**Task 15 (SSL)**

**Создание сертификатов и ключей SSL**

С помощью команд, изученных на лекции, я создал ключи и сертификаты SSL для клиента и сервера.

Ключи и сертификаты были созданы от имени root. Для файла ключа понадобилось изменить владельца на пользователя postgres.

**Конфигурирование PostgreSQL**

В файле postgresql.conf я изменил следующие параметры:

ssl=on — чтобы включить SSL

С помощью параметров ssl\_ca\_file, ssl\_cert\_file, ssl\_key\_file я задал пути к соответствующим сертификатам и ключам.

ssl\_ciphers='HIGH:MEDIUM:+3DES:!aNULL'

listen\_addresses='\*' — чтобы обеспечить возможность удаленного подключения к PostgreSQL с любых IP-адресов.

В файле pg\_hba.conf, я добавил следующую строку, чтобы разрешить подключение с любого IP-адреса по паролю, который будет передаваться в захэшированном виде:

| host all all 0.0.0.0/0 md5 |
| --- |

**Проверка SSL-подключения**

Для проверки подключения я выполнил следующую команду на клиенте:

| psql -p 5432 "sslmode=require dbname=postgres" -U postgres -h pgmaster.course.net |
| --- |

Команда была выполнена успешно, запустилась консоль psql, с помощью которой можно выполнять команды в базе данных.

**PgBench**

PgBench без SSL я запускал с помощью следующей команды:

| pgbench -t 1000 -c 10 -C -p 5432 "sslmode=disable dbname=postgres" -U postgres -h pgmaster.course.net |
| --- |

С флагом -C новое подключение устанавливается для каждой транзакции, а не для каждого клиента. Использование этого флага дает возможность более точно измерить влияние SSL на latency и TPS транзакций.

Были получены следующие результаты:

* 119.681 ms — latency average
* 83.555653 — tps (including connections establishing)
* 88.144864 — tps (excluding connections establishing)

PgBench с SSL я запускал с помощью следующей команды:

| pgbench -t 1000 -c 10 -C -p 5432 "sslmode=require dbname=postgres" -U postgres -h pgmaster.course.net |
| --- |

Эта команда отличается от предыдущей тем, что “sslmode=disable” заменено на “sslmode=require”.

Были получены следующие результаты:

* 213.933 ms — latency average
* 46.743499 — tps (including connections establishing)
* 50.352513 — tps (excluding connections establishing)

С SSL:

* latency выше в 1.79 раза
* tps (including connections establishing) ниже в 1.79 раза
* tps (excluding connections establishing) ниже в 1.75 раза

Таким образом, SSL приводит к значительному замедлению транзакций.