
Криптографические
параметры
PostgreSQL
Технический
Центр
Интернет

Технический
Центр
Интернет

Криптографические параметры PostgreSQL

Дмитрий Белявский

PgConf.ru - 2018

6 февраля 2018

Протокол TLS

Технический Центр Интернет

Актуальные версии: 1.0 – 1.2

Шифрование

Аутентификация

Технический
Центр
Интернет

OpenSSL

- Поддерживаемые версии: 1.0.2, 1.1.0
- Разумные умолчания
  - *AES*
  - *Ключевой обмен по Диффи-Хеллману*
- Свой конфигурационный файл?
  - *OPENSSL_CONF=/path/to/my.conf*
  - *Например, если нужен ГОСТ*

Параметры сервера

Технический Центр Интернет

postgresql.conf

- ssl = on
- ssl_cert_file/ssl_key_file
- ssl_crl_file
- ssl_dh_params_file
- ssl_ciphers
- ssl_ca_file – для авторизации по сертификатам

Технический Центр Интернет

Без неё – только шифрование

- По умолчанию выключена
- Реализована через libpq
  - *~/.postgresql/root.crt*
  - *~/.postgresql/postgresql.crt*
  - *~/.postgresql/postgresql.key*

- Подробности: https://www.postgresql.org/docs/10/static/libpq-ssl.html

Технический Центр Интернет

Настройки pg_hba.conf

- Опция clientcert
  - *Включает проверку сертификата*
  - *clientcert=0 – можно идти без сертификата*
  - *clientcert=1 – требуется сертификат*
  - *Для любого auth-метода*
- Auth-метод cert
  - *Берёт имя пользователя из поля CN сертификата*
  - *Опция map*

Пакет sslinfo

- ssl_is_used(), ssl_version(), ssl_cipher()
- ssl_client_cert_present()
- ssl_client_dn()/ssl_client_dn_field(fieldname text)
- ssl_client_serial()/ssl_issuer_dn()

- Документация: https://www.postgresql.org/docs/current/static/sslinfo.html

Немного про auth

Технический Центр Интернет

- cert – описана ранее
- На основе пароля
  - *password*
  - *md5*
  - *scram-sha-256 (10+), RFC 7677*
- Для апгрейда:
  - *password_encryption = scram-sha-256*
  - *Проверить всех клиентов*
  - *Перегенерить пароли*
  - *Сменить метод авторизации в pg_hba.conf*

- Простое изложение схемы: https://www.openscg.com/2017/12/salted-challenge-response-authentication-mechanism-scram-authentication/

Вопросы?

beldmit@tcinet.ru