Курс «Базы данных»

Тема. Системные привилегии

Барабанщиков
Игорь Витальевич

План лекции

- Безопасность БД
- Учетная запись пользователя БД
- Создание пользователей БД
- Системные привилегии
- Предоставление и отмена системных привилегий

Безопасность БД

- Современные СУБД работают в **многопользовательском режиме**.
- В многопользовательской среде необходимо обеспечить безопасность:

  - ***доступа пользователей*** к базе данных;

  - ***использования*** базы данных.
- Этим занимается администратор БД.

Защита сервера Oracle

Средства защиты сервера СУБД Oracle позволяют делать следующее:

- **Управлять доступом** к базе данных
- **Предоставлять право доступа** к конкретным объектам базы данных
- **Проверять выданные и полученные *привилегии*** с помощью словаря базы данных

Учетная запись пользователя

- Чтобы получить доступ к БД, пользователь должен указать корректную учетную запись пользователя базы данных и **успешно аутентифицироваться**.
- У каждого пользователя БД должна быть *уникальная учетная запись* базы данных.
- Oracle рекомендует это, чтобы:

  - избежать потенциальных дыр в системе безопасности

  - обеспечить содержательные данные для аудита

Данные учетной записи

Учетная запись пользователя БД содержит:

- Уникальное имя пользователя
- Метод аутентификации
- Табличное пространство по умолчанию
- Временное табличное пространство
- Профиль пользователя
- Группа потребителей
- Статус блокирования

Аутентификация и авторизация

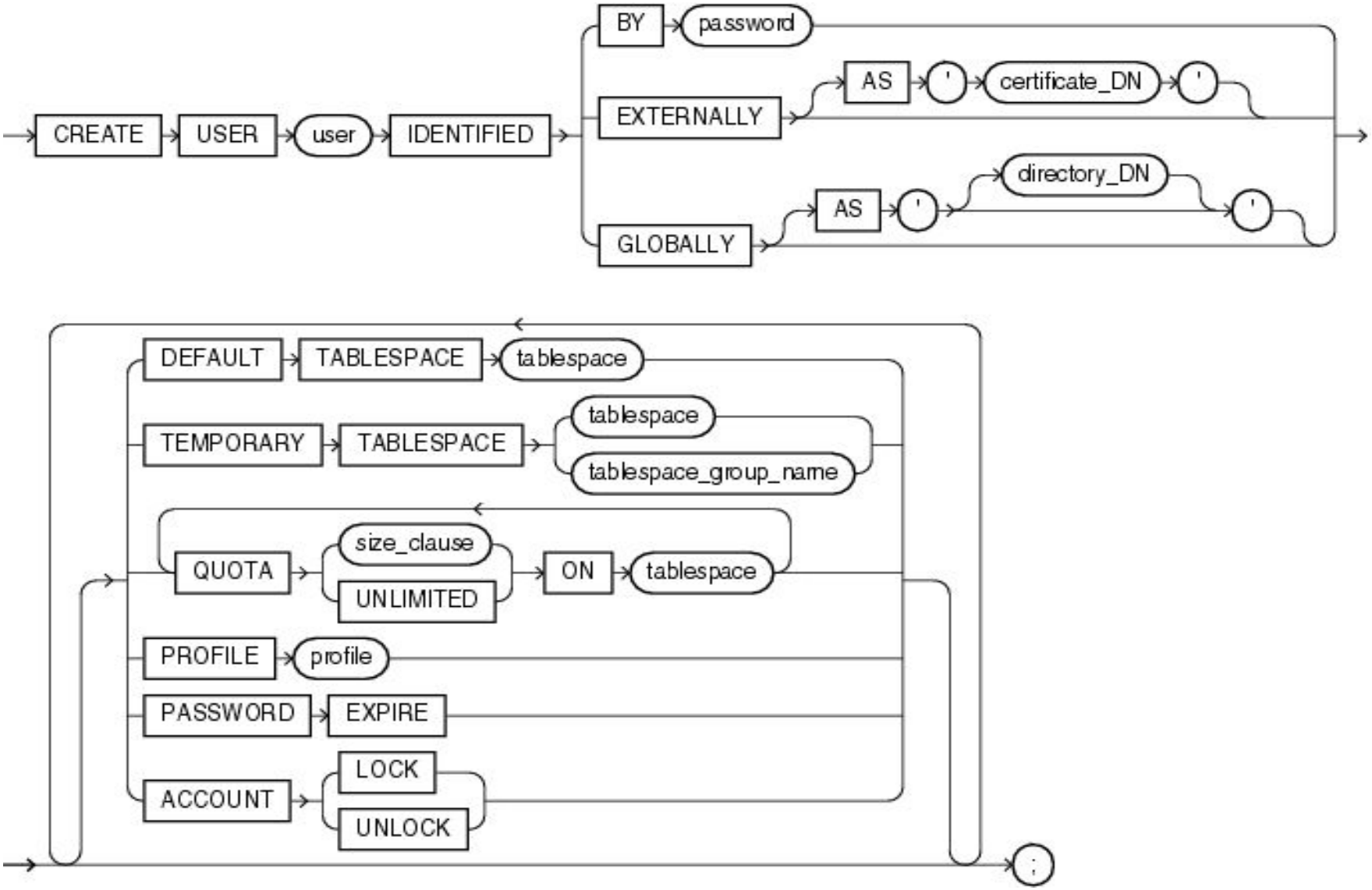
процедура проверки подлинности

например: аутентификация по паролю
проверка подлинности пользователя путём сравнения введённого им пароля с паролем, который хранится в БД

1. Предоставление прав на выполнение определённых действий определённому лицу или группе лиц
2. Процесс проверки (подтверждения) данных прав при попытке выполнения этих действий

например: создание таблиц, триггеров

Синтаксис CREATE USER



Пример. Создание пользователя

Пользователь БД Oracle может быть создан SQL-оператором **CREATE USER:**

```
CREATE USER ivan
  IDENTIFIED BY password
  DEFAULT TABLESPACE data_ts
  QUOTA 100M ON test_ts
  TEMPORARY TABLESPACE temp_ts
  PROFILE clerk
  ACCOUNT unlock;
```

Привилегии

- При создании пользователя БД командой CREATE USER он **не получает никаких прав** на выполнение каких-либо действий в БД.
- Чтобы пользователь получил права на выполнение действий в БД ему **надо выдать привилегии.**
- *Привилегии* **определяют, что может делать** пользователь в БД.

Привилегии

Привилегии — это набор действий (операций), которые пользователи могут выполнять над объектами БД.

Все привилегии делятся на 2 группы:

- **Системные привилегии:** разрешает выполнение операций над целым классом объектов.
- **Объектные привилегии:** выполнение операций, манипулирование содержимым конкретного объекта БД.

Системные привилегии

- Имеется более 100 системных привилегий.
- Системные привилегии выдаются администратором БД

Примеры

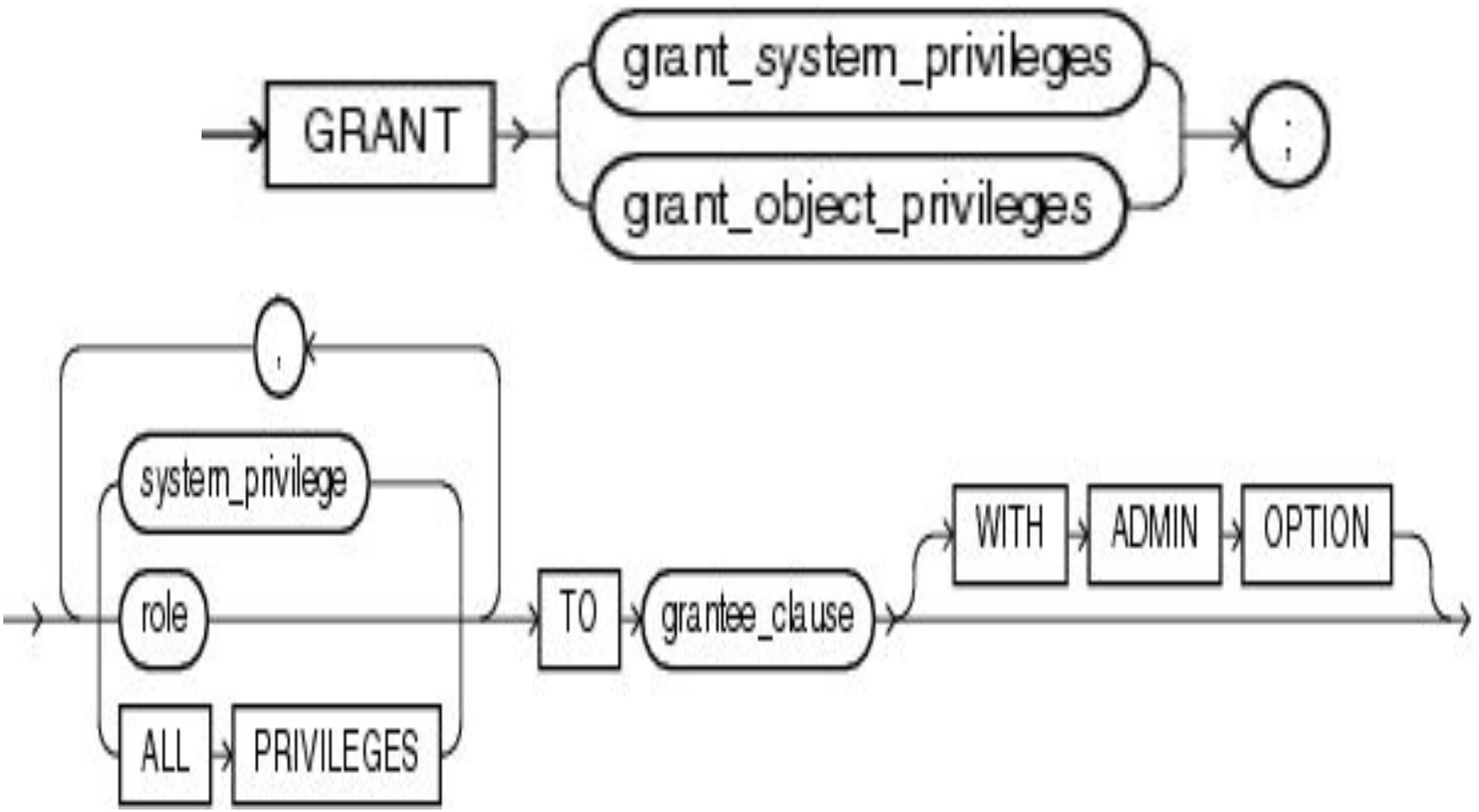
- CREATE USER - привилегия создавать других пользователей (эта привилегия обязательна для роли ДБА)
- DROP USER - Привилегия на удаление другого пользователя
- DROP ANY TABLE - Привилегия на удаление таблицы в любой схеме
- SELECT ANY TABLE – привилегия на чтение данных из любой таблицы БД (в любой схеме)

Назначение системных привилегий

- После того как пользователь создан, администратор БД может предоставить этому пользователю **конкретные системные привилегии.**
- Для предоставления системных привилегий пользователям администратор базы данных использует команду **GRANT**.

```
GRANT privilege [, privilege...]
TO user [, user| role, PUBLIC...];
```

Синтаксис команды GRANT



Пример системных привилегий разработчика БД

Системная привилегия	Разрешенные операции
CREATE PROCEDURE	Право создавать в схеме пользователя хранимую процедуру, функцию или пакет.
CREATE VIEW	Право создавать в схеме пользователя представление.
CREATE SEQUENCE	Право создавать в схеме пользователя последовательность.
CREATE TABLE	Право создавать в схеме пользователя таблицы.
CREATE SESSION	Право устанавливать соединения с базой данных.

Системные привилегии: ALTER

Привилегия	Описание
ALTER DATABASE	Позволяет изменять саму БД
ALTER USER	Позволяет изменять пользователя и его параметры (пароль, профиль, роль и т.д.)
ALTER PROFILE	Позволяет изменять профили
ALTER TABLESPACE	Позволяет изменять табличные пространства

Для любого объекта – ANY:

ALTER ANY PROCEDURE	Разрешает изменение любой хранимой функции процедуры или пакета в любой схеме
ALTER ANY ROLE	Разрешает изменение любой роли БД
ALTER ANY SEQUENCE	Разрешает изменение любой последовательности в БД
ALTER ANY TABLE	Разрешает изменение любой таблицы или представления в схеме БД
ALTER ANY TRIGGER	Позволяет разрешать, запрещать компилировать любой триггер в любой схеме БД
ALTER ANY INDEX	Разрешает изменение любого индекса в любой схеме

Системные привилегии: CREATE

Создавать объект в любой схеме:

- CREATE ANY PROCEDURE;
- CREATE ANY SEQUENCE;
- CREATE ANY TABLE;
- CREATE ANY TRIGGER;
- CREATE ANY VIEW;
- CREATE ANY INDEX;

Создавать объект в конкретной схеме

- CREATE PROCEDURE;
- CREATE SEQUENCE;
- CREATE TABLE;
- CREATE TRIGGER;
- CREATE VIEW;
- CREATE INDEX;

- CREATE SESSION
- CREATE ROLE

Системные привилегии: DROP

Удаление объектов в любой схеме:

- DELETE ANY TABLE;

- DROP ANY PROCEDURE;
- DROP ANY SEQUENCE;
- DROP ANY TABLE;
- DROP ANY TRIGGER;
- DROP ANY VIEW;
- DROP ANY INDEX;

Удаление объектов в конкретной схеме

- DROP PROCEDURE;
- DROP SEQUENCE;
- DROP TABLE;
- DROP TRIGGER;
- DROP VIEW;
- DROP INDEX;

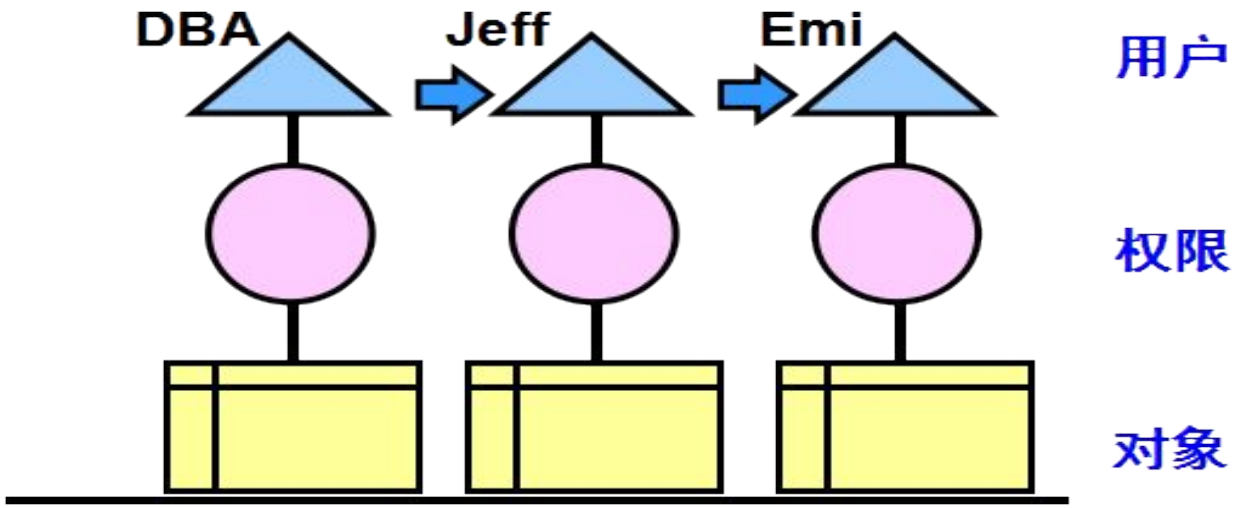
Пример. Назначение системных привилегий

Администратор БД может назначить пользователю конкретные системные привилегии:

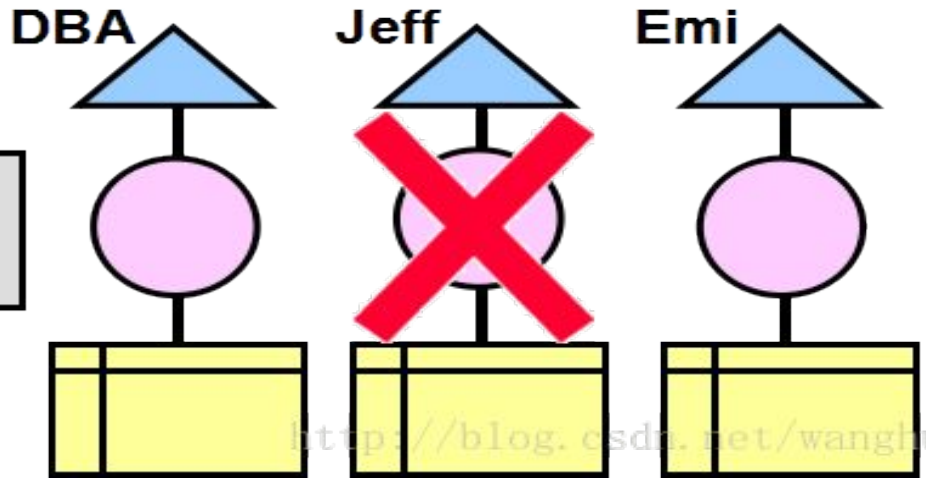
```
SQL>GRANT  create table,  create view,
    2   create procedure TO  petr;

SQL> GRANT select any table TO ivan
    2    WITH  ADMIN  OPTION;
```

Отмена системных привилегий, выданных с ADMIN OPTION

GRANT



REVOKE




```
REVOKE CREATE
TABLE FROM jeff;
```

Итоги

- Управление доступом к БД выполняется на основе учетных записей пользователей и прав доступа (привилегий).
- В СУБД Oracle имеется 2 вида привилегий: системные и объектные.
- Системные привилегии выдаются администратором БД.