SOLAR

SafeConnect

Версия 1.17.0

Инструкция по настройке репликации

Москва, 2026

Содержание

Перечень терминов и сокращений 3
1. Настройка репликации с использованием HAProxy, Patroni и etcd 4
    1.1. Общие сведения 4
    1.2. Настройка репликации 5
    1.3. Ручная настройка webrdp, kiosk, webssh 11
    1.4. Проверка статуса кластера и логов Patroni 11
2. Миграции на новую схему репликации с версии 1.13.1 (и ранее) 12
    2.1. Описание архитектуры 12
        2.1.1. Схема работы репликации в SafeConnect 1.13.1 (и ниже) 12
        2.1.2. Схема работы репликации в SafeConnect 1.14.0 (и выше) 13
        2.1.3. Сравнение версий 15
    2.2. Миграция на новую схему репликации 16

Перечень терминов и сокращений

БД	База данных
ОС	Операционная система
AD	Active Directory – это служба каталогов, разработанная компанией Microsoft для операционных систем Windows
DNS	(Domain Name System) – распределённая иерархическая система, которая преобразует доменные имена в IP-адреса и тем самым обеспечивает доступ к ресурсам в интернете
etcd	Надежное распределенное хранилище «ключ-значение», которое позволяет координировать конфигурации и обнаруживать сервисы в динамичных и масштабируемых средах
HA	High Availability – высокая доступность
IP	(Internet Protocol) — это сетевой протокол, который обеспечивает передачу данных между устройствами в сети, например, в интернете. Он определяет правила и механизмы для адресации, маршрутизации и передачи данных, гарантируя, что пакеты с информацией достигают нужного получателя
NTP	(Network Time Protocol) – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
WAL	(Write-Ahead Log – журнал упреждающей записи) – это механизм в PostgreSQL, который фиксирует изменения в данных перед их фактическим сохранением в базе данных. Он позволяет восстановить базу данных до последнего сохранённого состояния в случае сбоя
Кластер	Совокупность серверов, соединённых между собой управляющими связями.
Узел	Сервер в составе информационной системы

1. Настройка репликации с использованием HAProxy, Patroni и etcd

1.1. Общие сведения

Для работы SafeConnect в режиме высокой доступности требуется отказоустойчивый сервис БД PostgreSQL. Все узлы SafeConnect подключаются к данному сервису и работают с ним. Процесс синхронизации между узлами включает в себя копирование всех созданных данных, за исключением настроек NTP, Syslog, сетевых настроек и лицензирования.

Примечание

Настройки кастомизации (брендирования) обновляются отдельно от остальных параметров и могут быть оперативно обновлены перезапуском узла.

В данном разделе описано построение отказоустойчивого кластера PostgreSQL с использованием HAProxy, Patroni и etcd.

Для работы Patroni требуется распределенное хранилище etcd:

- минимальный набор узлов с etcd = 3;
- минимальный набор узлов с Patroni = 2.

Для оптимизации работы Patroni под условия заказчика можно обратиться к документации Patroni (**https://patroni.readthedocs.io/en/rel_3_3/**) .

Взаимодействие разных компонентов системы друг с другом реализовано по портам: 2379, 2380, 5416, 5432, 6432, 8018.

Примечание

Ввиду небольшого размера БД SafeConnect сервис устанавливается на самих узлах. При установке SafeConnect требуемые пакеты уже установлены и необходимо настроить их работу.

Все пароли, токены, IP-адреса в данной инструкции приведены для примера.

Внимание!

При изменении настроенной конфигурации кластера для сохранения данных нужно использовать функционал добавления/удаления членов кластера etcd.

Во время проведения работ сервис SafeConnect будет недоступен!

1.2. Настройка репликации

SafeConnect может работать в кластерной конфигурации. Для того чтобы обеспечить синхронизацию данных между несколькими Порталами, работающими в «кластерной» конфигурации, необходимо настроить репликацию данных между этими Порталами. Настройка осуществляется в веб-интерфейсе Портала в разделе **Настройки > Репликация** путем формирования конфигурационного файла и его загрузки на каждый из узлов кластера.

Внимание!

Если несколько администраторов будут вводить данные в разные Порталы (произвольно), то в случае конфликта ввода данных (администраторы вводят информацию в одни и те же поля), сохранятся данные, введенные последними. Вне зависимости от того на каком Портале это было сделано.

Для работы репликации необходимы HAProxy, Patroni и etcd.

Примечание

Предварительная настройка HAProxy, Patroni и etcd не требуется, так как при установке каждого узла SafeConnect эти компоненты автоматически устанавливаются и настраиваются.

Для настройки репликации следует:

Внимание!

Перед включением репликации необходимо выключить интеграцию с NTP-сервером!

1. Перейти в раздел **Настройки > Репликация** (Рис.1.1).

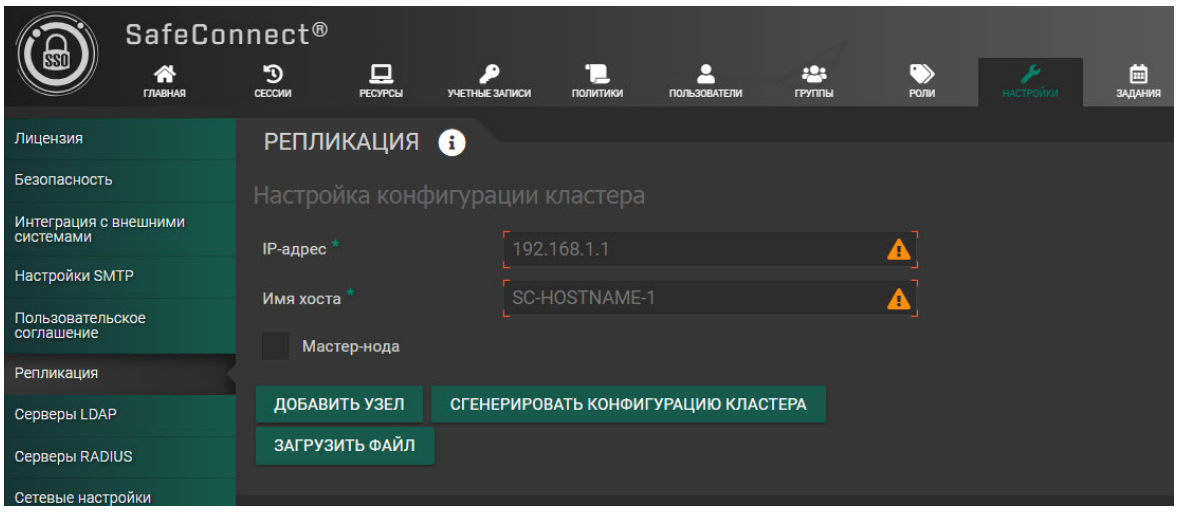


Рис. 1.1. Раздел «Репликация»

2. Добавить IP-адрес узла для репликации и имя узла (Рис.1.2). Если этот узел будет основным в кластере, установить флажок **Мастер-нода**.

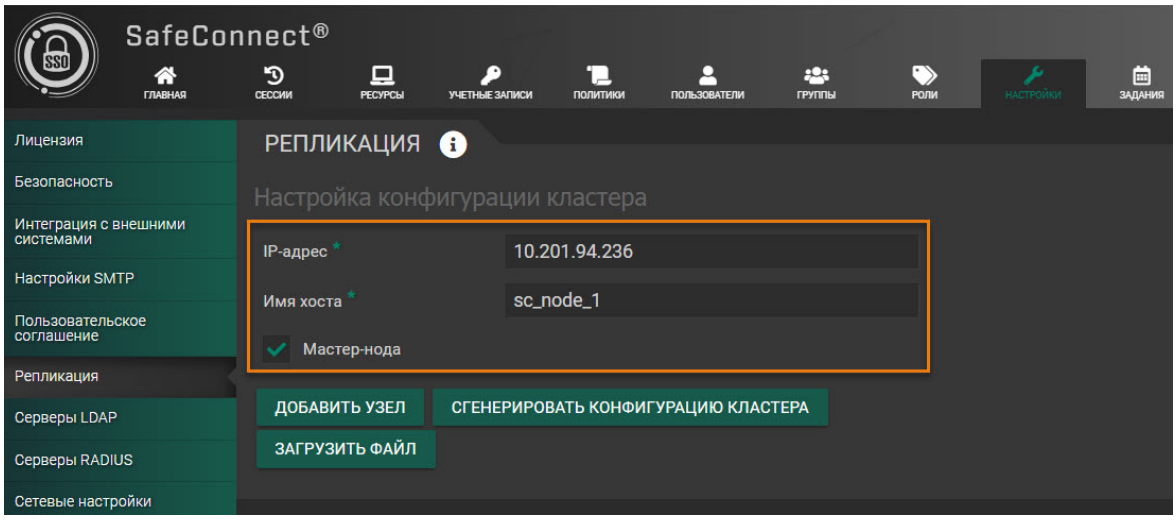


Рис. 1.2. Настройка IP-адреса и имени узла

3. Для формирования кластера репликации добавить несколько узлов кнопкой **Добавить узел** (Рис.1.3).

   Каждому узлу задать IP-адрес и имя.

Внимание!

Для корректной работы репликации требуется минимум 3 узла.

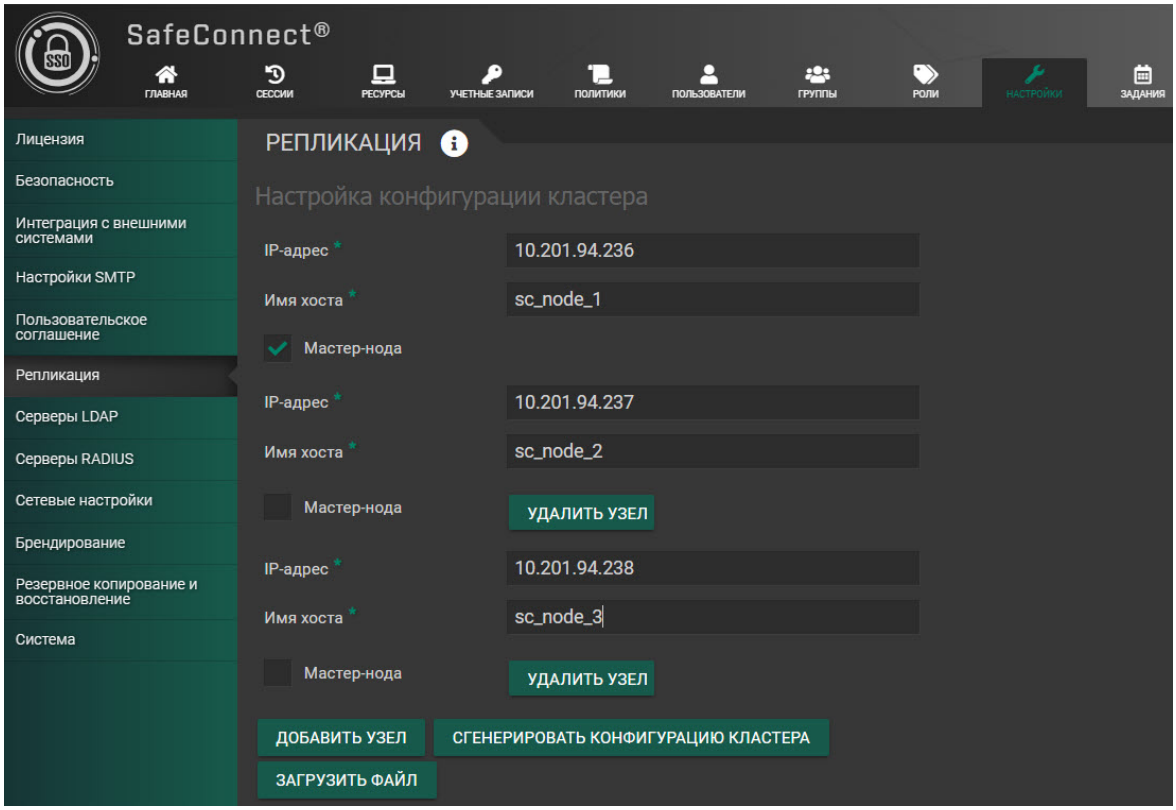


Рис. 1.3. Настройка нескольких узлов

4. После добавления и настройки всех узлов нажать кнопку **Сгенерировать конфигурацию кластера**.

5. На основном узле кластера (с установленным флажком **Мастер-нода**) войти в раздел **Настройки > Репликация** и загрузить созданную конфигурацию, используя кнопку **Загрузить файл** (Рис.1.4).

Внимание!

После загрузки файла все данные узла будут удалены, а сервисы – перезагружены. Возникающие при этом сообщения можно игнорировать.

После загрузки файла автоматически будет создана новая база данных.

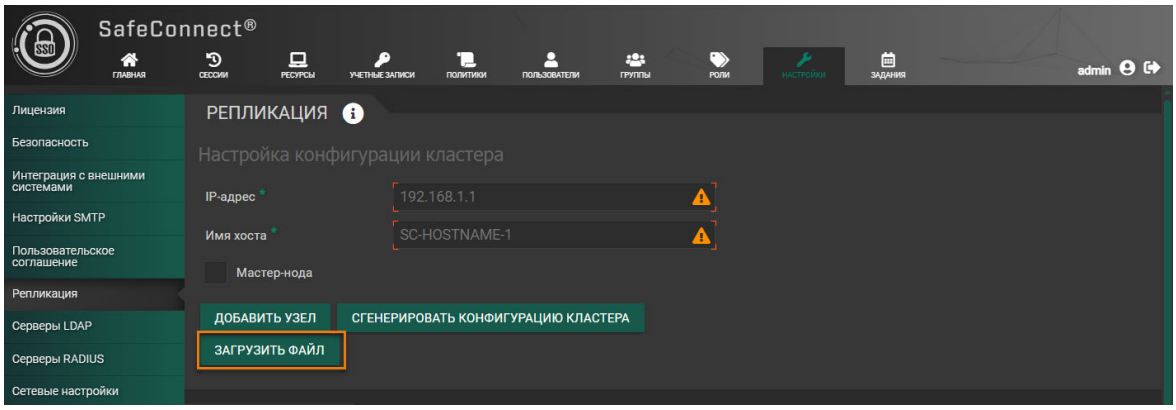


Рис. 1.4. Загрузить файл конфигурации

6. Подождать несколько минут и обновить страницу. Откроется окно создания пользователя с ролью **Главный администратор** (Рис.1.5). Создание пользователя требуется, так как при выполнении предыдущих шагов была создана новая пустая БД.

Внимание!

Применение настроек происходит не сразу, для обновления статуса репликации требуется обновить страницу.

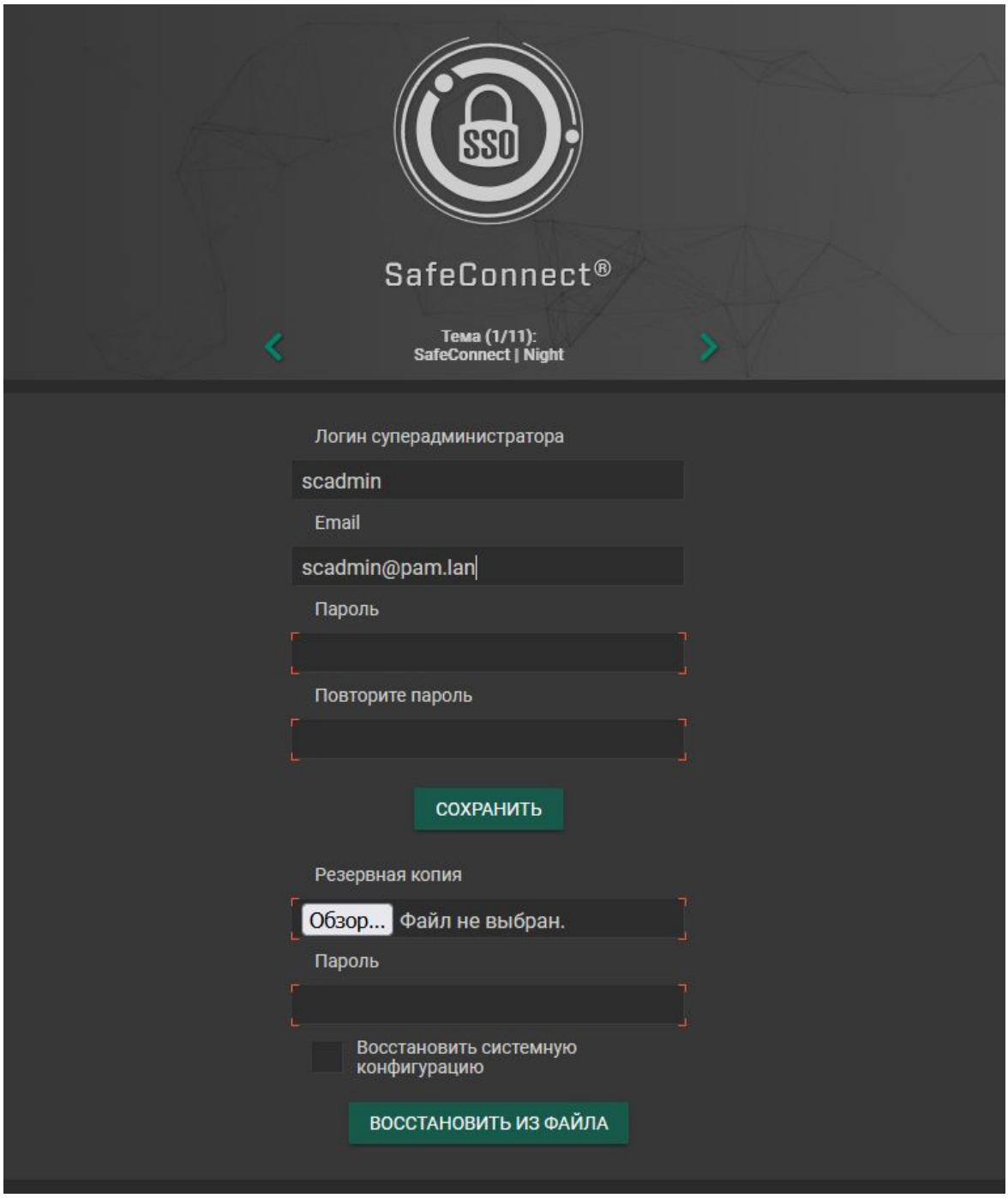


Рис. 1.5. Окно создания пользователя с ролью «Главный администратор»

7. Создать пользователя с ролью **Главный администратор**. Эта учетная запись будет основной для дальнейшей настройки кластера репликации и управления узлов в целом.

8. Последовательно войти в раздел **Настройки > Репликация** каждого из узлов создаваемого кластера (указанных в файле конфигурации), и загрузить файл конфигурацию, используя кнопку **Загрузить файл** (Рис.1.4).

Примечание

После конфигурирования всех узлов кластера запустится процесс синхронизации между узлами: копирование всех созданных данных, за исключением настроек NTP, Syslog, разделов брендирования и лицензирования.

9. После конфигурирования всех узлов кластера на одном из узлов войти в раздел **Настройки > Репликация** и проверить статус репликации и узлов кластера в блоке **Мониторинг** (Рис.1.6).

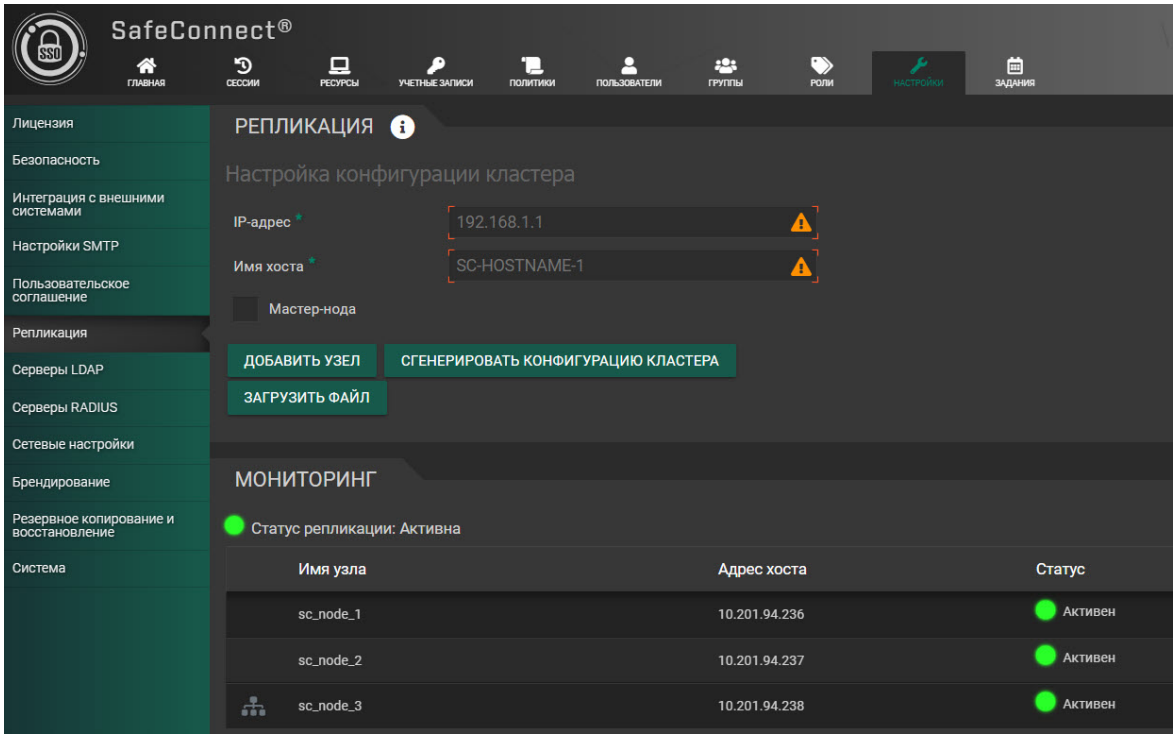


Рис. 1.6. Статус репликации и узлов кластера в блоке «Мониторинг»

10. После настройки и включения репликации можно произвести настройку NTP и Syslog (инструкции по настройке описаны в документе *Руководство администратора*).

Внимание!

Настройки NTP и Syslog на всех узлах должны быть идентичными!

Примечание

Данные, созданные при выключенной репликации, после запуска скопированы не будут.

Взаимодействие разных компонентов системы друг с другом реализовано по портам 2379, 2380, 5416, 5432, 6432, 8018.

11. Выполнить ручную настройку webrdp, kiosk, webssh по инструкции в разделе 1.3.

1.3. Ручная настройка webrdp, kiosk, webssh

Внимание!

При возникновении ошибки подключения к целевым ресурсам выполните команды.

Для выполнения настройки необходимо:

1. Получить пароль от БД для выполнения команды:

```
PG_PASSWORD=$(awk '/admin:/ {found=1} found && /password:/ {print $2; exit}'
/etc/patroni/config.yml)
```

2. Получить секреты узла SafeConnect, подставить их в файлы конфигурации сервисов, перезапустить сервисы единой командой:

```
sudo ansible-playbook -i localhost, --connection=local --extra-vars
"ansible_python_interpreter=/usr/bin/python3 db_user=www-data db_name=portal
db_password=$PG_PASSWORD" --start-at-task "Get node_id for component configuration" /opt/sc-
ansible/roles/sc-manager/tasks/replication.yml
```

1.4. Проверка статуса кластера и логов Patroni

Проверить логи Patroni командой:

```
journalctl -u patroni -r
```

Проверить статус кластера Patroni командой:

```
patronictl -c /etc/patroni/config.yml list
```

Пример вывода команды:

```
+---------+--------------+---------------------+--------+---------+----+-----------+
| Cluster |    Member    |        Host         |  Role  |  State  | TL | Lag in MB |
+---------+--------------+---------------------+--------+---------+----+-----------+
|   pam   | QA-SSO-SC-01 | 192.168.151.31:5416 | Leader | running | 12 |         0 |
|   pam   | QA-SSO-SC-02 | 192.168.151.32:5416 |        | running | 12 |         0 |
+---------+--------------+---------------------+--------+---------+----+-----------+
```

Рис. 1.7. Статус кластера Patroni

2. Миграции на новую схему репликации с версии 1.13.1 (и ранее)

В данном разделе описывается процесс перехода от схемы репликации в версии SafeConnect 1.13.1 (и ниже) к новой схеме, а также приводятся необходимые предварительные проверки, требования к окружению и рекомендации по снижению рисков при выполнении работ.

Новая схема репликации направлена на повышение отказоустойчивости, улучшение производительности и упрощение сопровождения системы SafeConnect. В документе рассматриваются особенности архитектуры обновленного решения, порядок подготовки к миграции, пошаговые сценарии выполнения операций, а также действия по проверке корректности работы после перехода.

Инструкция, приведенная в этом разделе, может использоваться как при плановом обновлении существующих инсталляций, так и при развертывании новых стендов с последующей миграцией данных. Соблюдение описанных в документе шагов и рекомендаций позволит обеспечить контролируемый и предсказуемый процесс перехода на новую схему репликации с минимальным влиянием на текущую эксплуатацию SafeConnect.

2.1. Описание архитектуры

2.1.1. Схема работы репликации в SafeConnect 1.13.1 (и ниже)

На схеме (Рис.2.1) показана архитектура из трёх серверов с репликацией SafeConnect версии 1.13.1 (и ниже) баз данных (далее – БД) **PostgreSQL** с помощью сервиса **Bucardo.**

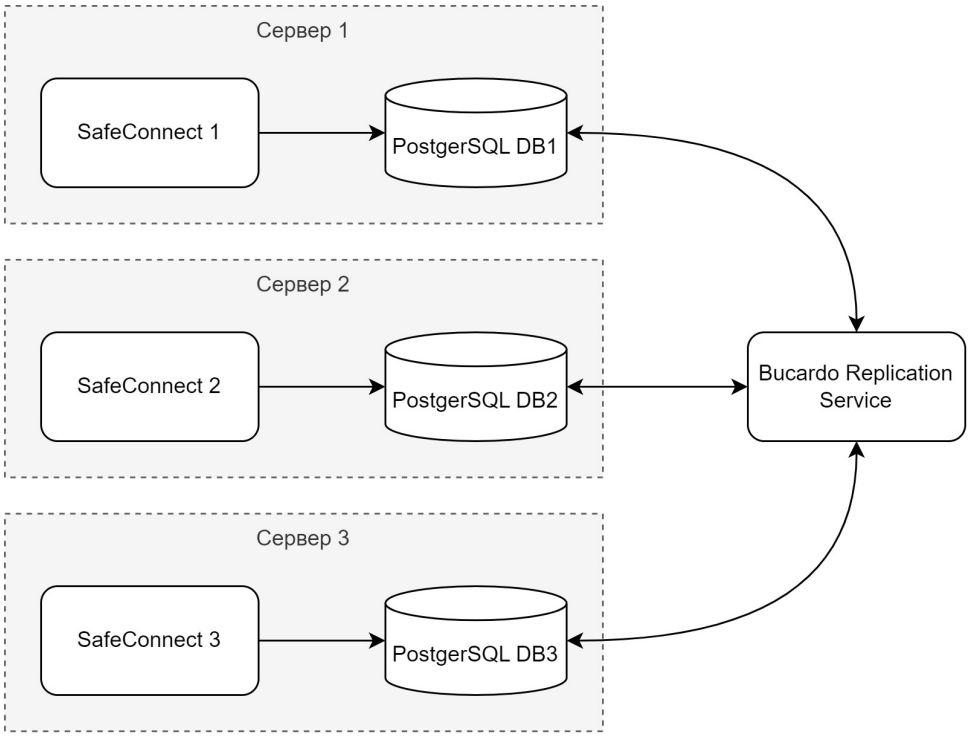


Рис. 2.1. Схема репликации в SC 1.13.1 (и ниже)

Сервер 1:

- Узел SafeConnect обращается к локальной БД PostgreSQL DB (далее – DB1).
- Между узлом SafeConnect и DB1 есть прямое соединение: портал читает и записывает данные в свою БД.

Сервер 2:

- Аналогично, на втором сервере есть свой узел SafeConnect и своя БД PostgreSQL (далее – DB2).
- SafeConnect на сервере 2 напрямую взаимодействует с DB2.

Сервер 3

- На третьем сервере также развернут SafeConnect и локальная PostgreSQL (далее – DB3).
- SafeConnect подключается к DB3 и выполняет с ней все операции.

Сервис репликации Bucardo:

- Отдельно выделен компонент Bucardo Replication Service, который отвечает за репликацию данных между тремя БД DB1, DB2 и DB3.
- Каждая БД (DB1, DB2, DB3) двунаправленно связана с Bucardo: данные могут передаваться от БД к Bucardo и обратно.

В итоге:

- На каждом из трёх серверов работает узел SafeConnect со своей локальной БД PostgreSQL.
- Сервис **Bucardo** обеспечивает обмен и синхронизацию данных между всеми БД, формируя распределённую репликацию между серверами.

2.1.2. Схема работы репликации в SafeConnect 1.14.0 (и выше)

На схеме (Рис.2.2) изображена архитектура высокодоступного (High Availability, HA) кластера **PostgreSQL,** к которому подключаются несколько узлов SafeConnect через балансировщик HAProxy и управляющий кластер **Patroni**.

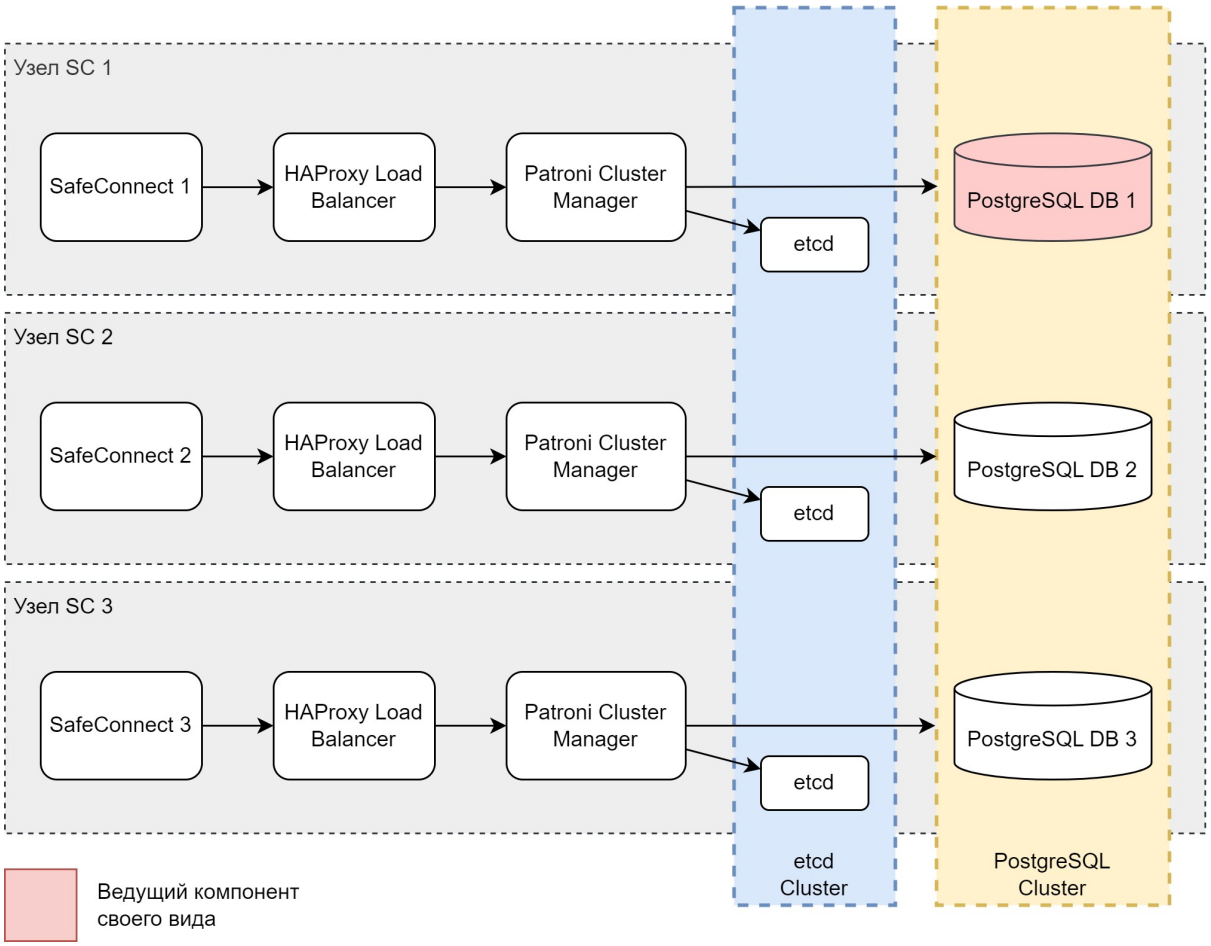


Рис. 2.2. Схема репликации в SC 1.14.0

В блоках **Узел SC N** находятся компоненты SafeConnect, HAProxy Load Balancer, Patroni Cluster Manager, etcd и PostgreSQL DB, которые реализуют отказоустойчивый кластер баз данных PostgreSQL с надежным подключением нескольких приложений SafeConnect.

SafeConnect:

Приложение SafeConnect подключается к компоненту HAProxy, а не напрямую к БД PostgreSQL. При этом запросы всегда передаются основной БД.

HAProxy Load Balancer:

Балансировщик нагрузки HAProxy периодически получает от Patroni Cluster Manager информацию о том, какая БД сейчас является основной. Опрос проводится автоматически каждые 15 секунд.

HAProxy использует эти данные для прозрачного перенаправления запросов SafeConnect к основной БД.

Patroni Cluster Manager:

- Patroni отвечает за управление кластером PostgreSQL: выбор основной БД, переключение ролей при сбоях (failover), контроль состояния БД.
- Проверяет наличие основной БД в кластере etcd;

- Если основная БД не найдена, Patroni вставляет новое значение в etcd, утверждая нового лидера;
- Если основная БД изменилась, Patroni сигнализирует об этом HAProxy;
- На схеме Patroni подключён к кластеру БД. Это показывает, что Patroni контролирует все три БД PostgreSQL.
- Связь Patroni и etcd отражает использование кластера etcd как распределённого хранилища конфигурации, чтобы все серверы БД мгновенно узнавали, кто сейчас является главным, и не допускали одновременной работы двух основных БД при сбоях.

Etcd Cluster:

- etcd служит для хранения служебной информации Patroni: какие БД в кластере активны, их состояние и конфигурация, какая из БД является ведущей.
- Между всеми etcd в кластере есть взаимосвязи.
- За счёт etcd Patroni может надёжно согласовывать решения о смене основной БД, избегая состояния, при котором из-за потери связи в кластере появляются две основные БД, что приводит к порче и рассинхронизации данных (split-brain). При падении основной БД новый лидер определяется голосованием.
- На схеме это выражено связью Patroni и etcd, где etcd выступает как внешний отказоустойчивый координатор.

PostgreSQL Cluster:

- В блоке PostgreSQL Cluster находятся три БД PostgreSQL.
- Между всеми БД в кластере есть взаимосвязи.
- Конкретная роль (основная БД или реплика) в каждый момент времени определяется Patroni, который следит за состоянием и при необходимости инициирует переключение

В итоге:

- Приложения SafeConnect подключаются к кластеру БД PostgreSQL через HAProxy, не зная, какая БД PostgreSQL сейчас основная.
- Patroni управляет кластером БД (ролями, репликацией, failover) и использует etcd для распределённой координации.
- Три БД PostgreSQL образуют отказоустойчивый кластер, в котором данные реплицируются между БД, обеспечивая высокую доступность и непрерывность работы для узлов SafeConnect.

2.1.3. Сравнение версий

Основные недостатки Bucardo (репликация в SafeConnect 1.13.1 и ниже) по сравнению со связкой Patroni + etcd (репликация в SafeConnect 1.14.0 и выше) обусловлены разницей в архитектуре: Bucardo – это логическая репликация на триггерах, тогда как Patroni управляет физической потоковой репликацией для обеспечения высокой доступности.

Ключевые недостатки Bucardo:

- **Высокая нагрузка на БД (Overhead)**: Bucardo использует триггеры для отслеживания изменений в каждой таблице. Это создает дополнительные накладные расходы на диск, процессор и увеличивает время выполнения каждой транзакции на источнике. Patroni использует штатные WAL-логи, что практически не нагружает БД.
- **Отсутствие автоматического переключения при сбое (Failover)**: Bucardo предназначен для синхронизации данных, а не для управления состоянием кластера. В случае падения основного сервера Bucardo не переключит трафик на реплику автоматически. Patroni же специально создан для автоматического выбора нового лидера через etcd, исключая риск рассинхронизации данных (split-brain).
- **Сложность поддержки схемы**: При изменении структуры таблиц в Bucardo часто требуется ручное вмешательство или перенастройка репликационных сетов. Физическая репликация в Patroni автоматически передает все изменения структуры.
- **Конфликты данных**: Поскольку Bucardo часто используется в режиме Multi-Master, возникают конфликты при одновременной записи в одну строку на разных серверах, которые нужно разрешать программно. Patroni работает в режиме Single-Master, что гарантирует строгую согласованность данных.
- **Устаревание технологии**: Bucardo обновляется редко (последние значимые версии выходили несколько лет назад) и считается полу-устаревшим решением после появления встроенной логической репликации в PostgreSQL 10+.

Резюме: Bucardo хорош для выборочной репликации данных между разными версиями ОС/БД или сложной синхронизации. Для обеспечения надежности и High Availability промышленным стандартом является Patroni + etcd.

2.2. Миграция на новую схему репликации

Для миграции на новую схему репликации необходимо выполнить следующее:

1. Остановить работу на всех узлах SafeConnect.
2. Снять и сохранить резервную копию основной БД PostgreSQL по инструкции в разделе **Резервное копирование и восстановление** документа *Руководство администратора*.
3. Выполнить настройку кластера репликации на всех узлах SafeConnect по инструкции в разделе 1.
4. Восстановить резервную копию основной БД PostgreSQL в БД каждого узла кластера по инструкции в разделе **Резервное копирование и восстановление документа** [Руководство администратора].
5. Продолжить работу на всех узлах SafeConnect.