Руководство пользователя: Шифрование данных TDE

Центр разработки PostgreSQL

Exported on 05/29/2020

Table of Contents

PostgresSQL Sber Edition использует шифрование данных для предотвращения несанкционированного доступа к пользовательским данным, хранящимся в файлах данных, журналах изменений, резервных копиях и временных файлах БД. Шифрование позволяет защитить данные от пользователей, имеющих доступ к файловой системе и/или операционной системе серверов СУБД PostgreSQL Sber Edition.

Ограничения реализации:

- не поддерживается шифрование данных на уровне колонок таблиц и партиций баз данных СУБД PostgreSQL Sber Edition;
- не поддерживается перенос туда и обратно отношений между шифрованным и не шифрованным табличными пространствами;
- не поддерживается защита информации в скриптах SQL дампов, выгружаемых утилитами pg_dump, pg_dumpall и подобных;
- не поддерживается возможность включения/выключения шифрования после первичной инициализации кластера - при изменении режима шифрования на работающем кластере не будет выполняться расшифровывание/зашифрование WAL;
- восстановление резервных копий снятых с серверов с включенным шифрованием возможно только на серверах, входящих в тот же кластер высокой доступности, что и источник резервной копии. Сервера должны быть настроены на подключение к той же KMS, что и сервер-источник резервной копии;
- решение описано с учетом свойств KMS, соответствующих HashiCorp Vault (Выбор KMS для задач СУБД PostgreSQL[1])

Управление функциями прозрачного шифрования данных СУБД PostgreSQL выполняется посредством следующих интерфейсов

- задание администратором безопасности параметров соединения с KMS и шифрование credentials для соединения с KMS через вызов утилиты настройки соединения на экземпляре СУБД PostgreSQL;
- включение/выключение шифрования табличных пространств через задание параметров табличных пространств в командах DDL на экземпляре СУБД PostgreSQL;
- управление перешифрованием при замене мастер-ключа выполняется через вызов функций расширения управления шифрованием на экземпляре СУБД PostgreSQL;
- восстановление шифрования ключей при сбое перешифрования выполняется через вызов функции расширения управления шифрованием на экземпляре СУБД PostgreSQL;
- замена/первоначальное задание мастер-ключа для кластера высокой доступности в KMS выполняется вызовом функции расширения управления шифрованием на мастер-инстансе СУБД PostgreSQL кластера;

Подход к шифрованию

Для шифрования блоков данных используются симметричные алгоритмы блочного шифрования: на данный момент AES-256. Ключи шифрования организуются в 2х уровневую иерархию, корнем которой является периодически ротируемый мастер-ключ, посредством которого выполняется шифрование ключей 2го уровня - ключей шифрования объектов баз данных. Ключи 2го уровня не ротируются, что исключает необходимость перешифрования данных при смене мастер-ключа. Ротация мастер-ключа кластера высокой доступности инициируется и выполняется посредством выполнения функции смены мастер-ключа на мастер-инстансе СУБД PostgreSQL, входящем в кластер. Для восстановления шифрования ключей при внезапном падении СУБД PostgreSQL в процессе перешифрования ключей, реализуется функция восстановления шифрования. Все сервера кластера высокой доступности выполняют периодическую проверку, в соответствии с настройками, соответствия текущего мастер-ключа мастер-ключу из KMS, и, в случае несоответствия выполняют процедуру перешифрования ключей.

1 https://sbtatlas.sigma.sbrf.ru/wiki/pages/viewpage.action?pageId=1353063171

Инфраструктура мастер-ключей шифрования в KMS

Используется хранилище key-value в KMS

- параметры и ключи, относящиеся к шифрованию, сгруппированы в параметрах, путь к которым начинается как postgresql/<id кластера>/keys;
- ключ postgresql/<id кластера>/keys/actual_master_key - метка актуального мастер-ключа. При возможности, используется версионирование значений;
- ключ postgresql/<id кластера>/keys/prev_master_key - метка предыдущего мастер-ключа. При возможности, используется версионирование значений;
- ключ postgresql/<id кластера>/keys/wal_key - значение ключа шифрования WAL кластера. При возможности, используется версионирование значений;
- ключи postgresql/<id кластера>/keys/master_key_value_<timestamp> - значение мастер-ключа, <timestamp> - дата и время в формате ГГГГММДД_ЧЧммСС, где ГГГГ - год в формате 4 цифры, ММ - месяц с ведущим нулем при необходимости, ДД - день с ведущим нулем при необходимости, ЧЧ - часы в формате 24 часа, с ведущим нулем при необходимости, мм - минуты с ведущим нулем при необходимости, СС - секунды с ведущим нулем при необходимости;

Инфраструктура ключей шифрования в общих файлах экземпляра PostgreSQL

- файл enc_connection_settings.cfg - содержит
  - параметры соединения с KMS
  - зашифрованные credentials для соединения с KMS;

  не включается в резервные копии БД, является настройкой экземпляра СУБД;

- файл global/enc_settings.cfg - содержит
  - метку(ключ в KMS) актуального мастер-ключа шифрования
  - метку(ключ в KMS) предыдущего мастер-ключей шифрования
  - флаг необходимости шифрования WAL - по умолчанию включен

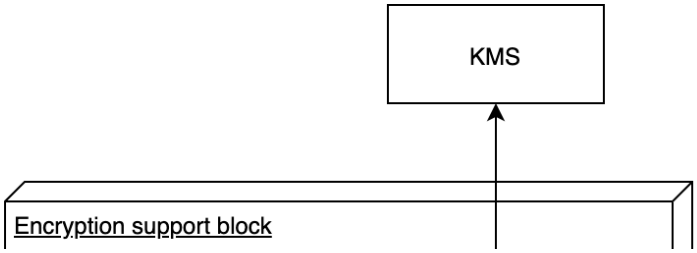
  включается в резервные копии БД;

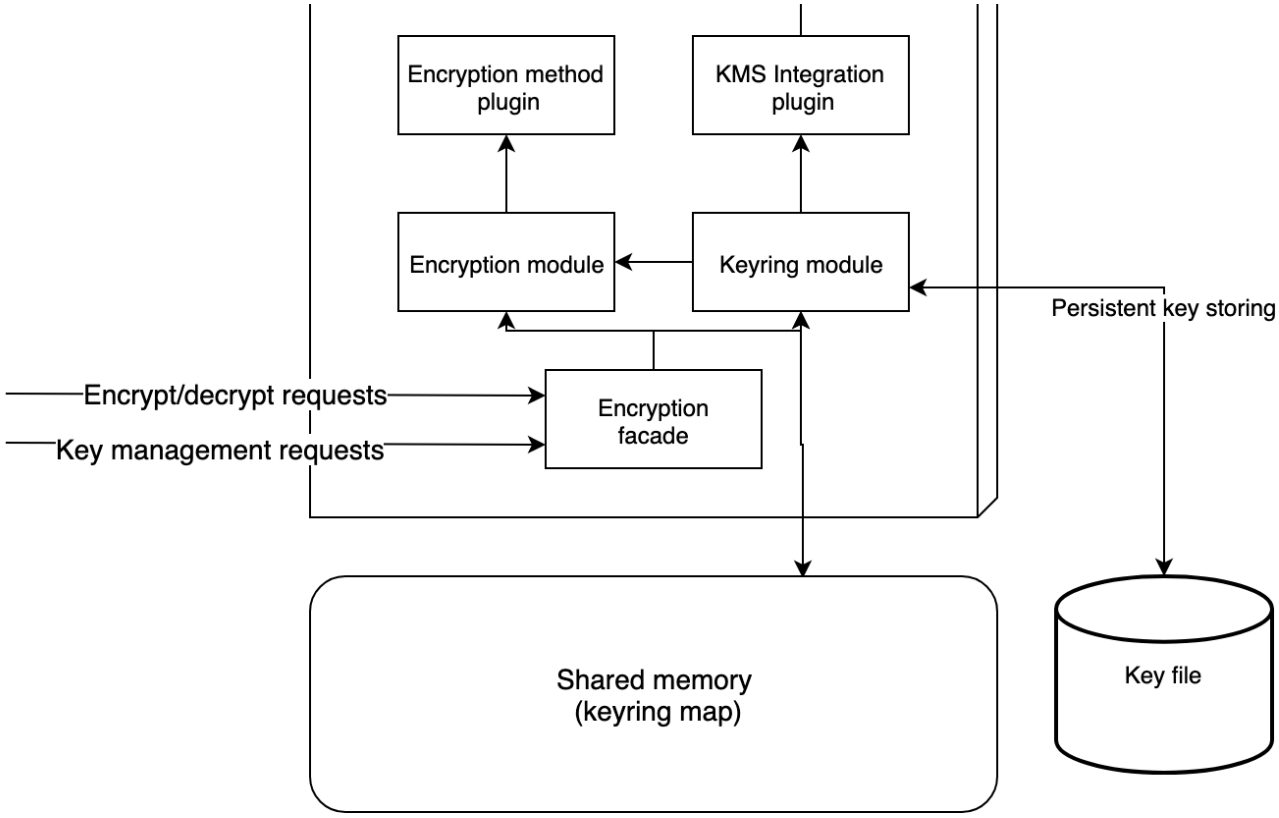
- файл global/enc_keys.json - содержит ключи шифрования табличных пространств, отношений и WAL.
  - objtype - тип объекта, которому назначен соответствующий ключ шифрования. 'W' - WAL, 'T' - табличное пространство, 'R' - отношение
  - objoid - OID объекта, которому назначен соответствующий ключ шифрования. Для WAL должен быть null
  - objkey - ключ шифрования объекта в зашифрованном виде
  - objmaster - контрольный блок из метки мастер-ключа, OID базы данных, типа и OID, зашифрованный ключем шифрования
  - objdboid - oid базы данных объекта

  включается в резервные копии БД;

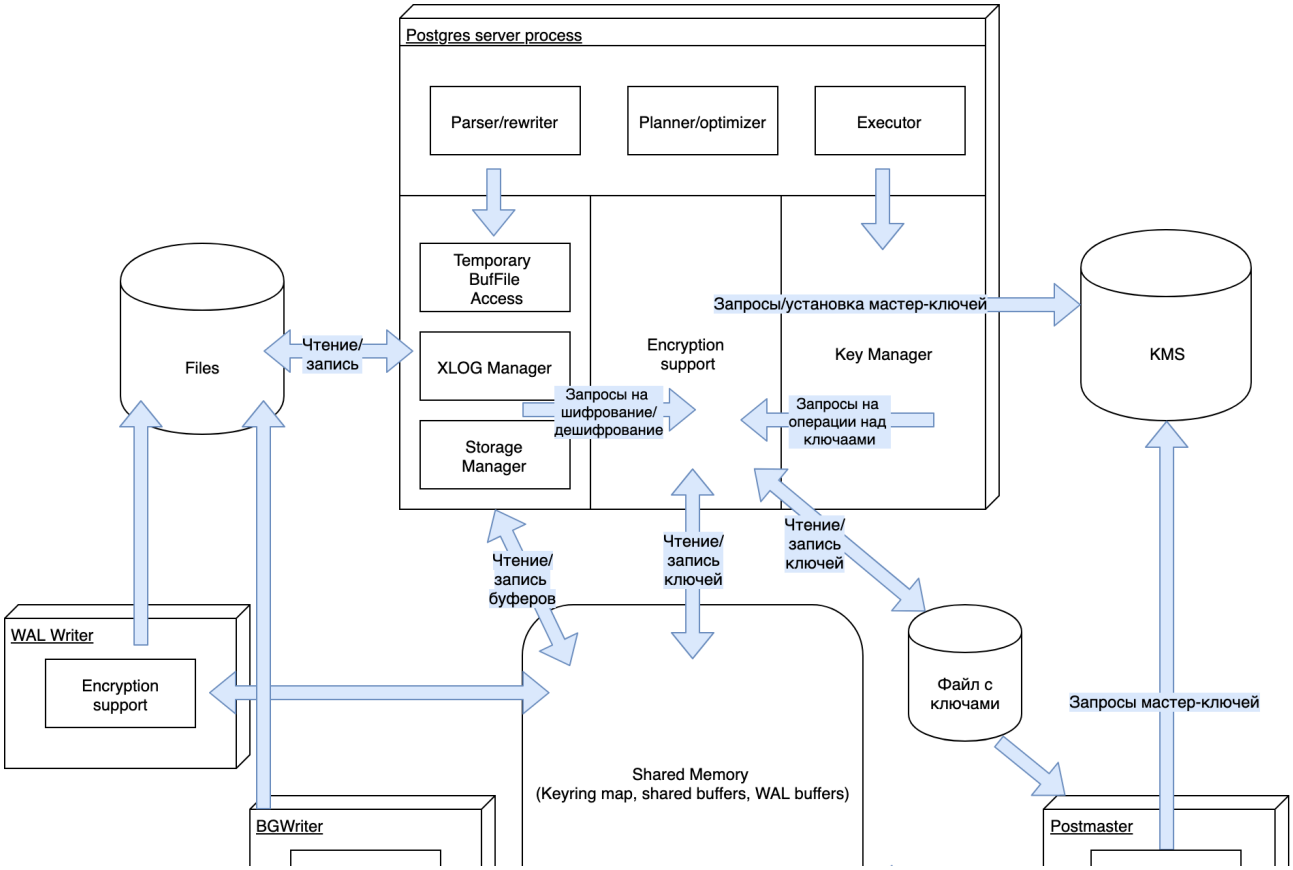
Общая архитектура решения

Концептуальная архитектура инфраструктуры шифрования и управления ключами





Концептуальная архитектура PostgreSQL при реализации прозрачного шифрования

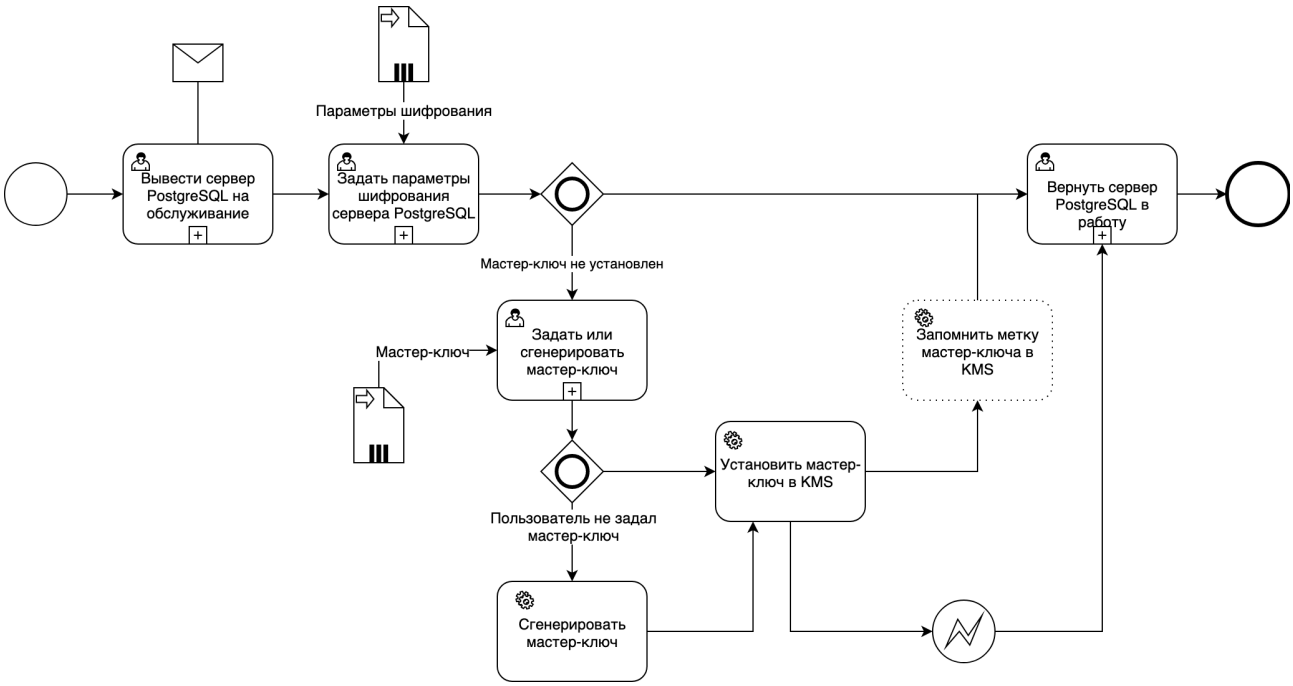


Помимо указанных на схеме, Encryption support включается также в следующие процессы и утилиты

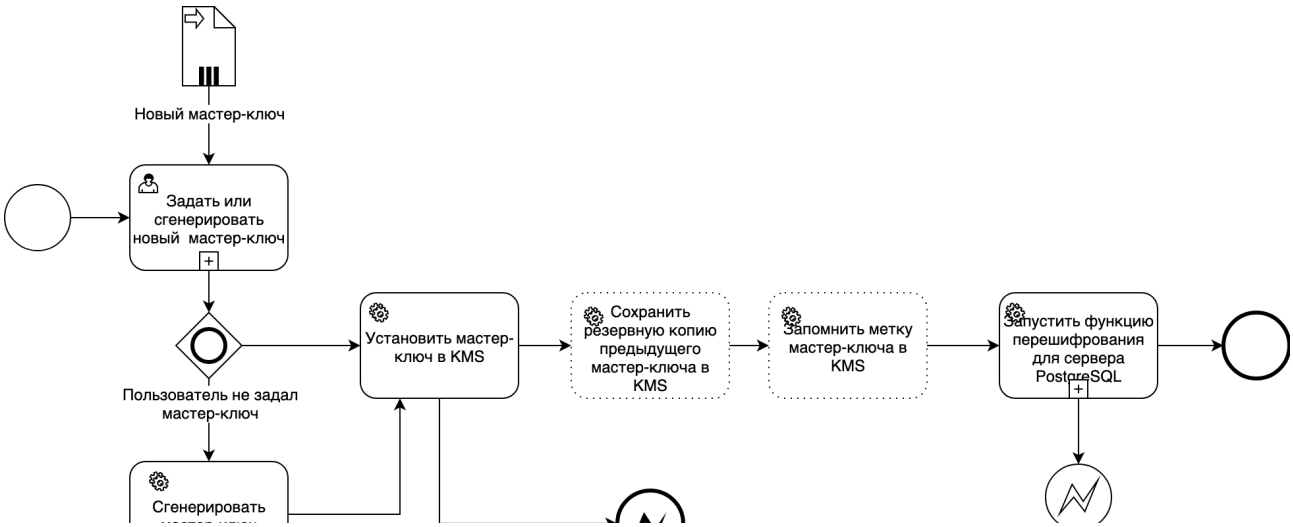
- WAL Sender
- WAL Receiver
- pg_receivewal
- pg_rewind
- pg_verify_checksums
- pg_waldump
- pg_restore

Схемы процессов

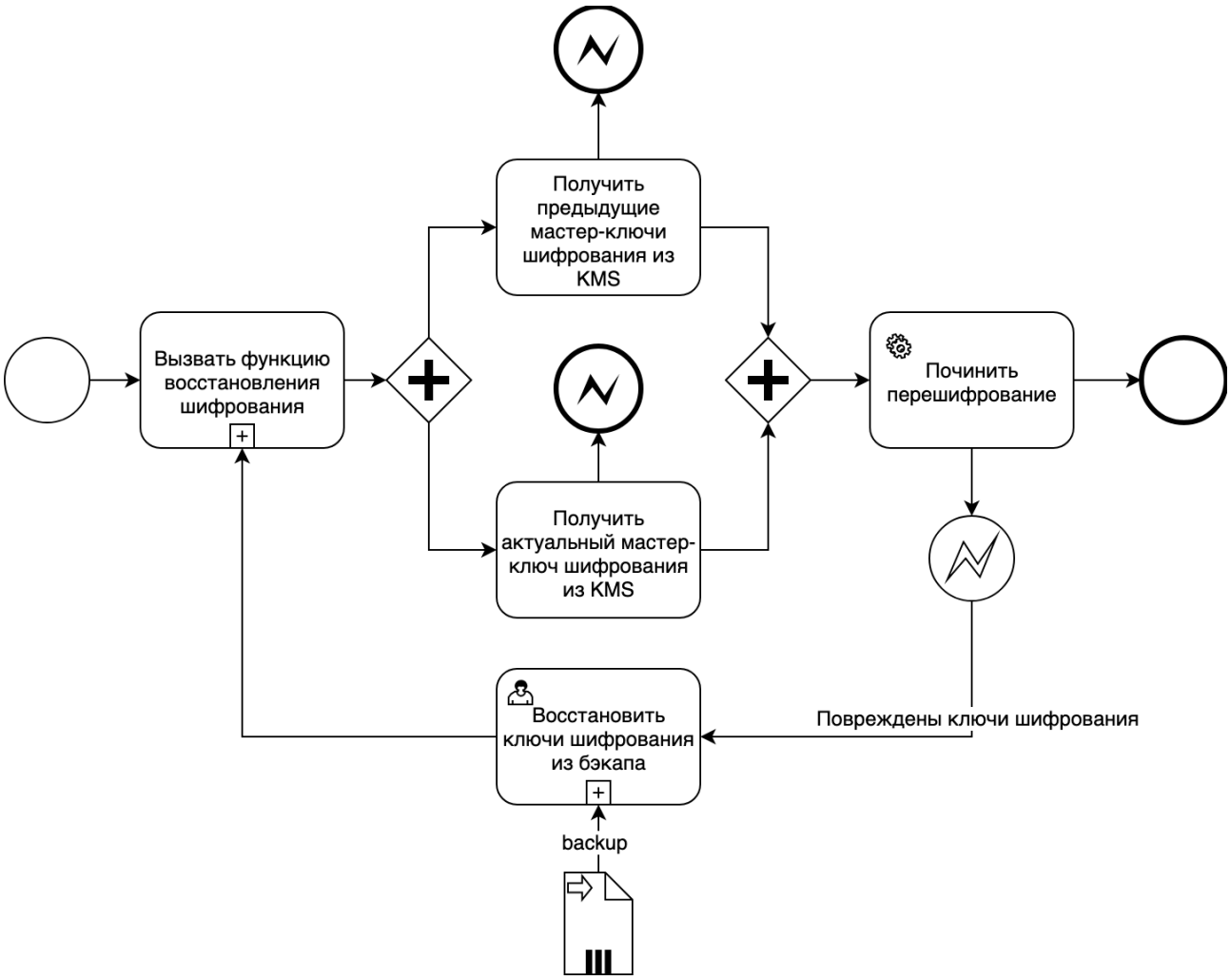
Первоначальная настройка шифрования для сервера СУБД PostgreSQL



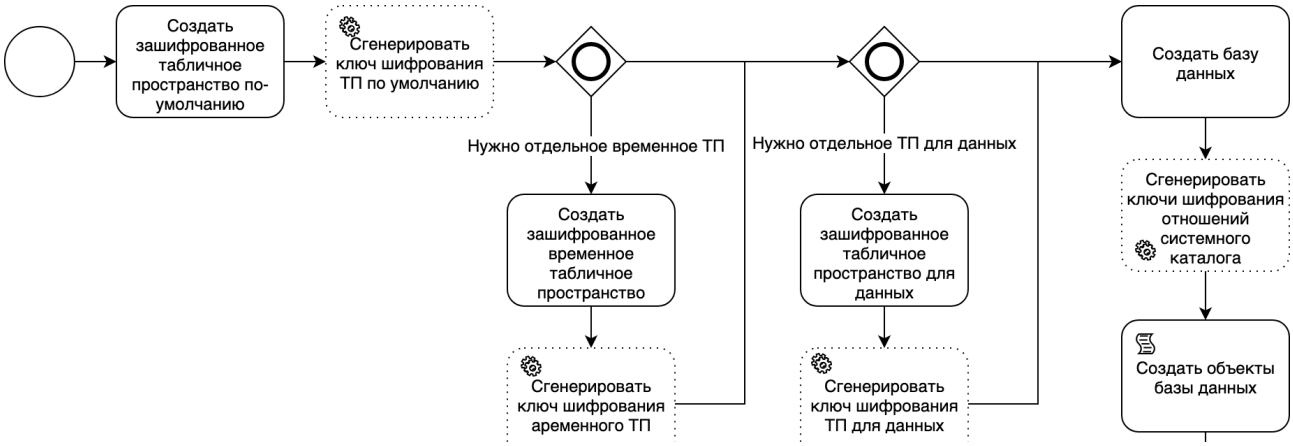
Смена мастер-ключа шифрования

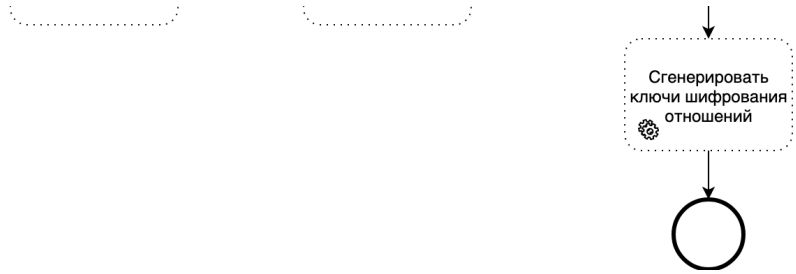


Восстановление шифрования БД при сбое процесса перешифрования БД

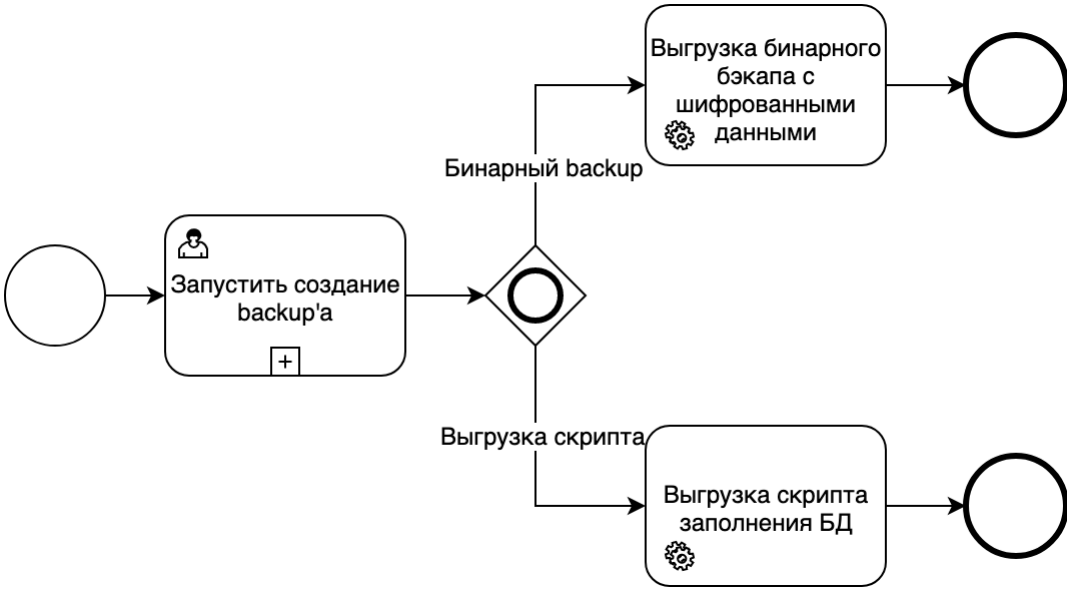


Шифрование БД и объектов БД

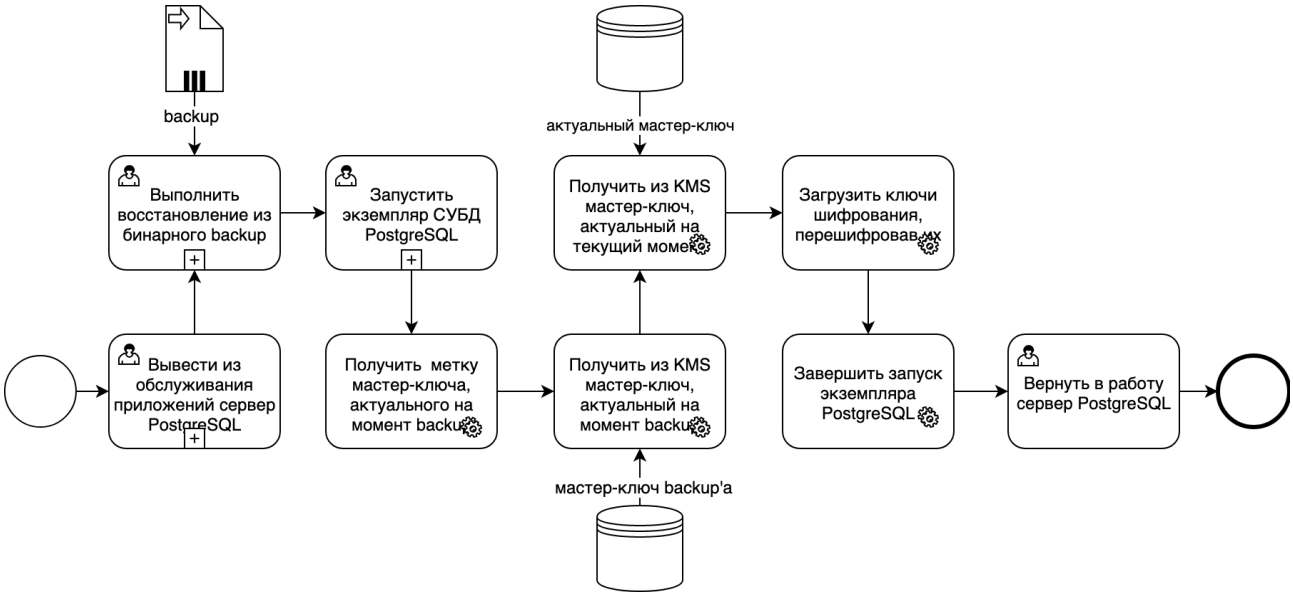




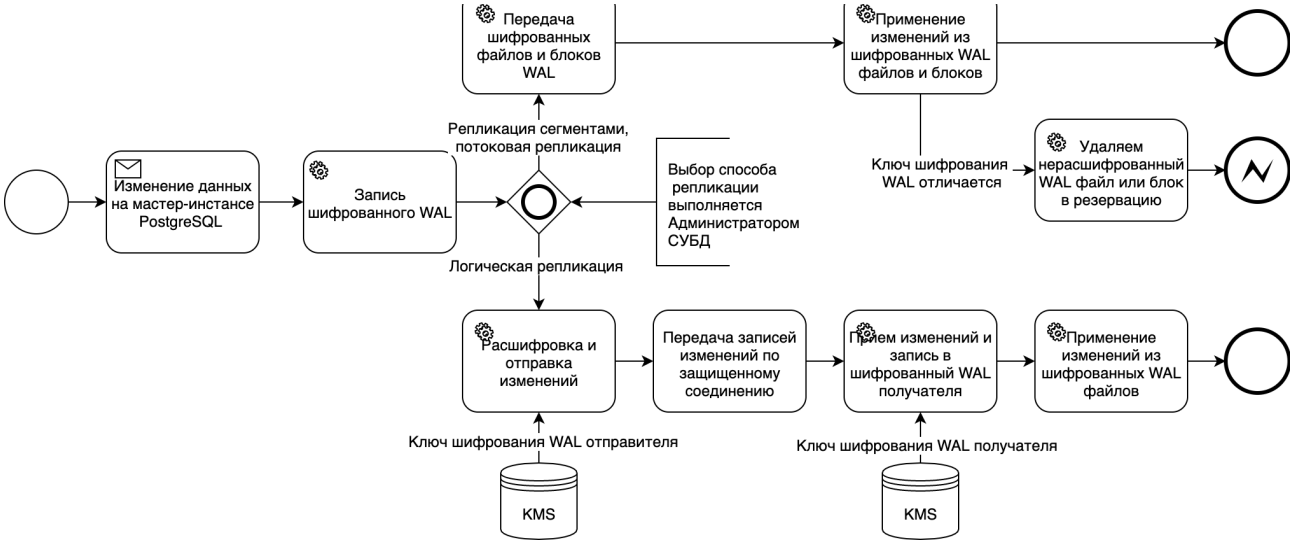
Создание резервной копии БД, содержащей зашифрованные данные



Восстановление из бинарной резервной копии БД



Репликация между серверами PostgreSQL, содержащими зашифрованные данные


Передача шифрованных файлов и блоков WAL
Применение изменений из шифрованных WAL файлов и блоков
Репликация сегментами, потоковая репликация
Изменение данных на мастер-инстансе PostgreSQL
Запись шифрованного WAL
Выбор способа репликации выполняется Администратором СУБД
Ключ шифрования WAL отличается
Удаляем нерасшифрованный WAL файл или блок в резервацию
Логическая репликация
Расшифровка и отправка изменений
Передача записей изменений по защищенному соединению
Прием изменений и запись в шифрованный WAL получателя
Применение изменений из шифрованных WAL файлов
Ключ шифрования WAL отправителя
Ключ шифрования WAL получателя
KMS
KMS

1 Руководство для сотрудника сопровождения

Сотрудник сопровождения (Администратор PostgreSQL) участвует в процессах (см. Схемы процесса):

- Первоначальная настройка шифрования для сервера СУБД PostgreSQL
- Смена мастер-ключа шифрования
- Восстановление шифрования БД при сбое процесса перешифрования БД
- Шифрование БД и объектов БД
- Создание резервной копии БД, содержащей зашифрованные данные
- Восстановление из бинарной резервной копии БД

Первоначальная настройка шифрования для сервера СУБД PostgreSQL

- Администратор БД выводит из обслуживания СУБД PostgreSQL для настройки шифрования. Остановка СУБД не производится.
- Администратор БД вводит в обслуживание СУБД PostgreSQL после настройки шифрования.

Смена мастер-ключа шифрования

- Администратор БД может вызывать функцию перешифрования ключей с коррекцией используемого мастер-ключа

Восстановление шифрования БД при сбое процесса перешифрования БД

- Администратор БД вызывает функцию восстановления шифрования
- Администратор БД выполняет перешифрование ключей шифрования, закодированных предыдущим мастер-ключем, с использованием актуального ключа. Ключи, закодированные актуальным ключем - остаются без изменений
- Администратор БД выполняет восстановление системного каталога ключей шифрования из бэкапа.

Шифрование БД и объектов БД

- Администратор БД создает шифрованное табличное пространство по-умолчанию для создаваемой шифруемой БД
- Администратор БД создает шифрованное временное табличное пространство для создаваемой шифруемой БД.
- Администратор БД создает шифрованное табличное пространство данных для создаваемой шифруемой БД.
- Администратор БД создает шифруемую базу данных, которая размещается в ранее созданных шифруемых табличных пространствах
- Администратор БД создает объекты базы, с указанием табличных пространств для размещения, или же размещаемых в табличном пространстве по-умолчанию

Создание резервной копии БД, содержащей зашифрованные данные

- Администратор БД инициирует создание бэкапа БД
- Администратор БД выполняет выгрузку бинарного бэкапа с шифрованными данными без их раскрытия
- Администратор БД выполняет выгрузку скрипта заполнения БД

Восстановление из бинарной резервной копии БД

- Администратор БД выводит из обслуживания приложений сервер PostgreSQL. Остановка СУБД не производится
- Администратор БД выполняет восстановление БД из бинарного бэкапа
- Администратор БД вводит в обслуживания приложений сервер PostgreSQL после восстановления.

2 Руководство для администратора безопасности

Администратор безопасности (Сотрудник ИБ) участвует в процессах (см. Схемы процесса):

- Первоначальная настройка шифрования для сервера СУБД PostgreSQL
- Смена мастер-ключа шифрования

Первоначальная настройка шифрования для сервера СУБД PostgreSQL

- Сотрудник ИБ выполняет настройку параметров СУБД, относящихся к шифрованию данных
- Сотрудник ИБ задает или генерирует мастер-ключ шифрования БД в KMS

Смена мастер-ключа шифрования

- Сотрудник ИБ задает или генерирует мастер-ключ шифрования БД в KMS

Настройка соединения с KMS на экземпляре СУБД PostgreSQL

Для настройки соединения администратор безопасности:

1. *запускает **setup_kms_credentials** утилиту на экземпляре СУБД PostgreSQL:*

```
$ /usr/local/pgsql/bin/setup_kms_credentials
Press Ctrl+C to exit
Choose action:
1. Set credentials
2. Show credentials
1
Choose credentials domain:
1. KMS
2. POSTGRESQL
1
Choose credentials type:
1. Userpass Auth Method
2. AppRole Auth Method
1
Enter path to file with KMS connection settings:
/home/postgres/pg_cluster/data/enc_connection_settings.cfg
Enter IP address:
10.53.67.97
Enter port:
8200
Enter login:
adminencryption
Enter password:
******
Confirm password:
******
Credentials for KMS with 'Userpass Auth Method' has been set successfully
```

2. *Установить права доступа на созданный файл:*

```
$ chmod 600 /usr/local/pgsql/data/enc_connection_settings.cfg
```

3 Руководство для разработчика прикладных сервисов

Реализованная функциональность не содержит инструкций для разработчика прикладных сервисов.