МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
 «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

Лабораторная работа №12

по дисциплине «Основы построения защищённых баз данных»

Выполнил: обучающийся гр. ВКБ43

Ковалев Данил Петрович

Проверил:

Скляров Алексей Викторович

Тема: динамическое управление доступом на основе контекста

Цель: разработать систему, которая динамически адаптирует права пользователей в зависимости от контекста (времени доступа, IP-адреса).

Вариант 1. Создайте таблицу clients с полями client\_id, name, email. Настройте доступ только для IP-адресов из сети 192.168.1.0/24. Реализуйте триггер для ограничения операций добавления данных в нерабочее время (9:00 – 18:00).

Задание 1. Создайте пользователей и роли, которые будут использоваться для проверки доступа. Назначьте пользователей к соответствующим ролям.

Для взаимодействия с базой данных использовалась система контейнеризации Docker. Конфигурация работы PostgreSQL для работы с Docker представлена на рисунке 1.

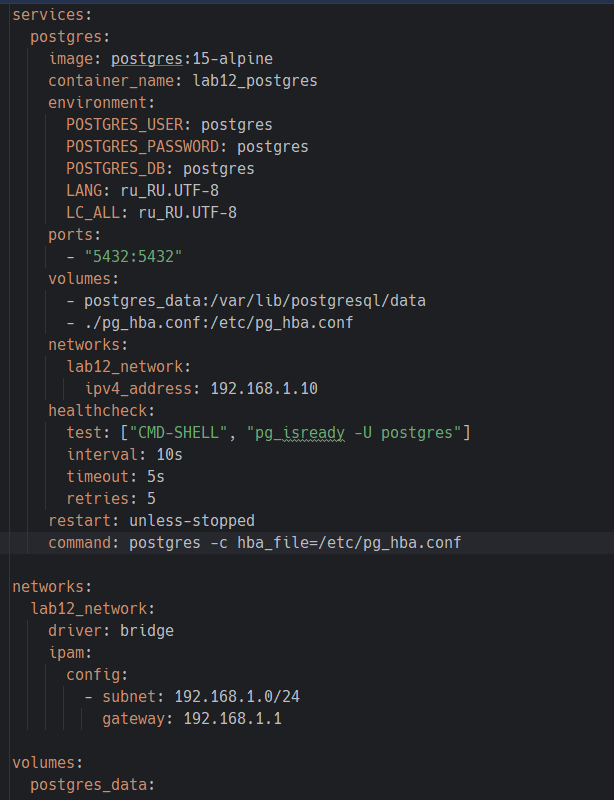


Рисунок 1 – конфигурация Docker compose для работы с PostgreSQL

Теперь перейдем к созданию пользователей и ролей. Для создания роли используется код, который представлен ниже на рисунке 2.

Изображение выглядит как текст, Шрифт, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 2 – создание ролей

Создадим теперь пользователей и назначим их к ролям, также выдадим доступ на подключение к основной базе данных, код для этого представлен на рисунке 3.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 3 – создание пользователей и выдача ролей пользователям

Создадим сразу таблицу, как требуется в нашем варианте. Код для создания таблицы представлен на рисунке 4.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4 – создание таблицы и добавление описания

Выдадим сразу права на таблицу и вставим тестовые данные, как представлено на рисунке 5.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 5 – создание прав на таблицу и выполнение запросов

Задание 2. Настройте файл pg\_hba.conf для ограничения доступа на основе IP-адреса.

Настроим ограничения по IP-адресу для созданных ролей в pg\_hba.conf. Конфигурация представлена на рисунке 6.

Изображение выглядит как текст, снимок экрана, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 6 – ограничения в pg\_hba.conf

Задание 3. Проверьте, что доступ с разрешенных IP-адресов возможен, а с других – запрещен.

Для проверки воспользуемся ещё Docker контейнерами, с помощью которых проверим корректность настройки pg\_hba.conf. Данные контейнеры представлены на рисунке 7.

Изображение выглядит как текст, снимок экрана, меню, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 7 – новые контейнеры для тестирования настройки pg\_hba.conf

Теперь попробуем проверить, что отрабатывает подключение с разных хостов. В итоге, при тестах вышло то, что представлено на рисунке, который представлен на рисунке 8.

Изображение выглядит как текст, программное обеспечение, Мультимедийное программное обеспечение, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 8 – проверка доступа

Задание 4. Напишите функцию и триггер для ограничения операций в зависимости от времени суток.

Функция для проверки времени ограничения операций представлена на рисунке 9.

Изображение выглядит как текст, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 9 – проверка ограничений по времени

Триггер для ограничения операций можно представить на рисунке 10.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 10 – триггер

Задание 5. Проверьте корректность работы триггера, выполняя запросы в разные временные интервалы.

Выполним запрос под вечер, проверив, что триггер корректно отрабатывает. Для проверки будем использовать запрос, который представлен на рисунке 11.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 11 - код для триггера

Вывод для триггера представлен на рисунке 12.

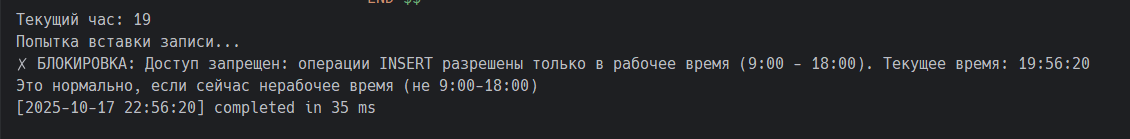


Рисунок 12 – вывод о блокировке

Задание 6. Включите RLS для таблицы и создайте политику, которая ограничивает доступ к строкам на основе роли пользователя или IP-адреса.

Для таблицы включим RLS, настройка представлена на рисунке 13.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 13 – включение RLS

Теперь представим на рисунке 14 кол для создания политики, которая ограничивает доступ к строкам на основе роли пользователя или IP-адреса. Конфигурация представлена на рисунке 14.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 14 – создание политик

Задание 7. Протестируйте политику, выполняя запросы от имени разных пользователей и ролей.

Проверка политики представлена на рисунке 15. В принципе ограничения полностью работают.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 15 – проверка работоспособности политики

Задание 8. Выполните тестирование созданной системы, чтобы убедиться, что доступ предоставляется или ограничивается в зависимости от контекста (времени, IP-адреса, роли).

Проверка с точки зрения времени доступа и т.п представлены на рисунках 16, 17.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 16 – ограничение по доступу

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 17 – ограничение по доступу