

Тема 8: Разграничение доступа. Обзор разграничения доступа.



PostgreSQL

- 1) Роли и атрибуты.**
- 2) Подключение к серверу.**
- 3) Привилегии.**
- 4) Политики защиты строк.**

Роль — пользователь СУБД

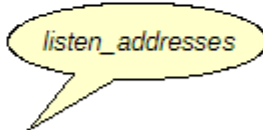
роль не связана с пользователем ОС

Свойства роли определяются атрибутами

| | |
|--------------------|------------------------------------|
| LOGIN | возможность подключения |
| SUPERUSER | суперпользователь |
| CREATEDB | возможность создавать базы данных |
| CREATEROLE | возможность создавать роли |
| REPLICATION | использование протокола репликации |
| и другие | |

1. Строки `pg_hba.conf` просматриваются сверху вниз.
2. Выбирается первая запись, которой соответствуют параметры подключения (тип, база, пользователь и адрес).

| # | TYPE | DATABASE | USER | ADDRESS | METHOD |
|-----|---------------|----------------|------------------|----------------|--------|
| | local | all | postgres | | peer |
| | local | all | all | | peer |
| | host | all | all | 127.0.0.1/32 | md5 |
| | host | all | all | :::1/128 | md5 |
| ... | | | | | |
| | local — сокет | | all — любая роль | | |
| | host — TCP/IP | | имя роли | | |
| ... | | | | | |
| | | all — любая БД | | all — любой IP | |
| | | имя БД | | IP/маска | |
| | | | | доменное имя | |



listen_addresses

3. Выполняется аутентификация указанным методом.

4. Удачно — доступ разрешается, иначе — запрещается (если не подошла ни одна запись — доступ запрещается)

| # | TYPE | DATABASE | USER | ADDRESS | METHOD |
|---|-------|----------|----------|--------------|--------|
| | local | all | postgres | | peer |
| | local | all | all | | peer |
| | host | all | all | 127.0.0.1/32 | md5 |
| | host | all | all | :::1/128 | md5 |

trust — верить

reject — отказать

scram-sha-256 и md5 — запросить пароль

peer — спросить ОС

На сервере

пароль устанавливается при создании роли или позже

пользователю без пароля будет отказано в доступе

пароль хранится в системном каталоге pg_authid

Ввод пароля на клиенте

вручную

из переменной окружения PGPASSWORD

из файла ~/.pgpass (строки в формате *узел:порт:база:роль:пароль*)

Привилегии определяют права доступа ролей к объектам

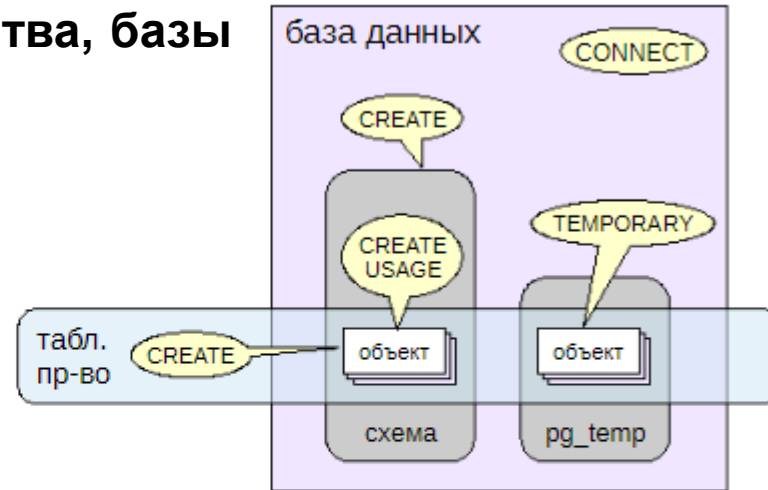
Таблицы

| | | | |
|------------|---------------------|---|--------------------------|
| SELECT | чтение данных | } | можно на уровне столбцов |
| INSERT | вставка строк | | |
| UPDATE | изменение строк | | |
| REFERENCES | внешний ключ | | |
| DELETE | удаление строк | | |
| TRUNCATE | опустошение таблицы | | |
| TRIGGER | создание триггеров | | |

Представления

| | |
|---------|--------------------|
| SELECT | чтение данных |
| TRIGGER | создание триггеров |

Табличные пространства, базы данных, схемы

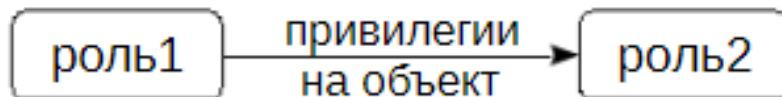


Последовательности

| | | | |
|--------|---------|---------|--------|
| SELECT | currval | | |
| UPDATE | | nextval | setval |
| USAGE | currval | nextval | |

Выдача привилегий

роль1: GRANT привилегии ON объект TO роль2;

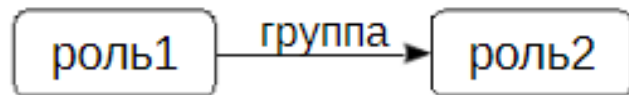


Отзыв привилегий

роль1: REVOKE привилегии ON объект FROM роль2;

Включение роли в группу

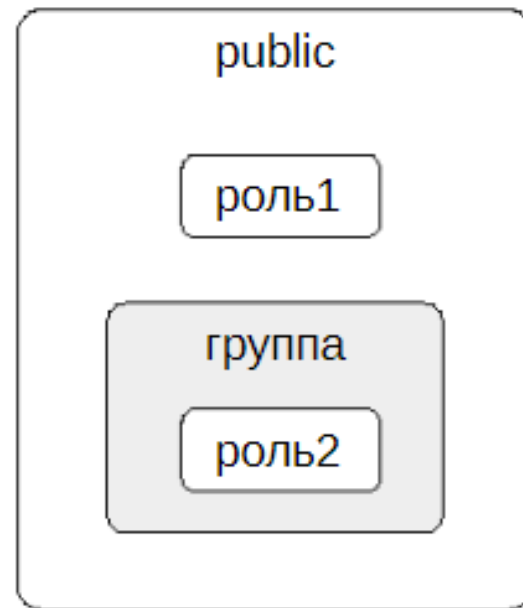
роль1: GRANT группа TO роль2;



псевдороль `public` неявно включает
в себя все остальные роли

Исключение роли из группы

роль1: REVOKE группа FROM роль2;



Кто входит в категорию

роли с атрибутом SUPERUSER

Права

**полный доступ ко всем объектам — проверки не
выполняются**

Кто входит в категорию

изначально — роль, создавшая объект (можно сменить)
а также роли, включенные в роль владельца

Права

изначально все привилегии для объекта (можно отозвать)
действия со своими объектами, не регламентируемые привилегиями,
например: удаление объекта, выдача и отзыв привилегий и т. п.

Кто входит в категорию

все остальные (не суперпользователи и не владельцы)

Права

доступ в рамках выданных привилегий

обычно наследуют привилегии групповых ролей

(но атрибут NOINHERIT требует явного переключения роли)

Единственная привилегия для функций и процедур

EXECUTE

выполнение

Характеристики безопасности

SECURITY INVOKER

выполняется с правами вызывающего(по умолчанию)

SECURITY DEFINER

выполняется с правами владельца

Привилегии псевдороди public

подключение к любой базе данных

доступ к схеме public и создание в ней объектов

доступ к системному каталогу

выполнение любых подпрограмм

привилегии выдаются автоматически для каждого нового объекта

Настраиваемые привилегии по умолчанию

возможность дополнительно выдать или отозвать привилегии

для только что созданного объекта

Дополнение к системе привилегий для разграничения доступа к таблицам на уровне строк

Политика применяется

к определенным ролям

к определенным командам (SELECT, INSERT, UPDATE, DELETE)

Политика определяет условие доступности строки

разрешительная: позволяет видеть строку, если условие выполнено

ограничительная: запрещает видеть строку, если условие не выполнено

отдельные условия (предикаты) для существительных и для новых

строк

Роли, привилегии и политики — гибкий механизм, позволяющий по-разному организовать работу

можно легко разрешить все всем

можно строго разграничить доступ, если это необходимо

При создании новых ролей надо позаботиться о возможности их подключения к серверу.

1. Создайте две роли (пароль должен совпадать с именем):—
employee — сотрудник магазина, — buyer — покупатель. Убедитесь,
что созданные роли могут подключиться к БД.
2. Отзовите у роли public права выполнения всех функций и
подключения к БД.
3. Разграничьте доступ таким образом, чтобы:
 - сотрудник мог только заказывать книги, а также— добавлять
авторов и книги,
 - покупатель мог только приобретать книги. Проверьте выполненные
настройки в приложении.