БЛОК 6. УПРАВЛЕНИЕ ДОСТУПОМ

ПРИВИЛЕГИИ

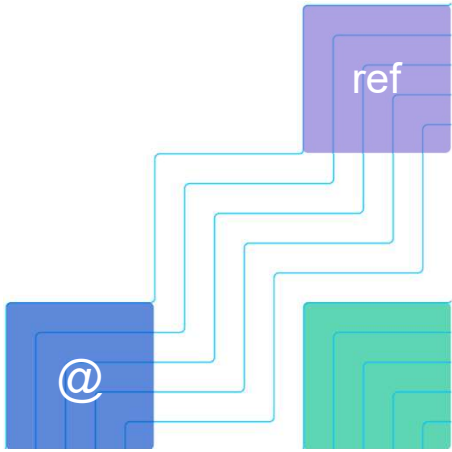
{ }

begin

ЦЕЛЬ УРОКА

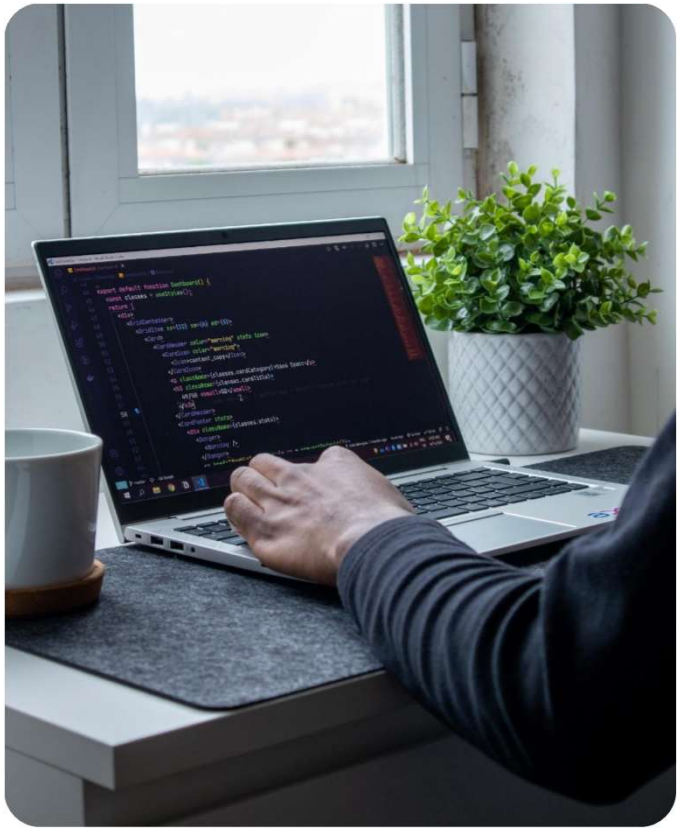
01

Понять, что такое привилегии и как правильно их настроить



СОДЕРЖАНИЕ УРОКА

1. Привилегии
2. Варианты настройки
3. Практика



ПРИВИЛЕГИИ

Набор действий, которые пользователь может совершать с объектами БД:

```
SELECT
INSERT
UPDATE
DELETE
TRUNCATE
CREATE
CONNECT
EXECUTE
```

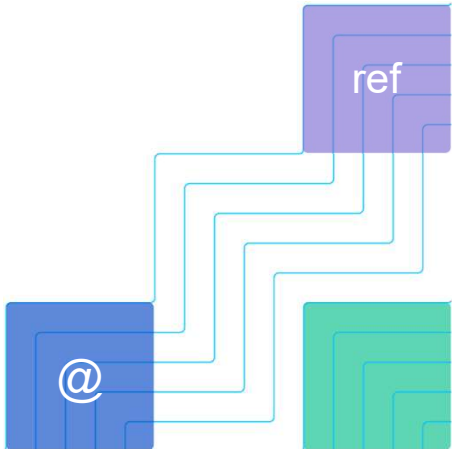
Набор прав, применимых к определённому объекту, зависит от типа объекта (таблица, функция и т. д.)

https://postgrespro.ru/docs/postgresql/14/sql-grant

ПРИВИЛЕГИИ

Суперпользователи

→ полный доступ ко всем объектам — проверки не выполняются, за исключением прав на вызов ХП (security definer/invoker)



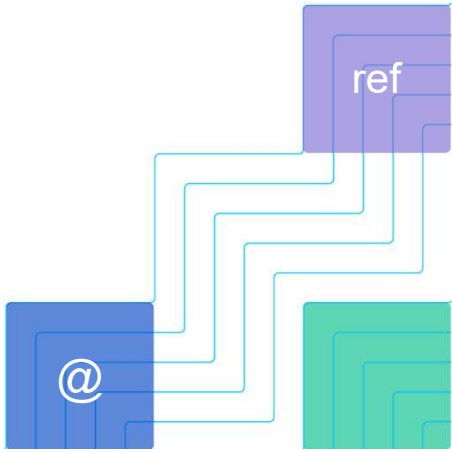
ПРИВИЛЕГИИ

Владельцы

→ доступ в рамках выданных привилегий (изначально получает полный набор)
а также действия, не регламентируемые привилегиями, например: удаление, выдача и отзыв привилегий и т. п.

Остальные роли

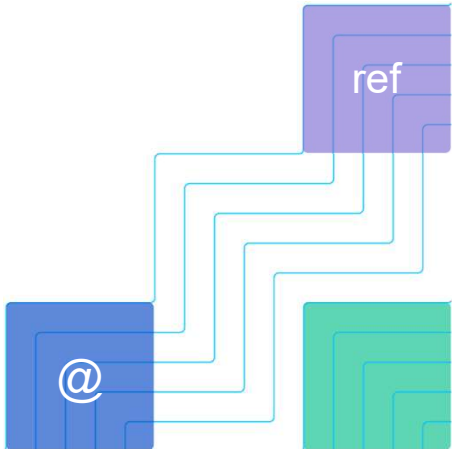
→ доступ исключительно в рамках выданных привилегий



ВЫДАЧА ПРИВИЛЕГИЙ

```
GRANT SELECT ON mytable TO PUBLIC;
GRANT SELECT, UPDATE, INSERT ON mytable TO admin;
GRANT SELECT (col1), UPDATE (col1) ON mytable TO
miriam_rw;
```

https://postgrespro.ru/docs/postgresql/14/sql-revoke



КАК ВЫГЛЯДЯТ ПРИВИЛЕГИИ

Посмотрим гипотетический пример:

```
\dp mytable     ----> miriam=arwdDxt

имя_роли=xxxx -- права, назначенные роли

        =xxxx -- права, назначенные PUBLIC

         r -- SELECT ("read", чтение)

            w -- UPDATE ("write", запись)

            a -- INSERT ("append", добавление)

            d -- DELETE

            D -- TRUNCATE

            x -- REFERENCES

            t -- TRIGGER

            X -- EXECUTE

            U -- USAGE

            C -- CREATE

            c -- CONNECT

            T -- TEMPORARY

arwdDxt -- ALL PRIVILEGES (все права для таблиц; для других объектов другие)

        * -- право передачи заданного права
        /yyyy -- роль, назначившая это право
```

ПЕРЕДАЧА ПРАВ НА ПРИВИЛЕГИИ

Выдача привилегии с правом передач

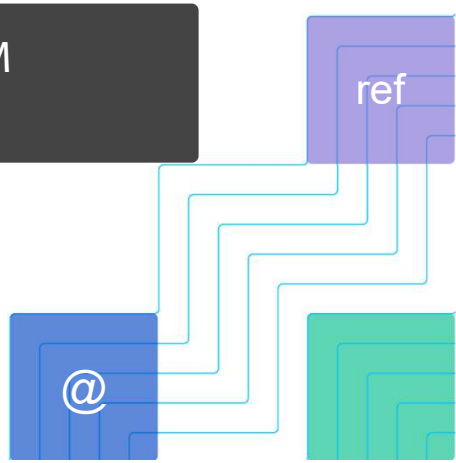
```
роль1: GRANT привилегии ON объект TO роль2 WITH GRANT OPTION;
```

Отзыв привилегии

```
роль1: REVOKE привилегии ON объект FROM роль2 CASCADE;
```

Отзыв права передачи

```
роль1: REVOKE GRANT OPTION FOR привилегии ON объект FROM
роль2 CASCADE;
```

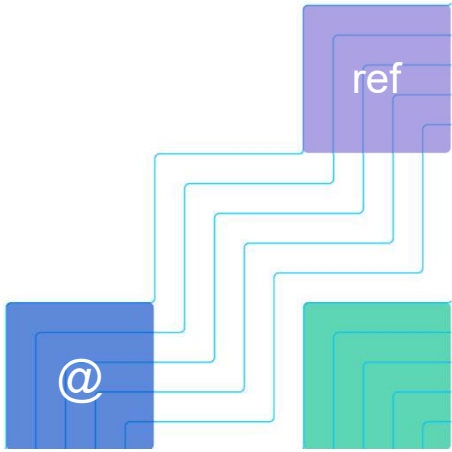


МОДЕЛИ ОРГАНИЗАЦИИ ДОСТУПА

1. Для каждого реального пользователя создавать соответствующего юзера в Постгресе

Плюсы: четко определяем права каждому пользователю

Минусы: очень громоздкая инфраструктура, потеря производительности

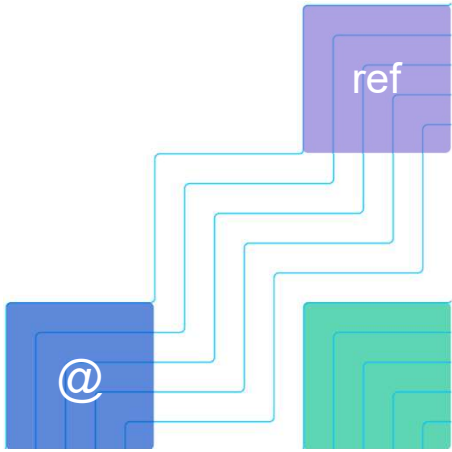


МОДЕЛИ ОРГАНИЗАЦИИ ДОСТУПА

2 Создать отдельную таблицу с пользователями, паролями и правами доступа и проверять доступ к тем или иных функциям уже на стороне приложения

Плюсы: легковесность и гибкость настройки, нет потери производительности

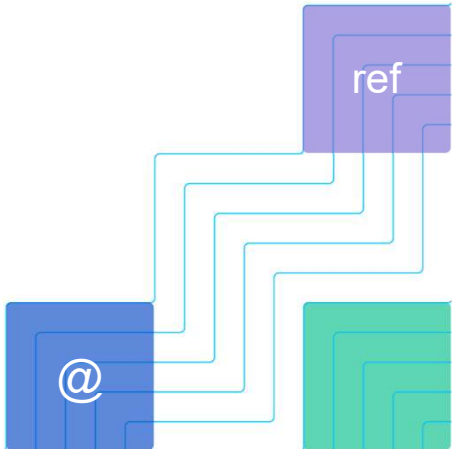
Минусы: необходимо на стороне приложения учитывать фактор ролевого доступа



ИТОГИ ЗАНЯТИЯ

01

Поняли, что такое привилегии и как правильно их настроить



ПРОВЕРОЧНОЕ ЗАДАНИЕ

Цель задания: научиться выдавать права пользователям

begin

ЗАДАНИЕ НА САМОПРОВЕРКУ

01

Зайти под пользователем postgres в psql

02

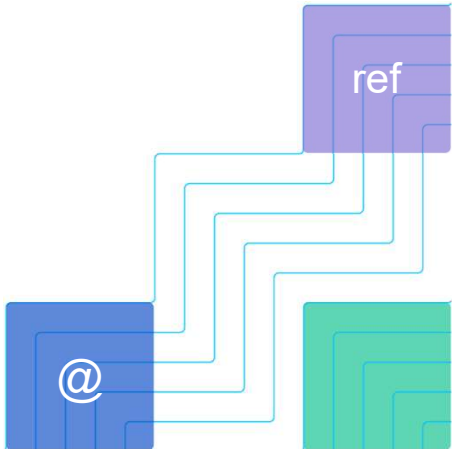
Выдать права на чтение на любую таблицу созданному на предыдущем уроке пользователю

03

Зайти в psql под этим созданным пользователем

04

Попробовать получить доступ к таблице на выбор записей, на которую выдали права на шаге 2



СПАСИБО

На следующем занятии мы рассмотрим следующий блок
Выполнение запросов, включающих темы:

- Типы данных
- Нормализация

End