий, предоставленных другим пользователям, используется команда REVOKE.
- Одновременно отменяются привилегии, предоставленные другим пользователям посредством опции WITH GRANT OPTION.

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

Отмена объектных привилегий: пример

Отмена пользователем Алисой привилегий **SELECT** и **INSERT**, предоставленных пользователю Скотту (Scott) на таблицу **DEPT**.

```
SQL> REVOKE  select, insert
  2  ON      dept
  3  FROM    scott;
Revoke succeeded.
```

Заключение

CREATE USER	Позволяет администратору базы данных создавать пользователей
GRANT	Позволяет пользователю предоставлять другим пользователям привилегии на доступ к своим объектам
CREATE ROLE	Позволяет администратору базы данных создавать именованные наборы привилегий
ALTER USER	Позволяет пользователям менять свои пароли
REVOKE	Отменяет привилегии на объект, предоставленные пользователям