




OTUS

ONLINE EDUCATION

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо
Напишите в чат, если есть проблемы
заодно проверяем, включена ли запись занятия



Логический уровень PostgreSQL

Ржевский Михаил

<http://hosting-it.ru>

Правила вебинара



Активно участвуем



Задаем вопрос в чат



Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара



Цели вебинара | После занятия вы сможете

1. **Иметь представление об логическом устройстве PostgreSQL**
2. **Знать как PostgreSQL работает с данными на логическом уровне**
3. **Уметь создавать и настраивать схемы и права доступа пользователей**

СМЫСЛ | Зачем вам это уметь, в результате:

- 1. Уверенно пользоваться консольной утилитой psql**
- 2. Понимание модели работы с правами доступа пользователей**
- 3. Умение задавать разные уровни настройки прав пользователей для разграничения доступа**

The background of the slide is an aerial photograph of a dense city skyline, likely New York City, with numerous skyscrapers. A semi-transparent blue overlay covers the entire image. In the center, there is a network diagram consisting of white dots connected by thin white lines, forming a complex web. The text "Логический уровень" is written in white, bold, sans-serif font across the middle of the slide.

Логический уровень

Загадка

Какая сущность существует и на физическом и на логическом уровне?

Отгадка

Schema

relation

Files

Отгадка

r = ordinary table,

i = index,

S = sequence,

v = view, <https://postgrespro.ru/docs/postgrespro/13/sql-createview>

m = materialized view,

<https://postgrespro.ru/docs/postgrespro/13/sql-creatematerializedview>

c = composite type,

<https://www.postgresql.org/docs/13/rowtypes.html>

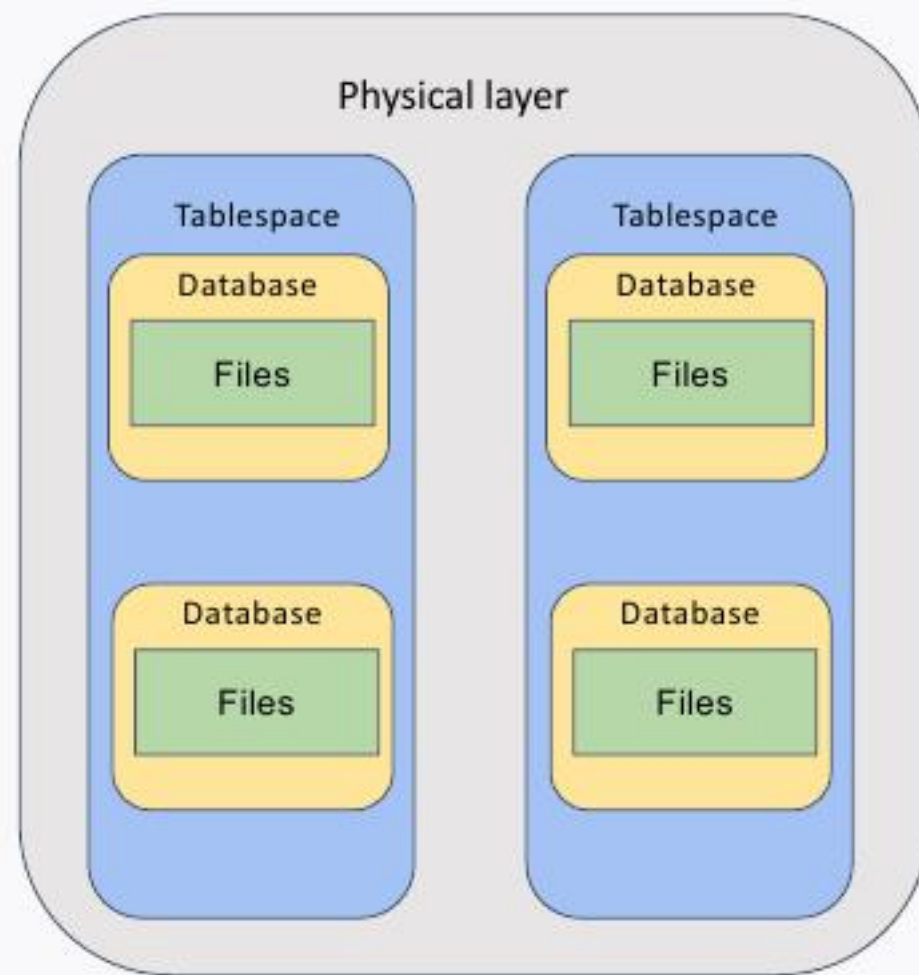
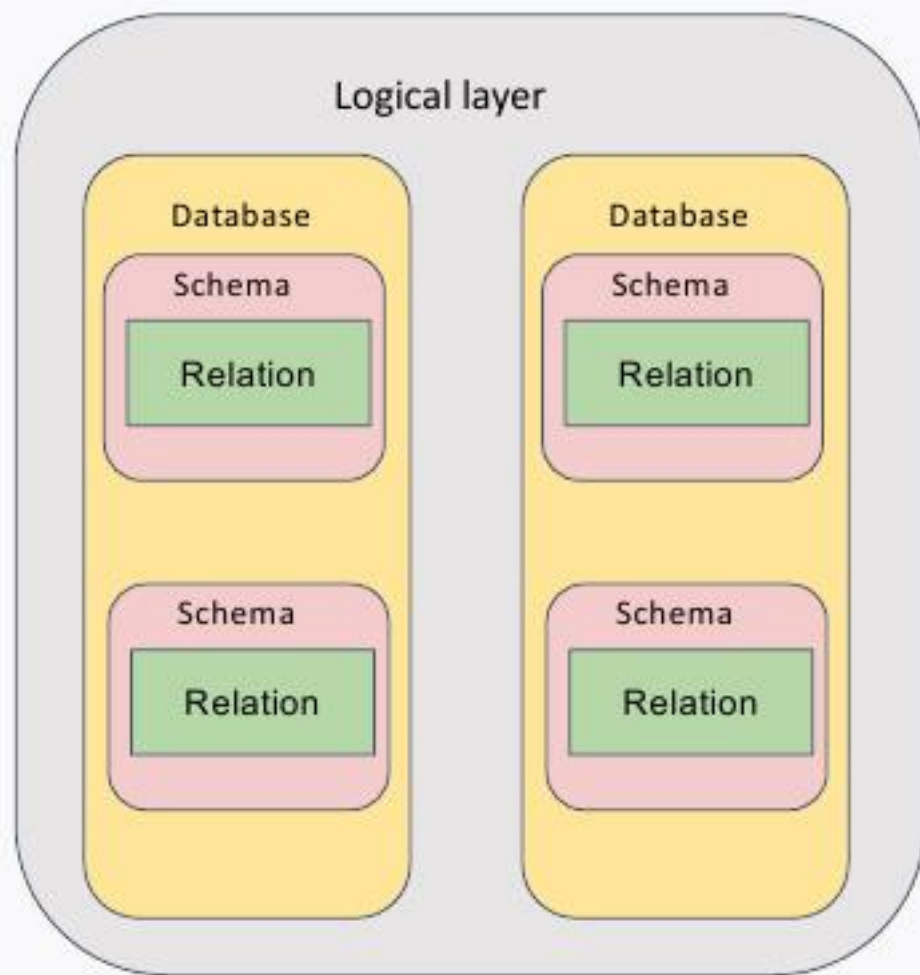
t = TOAST table,

f = foreign table,

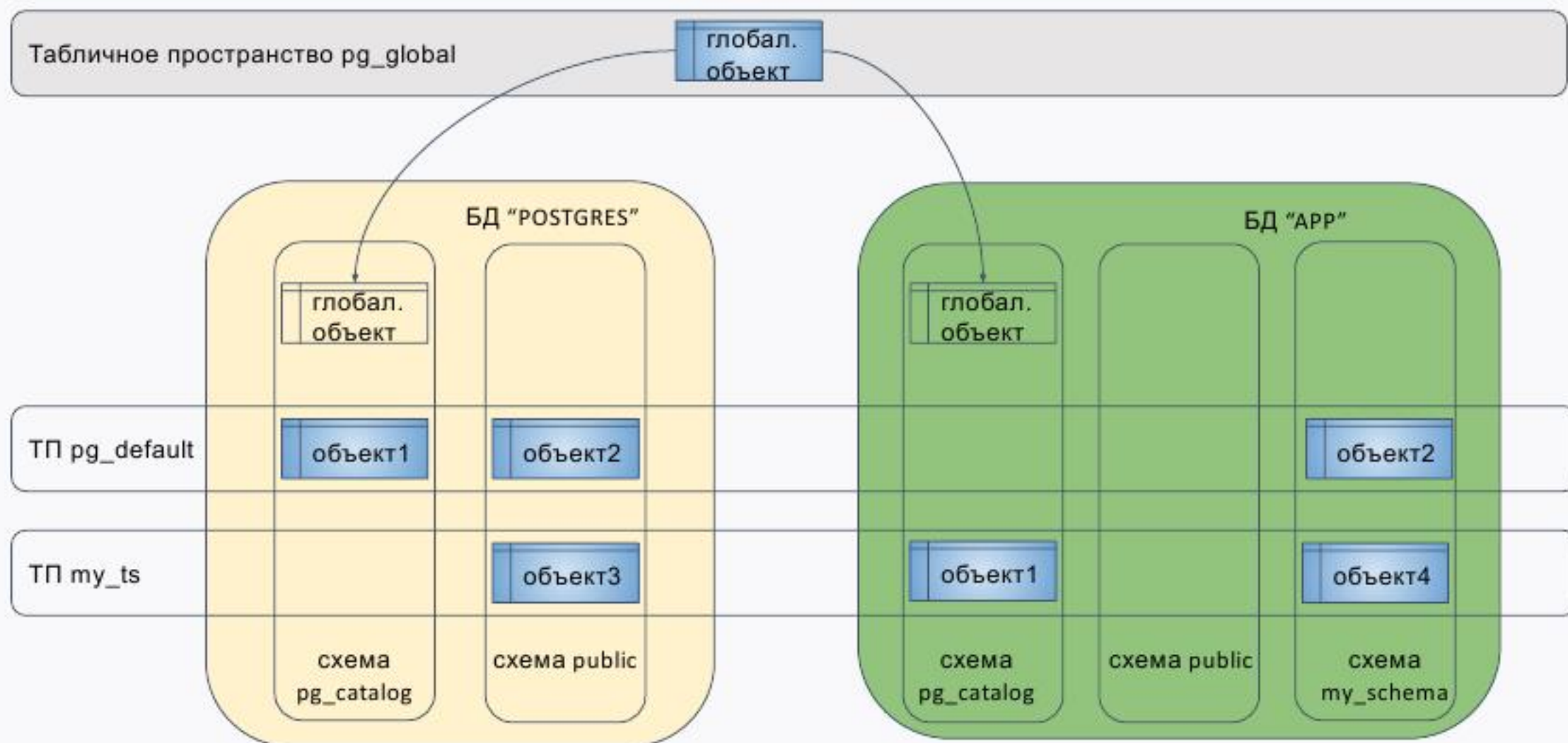
<https://postgrespro.ru/docs/postgrespro/13/sql-createforeigntable>

<https://www.postgresql.org/docs/13/catalog-pg-class.html>

Соответствие



Табличное пространство (ТП)



The background of the slide features an aerial photograph of a dense urban skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue and teal gradient. A network of thin, light blue lines connects various points across the gradient, creating a digital or data network aesthetic. The word "Database" is centered in a white, bold, sans-serif font.

Database

Database

Является контейнером самого верхнего уровня

По умолчанию в любом кластере есть как минимум 3 БД:

postgres

template0

template1

Присутствует на логическом и физическом уровне

Database

CREATE DATABASE имя

[[WITH] [OWNER [=] имя_пользователя]
[TEMPLATE [=] шаблон]
[ENCODING [=] кодировка]
[LOCALE [=] локаль[@провайдер]]
[LC_COLLATE [=] категория_сортировки[@провайдер]]
[LC_CTYPE [=] категория_типов_символов]
[TABLESPACE [=] табл_пространство]
[ALLOW_CONNECTIONS [=] разр_подключения]
[CONNECTION LIMIT [=] предел_подключений]
[IS_TEMPLATE [=] это_шаблон]]

<https://postgrespro.ru/docs/postgresql/14/sql-createdatabase>

Список диалектов и правил сортировки <https://postgrespro.ru/docs/postgresql/14/locale>

The background of the slide features an aerial view of a city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue and teal gradient. A network of thin, light blue lines connects various points across the gradient, creating a web-like pattern. The word "Schema" is centered in the middle of the slide in a white, sans-serif font.

Schema

Schema

CREATE SCHEMA *имя_схемы* [AUTHORIZATION *указание_роли*] [*элемент_схемы* [...]]

CREATE SCHEMA AUTHORIZATION *указание_роли* [*элемент_схемы* [...]]

CREATE SCHEMA **IF NOT EXISTS** *имя_схемы* [AUTHORIZATION *указание_роли*]

CREATE SCHEMA IF NOT EXISTS AUTHORIZATION *указание_роли*

Здесь *указание_роли* :

имя_пользователя

| CURRENT_USER

| SESSION_USER

<https://postgrespro.ru/docs/postgresql/14/sql-createschema>

The background of the slide is an aerial photograph of a dense city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue and teal gradient. A network of thin, light blue lines connects various points across the gradient, creating a digital or technological feel. In the center of this gradient, the word "Вопросы?" is written in a large, white, sans-serif font.

Вопросы?



Пользователи и права

Пользователи и права

Роль

пользователь СУБД

может включать в себя другие роли — быть «групповой ролью»

никак не связана с пользователем ОС

определяется на уровне кластера

Псевдороль public

неявно включает в себя все остальные роли

<https://postgrespro.ru/docs/postgresql/14/sql-createrole>

Пользователи и права

CREATE ROLE роль [WITH] атрибут [атрибут ...]

LOGIN возможность подключения

SUPERUSER суперпользователь

CREATEDB возможность создавать базы данных

CREATEROLE возможность создавать роли

REPLICATION использование протокола репликации

...

NOLOGIN

NOCREATEDB

...

<https://www.postgresql.org/docs/current/sql-createrole.html>

Пользователи и права

Включение роли в группу

роль1: GRANT группа TO роль2;

Исключение роли из группы

роль1: REVOKE группа FROM роль2;

Право управления участием в групповой роли имеют:

любая роль — в самой себе

роль с атрибутом SUPERUSER — в любой роли

роль с атрибутом CREATEROLE — в любой, кроме суперпользовательской

Пользователи и права

Включение в группу с передачей права управления

роль1: GRANT группа TO роль2 **WITH ADMIN OPTION**;

теперь роль2 управляет группой, включая передачу права управления:

роль2: GRANT группа TO роль3 WITH ADMIN OPTION;

роль2: GRANT группа TO роль4 WITH ADMIN OPTION;

Отзыв права передачи управления

роль1: **REVOKE ADMIN OPTION** FOR группа FROM роль2;

Владелец объекта

роль, создавшая объект

(а также роли, включенные в нее)

может быть изменен командой ALTER ... OWNER TO роль

\dt table_name

Пользователи и права

практика



Привилегии

Привилегии

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

GRANT & REVOKE

\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

Привилегии

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/postgrespro/13/sql-revoke>

<https://postgrespro.ru/docs/postgrespro/13/sql-alterdefaultprivileges>

Привилегии

Суперпользователи

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

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

Привилегии

Выдача привилегии с правом передачи

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;



Вопросы?

The background of the slide features an aerial view of a city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue and teal gradient. A network of white lines and dots, resembling a web or data structure, is visible across the entire background.

LDAP

LDAP

Установка LDAP+настройка

[How to connect Postgres with LDAP \(with StartTLS\) | EDB](#)

настройка LDAP для AD

[Учебный PostgreSQL - LDAP Аутентификация на активный каталог](#)

The background of the image is an aerial photograph of a dense city skyline, likely New York City, with numerous skyscrapers. The image is overlaid with a semi-transparent blue and teal gradient. A network of thin, light blue lines connects various points across the gradient, creating a digital or technological feel. The word "Порефлексируем" is written in a large, white, sans-serif font, centered horizontally and partially overlaid by the network lines.

Порефлексируем

Вопросы?

- Кто что запомнил за сегодня?
- Имеем ли мы право на вход по умолчанию?
- Что узнали нового?



ДЗ

- 1 создайте новый кластер PostgreSQL 13 (на выбор - GCE, CloudSQL)
- 2 зайдите в созданный кластер под пользователем postgres
- 3 создайте новую базу данных testdb
- 4 зайдите в созданную базу данных под пользователем postgres
- 5 создайте новую схему testnm
- 6 создайте новую таблицу t1 с одной колонкой c1 типа integer
- 7 вставьте строку со значением c1=1
- 8 создайте новую роль readonly
- 9 дайте новой роли право на подключение к базе данных testdb
- 10 дайте новой роли право на использование схемы testnm
- 11 дайте новой роли право на select для всех таблиц схемы testnm
- 12 создайте пользователя testread с паролем test123
- 13 дайте роль readonly пользователю testread
- 14 зайдите под пользователем testread в базу данных testdb
- 15 сделайте select * from t1;
- 16 получилось? (могло если вы делали сами не по шпаргалке и не упустили один существенный момент про который позже)
- 17 напишите что именно произошло в тексте домашнего задания
- 18 у вас есть идеи почему? ведь права то дали?
- 19 посмотрите на список таблиц
- 20 подсказка в шпаргалке под пунктом 20

ДЗ

- 21 а почему так получилось с таблицей (если делали сами и без шпаргалки то может у вас все нормально)
- 22 вернитесь в базу данных testdb под пользователем postgres
- 23 удалите таблицу t1
- 24 создайте ее заново но уже с явным указанием имени схемы testnm
- 25 вставьте строку со значением c1=1
- 26 зайдите под пользователем testread в базу данных testdb
- 27 сделайте `select * from testnm.t1;`
- 28 получилось?
- 29 есть идеи почему? если нет - смотрите шпаргалку
- 30 как сделать так чтобы такое больше не повторялось? если нет идей - смотрите шпаргалку
- 31 сделайте `select * from testnm.t1;`
- 32 получилось?
- 33 есть идеи почему? если нет - смотрите шпаргалку
- 31 сделайте `select * from testnm.t1;`
- 32 получилось?
- 33 ура!
- 34 теперь попробуйте выполнить команду `create table t2(c1 integer); insert into t2 values (2);`
- 35 а как так? нам же никто прав на создание таблиц и insert в них под ролью readonly?
- 36 есть идеи как убрать эти права? если нет - смотрите шпаргалку
- 37 если вы справились сами то расскажите что сделали и почему, если смотрели шпаргалку - объясните что сделали и почему выполнив указанные в ней команды
- 38 теперь попробуйте выполнить команду `create table t3(c1 integer); insert into t2 values (2);`
- 39 расскажите что получилось и почему



Спасибо за внимание!
Приходите на следующие вебинары

