Proposal for GSoC 2022

pgagroal: SCRAM-SHA-256-PLUS support (2022)

Haitao Wang
wanghaitao0125@zju.edu.cn

Date: 2022/4/18

1 Overview

pgagroal is a high-performance protocol-native connection pool for PostgreSQL. The goal of this project is to add SCRAM-SHA-256-PLUS support in order to enhance security when communicating with the connection pool.

2 Outline Design

SCRAM-SHA-256-PLUS is an authentication mechanism that allows user passwords to be processed and stored in clear text on the server.

pgagroal use `pgagroal-admin` tool to define the users known to the system. At present, the user's password is encrypted by AES with a master key and stored in `pgagroal_users.conf` file. Changing it to SCRAM-SHA-256-PLUS can enhance the security of the system.

I'm going to read the documents related to SCRAM-SHA-256-PLUS first, and then use OpenSSL to implement the API of SCRAM-SHA-256-PLUS in pgagroal to replace the original AES encryption mechanism.

This task should not make any changes to the user interface, and all changes should be limited to pgagroal internal.

3 Schedule

I June 1 - June 12

- Setup development environment
- Read the documents and be familiar with the knowledge related to SCRAM-SHA-256-PLUS.

II June 13 - June 26

- Get familiar with pgagroal code base.

III June 27 - August 7

- Design internal API.
- Code writing.

IV August 8 - September 4

- Testing.
- Bug fix.
- Documentation.

4 About Me

I am a master student in the school of computer science, Zhejiang University, and my research interest is applied cryptography.
I am familiar with C/C++ development and understand the principle of mainstream encryption algorithms.
I am now working on a project that uses Intel Software Guard Extension technology to build an encrypted database based on PostgreSQL. It can run on any computer with Intel SGX CPU and provide strong security for the data in the database with low performance loss.