ИНФРАСТРУКТУРА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Руководство администратора Агента СМЭВ4

Версия 3.11.0

**ПОДД СМЭВ**

Листов 52

Москва, 2024

Содержание

[1 Введение 5](#_Toc162862279)

[1.1 Область применения 5](#_Toc162862280)

[1.2 Краткое описание возможностей 5](#_Toc162862281)

[1.3 Уровень подготовки пользователя 5](#_Toc162862282)

[1.4 Перечень документации для работы с ПОДД СМЭВ 5](#_Toc162862283)

[2 Назначение и условия применения 6](#_Toc162862284)

[2.1 Назначение 6](#_Toc162862285)

[2.2 Требования к среде для развертывания Агента СМЭВ4 6](#_Toc162862286)

[2.2.1 Минимальные требования к серверу 6](#_Toc162862287)

[2.2.2 СКЗИ для работы Агента СМЭВ4 6](#_Toc162862288)

[2.3 Точки подключения к Агенту СМЭВ4 7](#_Toc162862289)

[3 Описание конфигурационного файла 8](#_Toc162862290)

[3.1 Состав и содержание файлов конфигурирования 8](#_Toc162862291)

[3.2 Реестр изменений файлов конфигурирования 8](#_Toc162862292)

[3.3 Формирование конфигурационного файла 10](#_Toc162862293)

[3.3.1 Общие настройки Агента 10](#_Toc162862294)

[3.3.2 Настройка CryptoPro 11](#_Toc162862295)

[3.3.3 Настройка регистрации Витрин и подключения к kafka (при использовании Витрин) 12](#_Toc162862296)

[3.3.3.1 Настройка создания топиков Агентом СМЭВ4 12](#_Toc162862297)

[3.3.3.2 Настройка параметров создаваемых топиков (опционально) 15](#_Toc162862298)

[3.3.3.3 Настройка взаимодействия через пользовательские топики (опционально) 15](#_Toc162862299)

[3.3.4 Настройка подключения к Ядру ПОДД СМЭВ, в том числе для работы в гео-распределенной конфигурации 18](#_Toc162862300)

[3.3.5 Настройка модуля подписания печатных форм 19](#_Toc162862301)

[3.3.6 Настройка приема и передачи БЛОБов (опционально) 20](#_Toc162862302)

[3.3.6.1 Настройка автоматического скачивания БЛОБ по ссылке Агентом СМЭВ4 20](#_Toc162862303)

[3.3.6.2 Настройка использования S3 для передачи БЛОБов 20](#_Toc162862304)

[3.3.7 Настройки разбиения получаемой информации на чанки (опционально) 21](#_Toc162862305)

[3.3.8 Настройка организации информационного обмена через API Gateway (опционально) 21](#_Toc162862306)

[3.3.9 Настройка параметров времени активации Агента СМЭВ4 (опционально) 23](#_Toc162862307)

[3.3.10 Настройка подключения к масштабированному Агенту СМЭВ4 (опционально) 23](#_Toc162862308)

[3.3.11 Настройка подключения к NTP 24](#_Toc162862309)

[3.3.12 Настройка типа аутентификации агента в ядре 24](#_Toc162862310)

[4 Настройка и запуск Агента СМЭВ4 25](#_Toc162862311)

[4.1 Порядок загрузки данных и программ 25](#_Toc162862312)

[4.2 Подготовка и настройка системы для запуска Агента СМЭВ4 без использования docker 25](#_Toc162862313)

[4.2.1 Состав и содержание дистрибутивного пакета 25](#_Toc162862314)

[4.2.2 Предварительные операции (установка «пре-реквизитов») 25](#_Toc162862315)

[4.2.3 Запуск Агента СМЭВ4 27](#_Toc162862316)

[4.2.4 Настройка ротации логов (опционально) 27](#_Toc162862317)

[4.3 Настройка и запуск Агента СМЭВ4 с использованием docker 28](#_Toc162862318)

[4.3.1 Предварительные условия 28](#_Toc162862319)

[4.3.2 Настройка ротации лог-файлов в docker (опционально) 29](#_Toc162862320)

[4.3.3 Состав и содержание дистрибутивного пакета 29](#_Toc162862321)

[4.3.4 Подготовка к запуску 29](#_Toc162862322)

[4.3.5 Запуск Агента СМЭВ4 30](#_Toc162862323)

[4.3.6 Информация по лицензированию CryptoPro 31](#_Toc162862324)

[4.4 Настройка предустановленного профиля Витрины в Агенте СМЭВ4 31](#_Toc162862325)

[4.5 Настройка сбора метрик Агента СМЭВ4 (опционально) 32](#_Toc162862326)

[4.5.1 Настройка Агента СМЭВ4 для передачи метрик в Prometheus 32](#_Toc162862327)

[5 Настройка и запуск NTP сервера 33](#_Toc162862328)

[5.1 Порядок загрузки данных и программ 33](#_Toc162862329)

[5.2 Настройка и запуск NTP сервиса БЕЗ использования docker 33](#_Toc162862330)

[5.2.1 Состав и содержание дистрибутивного пакета 33](#_Toc162862331)

[5.2.2 Предварительные операции (установка «пре-реквизитов») 33](#_Toc162862332)

[5.2.3 Запуск NTP сервиса 33](#_Toc162862333)

[5.3 Настройка и запуск NTP сервиса с использованием docker 33](#_Toc162862334)

[5.3.1 Предварительные условия 33](#_Toc162862335)

[5.3.2 Состав и содержание дистрибутивного пакета 34](#_Toc162862336)

[5.3.3 Подготовка к запуску 34](#_Toc162862337)

[5.3.4 Запуск NTP 34](#_Toc162862338)

[6 Типовые вопросы и проблемы 35](#_Toc162862339)

[7 Термины и определения 37](#_Toc162862340)

[8 История изменений документа 39](#_Toc162862341)

[9 Приложение А Добавление промежуточных сертификатов в ключ CryptoPro 42](#_Toc162862342)

[9.1 А.1 С использованием графического интерфейса 42](#_Toc162862343)

[9.2 А.2 С использованием командной строки ОС Linux 48](#_Toc162862344)

[10 Приложение B Список метрик Агента СМЭВ4 51](#_Toc162862345)

АННОТАЦИЯ

В данном программном документе приведено Руководство администратора Агента СМЭВ4, подсистемы, предназначенной для обеспечения доступа к данным СМЭВ, направленная на автоматизацию процесса передачи данных и уведомлений об изменении данных между организациями или органами власти, ответственными за формирование и ведение информационных ресурсов, зарегистрированных в НСУД.

В разделе «Введение» указаны область применения подсистемы, краткое описание ее возможностей, уровень необходимой подготовки пользователей подсистемы и перечень документации для работы с ПОДД СМЭВ.

В разделе «Назначение и условия применения» описано назначение подсистемы и требования к среде развертывания подсистемы.

В разделе «Подготовка к работе» описан состав и содержание дистрибутивного пакета, порядок загрузки данных, предварительные операции.

В разделе «Описание операций» описаны шаги по запуску и настройке Агента ПОДД СМЭВ.

Оформление документа произведено по требованиям ЕСПД (ГОСТ 19.101-77, ГОСТ 19.103-77, ГОСТ 19.104-78, ГОСТ 19.105-78, ГОСТ 19.106-78, ГОСТ 19.503-79, ГОСТ 19.604-78).

# 1 Введение

## 1.1 Область применения

ПОДД СМЭВ — подсистема обеспечения доступа к данным СМЭВ, направленная на автоматизацию процесса передачи данных и уведомлений об изменении данных между организациями или органами власти, ответственными за формирование и ведение информационных ресурсов, зарегистрированных в НСУД.

## 1.2 Краткое описание возможностей

ПОДД СМЭВ обеспечивает:

* + предоставление для Потребителей механизмов унифицированного доступа к данным, размещённым на Витринах Поставщиков, с использованием языка запросов, основанного на стандарте языка SQL;
  + предоставление для Потребителей возможности получения данных, связанных по ключевым полям или вычисляемому критерию;
  + предоставление для Потребителей возможности автоматического получения и актуализации данных из Витрины Поставщика посредством снапшотов и дельт;
  + доступ ИС Инициаторов к REST-сервисам ИС Ответчиков через API Gateway;
  + контроль полномочий Потребителей (Инициаторов) на доступ к данным, размещённым у Поставщиков (Ответчиков).

## 1.3 Уровень подготовки пользователя

Развертывание Агента СМЭВ4 должно осуществляться в соответствии с настоящим Руководством администратора.

Специалист должен обладать следующими знаниями и опытом:

* + администрирование КриптоПро;
  + администрирование docker (при его использовании).

## 1.4 Перечень документации для работы с ПОДД СМЭВ

Порядок подключения и использования ПОДД СМЭВ после установки Агента СМЭВ4 отражен в следующих документах [[1]](#footnote-1):

* + Методические рекомендации по работе с ПОДД СМЭВ;
  + Регламент подключения к СМЭВ 4.

# 2 Назначение и условия применения

## 2.1 Назначение

ПОДД СМЭВ состоит из следующих компонентов:

* + Ядро ПОДД СМЭВ – центральный компонент ПОДД СМЭВ, размещенный в ИЭП;
  + Агент СМЭВ4 – компонент ПОДД СМЭВ, устанавливаемый в контуре участника взаимодействия.

Агент СМЭВ4 представляет собой типовое программное обеспечение, устанавливаемое на стороне УВ и обеспечивающее сопряжение Витрин, хранилищ реплик, ИС УВ с ПОДД.

Данный документ содержит состав и содержание дистрибутивного пакета, порядок установки и описание настроек Агента СМЭВ4.

## 2.2 Требования к среде для развертывания Агента СМЭВ4

### 2.2.1 Минимальные требования к серверу

[Таблица 2.1](#_8a6d1d8e05256c19e19f11d91ca90680) содержит минимальные требования к характеристикам сервера для развертывания Агента СМЭВ4.

Таблица 2.1 Минимальные требования к характеристикам сервера для развертывания Агента СМЭВ4

|  |  |
| --- | --- |
| Характеристики | Агент СМЭВ4 |
| ОС | CentOS 7.9 |
| ЦПУ | 4-х ядерный процессор |
| Оперативная память | 8 Гб |
| Дисковое пространство | 20 Гб |

### 2.2.2 СКЗИ для работы Агента СМЭВ4

Канал связи между Агентом СМЭВ4 и Ядром ПОДД СМЭВ должен быть защищен программно-аппаратным комплексом СКЗИ с уровнем не хуже КС3.

Требования к установке СКЗИ:

* + При использовании mTLS:
    - Комплекс СКЗИ может быть установлен в другой подсети по отношению к Агенту СМЭВ4.
  + При отсутствии mTLS:
    - Комплекс СКЗИ должен быть установлен в закрытом контуре Агента СМЭВ4.
    - Комплекс СКЗИ должен быть установлен в той же подсети, что и Агент СМЭВ4.
    - Между Агентом СМЭВ4 и СКЗИ не допускается использование открытых сетей связи с возможностью доступа из вне (из сети интернет).

Для работы с электронными подписями Агенту СМЭВ4 необходимы следующие средства криптозащиты:

* + КриптоПро CSP.

Агент СМЭВ4 является сервером для всех его клиентов и при этом является клиентом для Ядра ПОДД СМЭВ.

Криптография в Агенте обеспечивается CSP.

Для аутентификации Агента в Ядре СМЭВ4 используется JWT токен.

для этого может использоваться:

1. mTLS с КриптоПро JCP
2. mTLS с stunnel
3. без mTLS, через СКЗИ с помощью подписанного запроса в keycloack
4. односторонний TLS, через СКЗИ с помощью подписанного запроса в keycloack

Таким образом, для работы Агента СМЭВ4 необходимо приобрести серверную лицензию для:

* + CryptoPro CSP 5.0;
  + CryptoPro JCP 2.0.

или другие в соответствии с применяемым вариантом канала в Ядро ПОДД СМЭВ.

[Прайс лист](https://www.cryptopro.ru/sites/default/files/docs/price.pdf) и типы лицензий доступны на официальном сайте поставщика: <https://www.cryptopro.ru/> Количество необходимых лицензий требуется рассчитать, ознакомившись с рекомендациями на сайте КриптоПро.

## 2.3 Точки подключения к Агенту СМЭВ4

[Таблица 2.2](#_87c82fc79b8df105548e3fef0d53c1b6) содержит точки подключения к Агенту СМЭВ4 и их назначение

Таблица 2.2 Точки подключения к Агенту СМЭВ4

|  |  |
| --- | --- |
| Порт (значение по умолчанию) [[2]](#footnote-2) | Назначение |
| 8183 | Обмены по Регламентированным SQL-запросам через JDBC-интерфейс |
| 8192 | * обмены по Регламентированным SQL-запросам через REST-интерфейс; * скачивание JDBC-драйвера; * получение списка спецификаций OpenAPI для Регламентированных REST-запросов. |
| 8171 (транспорт pulsar)  8172 (транспорт rsocket) | Обмены по Регламентированным REST-запросам.  Агенты Потребителя и Поставщика должны использовать единый транспорт.  Потребитель, в зависимости от используемого Поставщиком транспорта, должен направлять запросы в соответствующий этому транспорту порт Агента.  Примечания:   * Для использования транспорта rsocket, версия Агента должна быть 3.7.0 или выше как на стороне Потребителя, так и на стороне Поставщика.   При этом значение параметра agent.use-ca должно быть true как на стороне Потребителя, так и на стороне Поставщика ([Раздел 3.3.1](#_3.3.1_Общие_настройки)).   * При использовании транспорта pulsar поддерживается максимальный объем запросов не более 5 мегабайт.   Для транспорта rsocket поддерживается максимальный объем запросов не более 30 гигабайт. |

# 3 Описание конфигурационного файла

## 3.1 Состав и содержание файлов конфигурирования

Состав дистрибутива Агента СМЭВ4 (/distr/einfahrt):

* + /distr/einfahrt/certs/cp\_ca\_store – JKS с поддержкой корневых сертификатов Ростелекома (только при использовании mutual TLS - см. [Раздел 2.2.2](#_2.2.2_СКЗИ_для));
  + /distr/einfahrt/s3\_creds.properties – креденшелы для подключения к хранилищу S3 (опционально, только при использовании хранилища S3);
  + /distr/einfahrt/customLogLevels.xml – файл описания настроек логирования;
  + /distr/einfahrt/postgresql.json – файл описания профиля Витрины;
  + /conf/\*.yml – заготовки конфигурационных файлов для Потребителя и Поставщика, для тестовой и продуктивной среды.

В директории /conf/ пакета находятся типовые заготовки конфигурационного файла.

Необходимо взять заготовку конфигурационного файла в соответствии с потребностями:

* + шаблоны конфигурационного файла Агента для продуктивной среды:
    - conf/prod-consumer-application.yml – для Потребителя.
    - conf/prod-producer-application.yml – для Поставщика.
  + шаблоны конфигурационного файла Агента для продуктивной среды (2-х ЦОДовая конфигурация: ФЦОД, РЦОД):
    - conf/prodMC-consumer-application.yml – для Потребителя.
    - conf/prodMC-producer-application.yml – для Поставщика.
  + шаблоны конфигурационного файла Агента для тестовой среды (ТПОДД):
    - conf/test-consumer-application.yml – для Потребителя.
    - conf/test-producer-application.yml – для Поставщика.

Скопировать выбранный файл в каталог /distr/einfahrt под именем application.yml.

В скопированном конфигурационном файле application.yml задать необходимые параметры (в заготовке обозначены звездочками \*). Более подробное описание необходимых настроек файла application.yml указаны в разделах ниже.

## 3.2 Реестр изменений файлов конфигурирования

[Таблица 3.1](#_2db90a722b7f10ff7c0e4f734a59b204) содержит Реестр изменений. Фиксация изменений в данном документе ведётся с версии 2.11.0.

Таблица 3.1 Реестр изменений файлов конфигурирования

| Версия | Перечень изменений (относительно предыдущей версии) |
| --- | --- |
| 2.11.0 | Для экземпляров Агента СМЭВ4, использующих «печатные формы», добавлен параметр printable-form.max-content-length (Максимальный размер данных для подписания). |
| 2.12.0 | Добавлены **опциональные** параметры настроек таймаута запросов через API GW (см. [Раздел 3.3.8](#_3.3.8_Настройка_организации)).  При использовании значений по умолчанию добавление данных параметров в конфигурационный файл **не требуется**. |
| 2.12.1 | Изменений нет |
| 2.13.0 | Значительные изменения конфигурационного файла, для упрощения настроек пользователем:   * + для ряда параметров изменилось их расположение, вынесены на верхние уровни;   + параметры, значения которых не предназначены для изменения пользователем без значимых причин, убраны из конфигурационного файла.   Используйте поставляемые образцы файлов для внесения Ваших параметров подключения и применения полученного файла с Агентом СМЭВ4. |
| 2.14.0 | Изменений нет |
| 2.15.0 | * + Добавлен параметр «data-center.signature.keystore-type» с значением «JNI\_CSP»;   + Изменен формат описания печатных форм (только при их использовании). |
| 3.0.0 | * + Добавлены параметры подключения к Ядру data-center.nodes.node\*.broker-addresses;   + Версия java обновлена до 17.0.5. |
| 3.1.0 | * + В Агент добавлена дополнительная точка подключения API gateway - порт 8172 (см. [Раздел 2.3](#_2.3_Точки_подключения));   + Указана возможность изменения портов для обращения ИС Инициатора к Агенту при обмене через API Gateway (см. [Раздел 3.3.8](#_3.3.8_Настройка_организации));   + В файл конфигурации добавлен параметр podd-client.pool.size;   + Добавлены разделы по настройке и разворачиванию NTP сервиса:     - Настройка подключения к NTP;     - Настройка и запуск NTP сервиса БЕЗ использования docker;     - Настройка и запуск NTP сервиса с использованием docker. |
| 3.2.0 | * + Добавлен раздел «podd-client.routes» в конфигурационные файлы для подключения к одному ЦОД;   + Исключены параметры:   + datamart-registration.datamarts.registrationFlow;   + data-center.default-node.pulsar.auth.keycloak-connection.tls-verify- host-name;   + data-center.signature.additional-properties;   + allowance.enabled;   + Добавлен конфигурационный файл postgresql.json;   + Добавлен раздел по заданию настроек в файле postgresql.json:     - Настройка предустановленного профиля Витрины в Агенте ПОДД. |
| 3.2.1 | Изменений нет |
| 3.3.0 | * + Исключены параметры:   + api-gateway.client.options.pipelining;   + api-gateway.client.options.pipeliningLimit;   + С данного релиза возможно использование ключей КриптоПро, содержащих пробелы в алиасе;   + Изменён systemd unit для запуска агента, (см. [Раздел 4.2.3](#_4.2.3_Запуск_Агента)) |
| 3.4.0 | Изменений нет |
| 3.5.0 | * + Добавлен раздел «spring.profiles.active» для настройки активного функционала Агента СМЭВ4;   + Добавлены параметры управления созданием топиков Apache Kafka:     - datamart.create-topics.config;     - datamart.create-topics.query;     - datamart.create-topics.replication;     - datamart-registration.create-topics;     - replication.create-topics;     - query.create-topics;   + Исключены параметры:     - datamart.enabled (начиная с данной версии отключение производится с помощью выбора необходимого функционала параметром spring.profiles.active);     - Версия JDK обновлена до 17.0.6. При варианте установки без использования docker требуется обновление jdk на сервере, на котором устанавливается Агент. |
| 3.6.0 | Изменений нет |
| 3.7.0 | * + Версия JDK обновлена до 17.0.7. При варианте установки без использования docker требуется обновление jdk на сервере, на котором устанавливается Агент;     - Изменен формат указания подключения к keycloak: nodes.ID.pulsar.auth.keycloak-oauth.auth-server-url изменен на список адресов URL в параметре nodes.ID.pulsar.auth.keycloak-oauth.auth-server;   + Добавлены параметры времени активации Агента (см. [Раздел 3.3.9](#_3.3.9_Настройка_параметров));   + Добавлен параметр управления используемым транспортом (pulsar/rsocket): agent.use-ca (см. [Раздел 3.3.1](#_3.3.1_Общие_настройки));   + Удален параметр настройки передачи событий Витрины в СЦЛ через rsocket cls.datamart.use-ca, транспорт определяется общим параметром agent.use-ca (см. [Раздел 3.3.1](#_3.3.1_Общие_настройки));   + Добавлено ограничение на использование транспорта rsocket при обмене по Регламентированным REST-запросам (см. [Раздел 2.3](#_2.3_Точки_подключения)):     - значение параметра agent.use-ca должно быть true как на стороне Потребителя, так и на стороне Поставщика (см. [Раздел 3.3.1](#_3.3.1_Общие_настройки));     - версия Агента Потребителя и Поставщика должна быть не ниже 3.8.0;     - Потребитель и Поставщик должны использовать единый транспорт (rsocket/pulsar). |
| 3.8.0 | * + Добавлен параметр для управления возможностью получения метаданных Витрин при использовании JDBC-драйвера: query.metadata.storeToDb |
| 3.9.0 | Изменений нет |
| 3.9.1 | Изменений нет |
| 3.10.0 | Добавлено описание параметров создания топиков kafka (см. [Раздел 3.3.3.2](#_3.3.3.2_Настройка_параметров)) |
| 3.11.0 | Изменений нет |

## 3.3 Формирование конфигурационного файла

### 3.3.1 Общие настройки Агента

|  |
| --- |
| Внимание: |
| При использовании в качестве транспорта информационного обмена с ядром ПОДД pulsar (параметр agent.use-ca в конфигурационном файле установлен в значение false) не поддерживается одновременная работа более одного экземпляра Агента с одним и тем же agent.id. Исключение – масштабируемый Агент-Потребитель (см. [Раздел 3.3.10](#_3.3.10_Настройка_подключения)) |

1. При необходимости настроить список активного функционала Агента СМЭВ4.

*Предоставляемый шаблон конфигурационного файла имеет настройку по умолчанию для данного параметра. Применять изменения следует только в случае, если значения по умолчанию не подходят для данного Агента СМЭВ4.*

Параметр необязательный и может отсутствовать в конфигурационном файле. По умолчанию (при отсутствии в конфигурационном файле данного параметра) активен весь функционал Агента СМЭВ4.

*# Общие настройки агента*  
*# Оставить только нужные профили (т.е. только профили используемого функционала)*  
**spring**:  
 **profiles**:  
 **active**:  
 *# потребитель SQL-запросов*  
 - QueryConsumer  
 *# поставщик ответов на SQL-запросы*  
 - QueryProvider  
 *# потребитель уведомлений*  
 - ReplicationConsumer  
 *# поставщик дельт по подпискам*  
 - ReplicationProvider  
 *# потребитель REST РЗ*  
 - ApiGwConsumer  
 *# поставщик ответов по REST РЗ*  
 - ApiGwProvider

Пример: в случае использования Агента СМЭВ4 только как Инициатора (Потребителя), следует указать в данном списке в конфигурационном файле только значения \*Consumer.

1. Указать идентификатор Агента СМЭВ4 и задать настройки используемого транспорта (pulsar/rsocket):

agent:  
 # Идентификатор (мнемоника) агента  
 # При использовании id или ogrn состоящих только из цифр, их следует заключать в одинарные или двойные кавычки  
 id: \*\*\* ИДЕНТИФИКАТОР (МНЕМОНИКА) АГЕНТА \*\*\*  
 ogrn: '\*\*\* ОГРН АГЕНТА \*\*\*'  
 # использовать традиционный транспорт обмена с Ядром (pulsar, значение false)  
 # либо альтернативный вариант транспорта (rsocket, значение true)  
 use-ca: false

1. Получение информации о метаданных Витрин в Агенте СМЭВ4 (опционально)

Данная конфигурация не влияет на возможность исполнения информационного обмена и нужна только для получения возможности просмотра метаданных Витрин при использовании JDBC-драйвера. Для включения необходимо переопределить значение переменной в конфигурационном файле на true:

**query**:  
 **metadata**:  
 **storeToDb**: true

### 3.3.2 Настройка CryptoPro

Указать идентификатор и пароль ключа CryptoPro:

keys:  
 alias: \*\*\* ИДЕНТИФИКАТОР КЛЮЧА CryptoPro \*\*\*  
 password: \*\*\* ПАРОЛЬ КЛЮЧА CryptoPro \*\*\*

В случае, если алиас ключа КриптоПро содержит пробелы, его следует заключить в одинарные кавычки.

Указать путь к файлу trust store и пароль к нему (**только при использовании mTLS**, см. [Раздел 2.2.2](#_2.2.2_СКЗИ_для)):

trust-store:  
 path: /distr/einfahrt/certs/cp\_ca\_store  
 password: \*\*\* ПАРОЛЬ К TRUST STORE \*\*\*

где:

* + path – фактический путь к файлу cp\_ca\_store из дистрибутива (в данном примере – /distr/einfahrt/certs/cp\_ca\_store);
  + password – пароль от cp\_ca\_store.

Убедитесь, что пользователь, запускающий приложение, имеет доступ на чтение к этому файлу.

### 3.3.3 Настройка регистрации Витрин и подключения к kafka (при использовании Витрин)

|  |
| --- |
| Внимание: |
| указание адреса сервера(серверов) kafka (параметр datamart.kafka-bootstrap-servers) обязателен, если используется хотя бы один профайл из списка: QueryProvider, ReplicationConsumer, ReplicationProvider. Список включенных профайлов определяется параметром spring.profiles.active, см. описание выше. |

#### 3.3.3.1 Настройка создания топиков Агентом СМЭВ4

Далее приведено описание раздела конфигурации для настройки создания топиков Агентом СМЭВ4.

Доступна настройка взаимодействия нескольких схем Витрины через одну группу топиков.

Схемы Витрины могут общаться через одну группу топиков только в случае, если относятся к одному ПО «Витрина данных» и являются схемами одной (физической) Витрины.

Блок параметров datamarts.create-topics может отсутствовать в конфигурационном файле, в этом случае используются значения по умолчанию: включено автоматическое создание топиков для всех видов информационного обмена (Регламентированные SQL-запросы, Рассылки), отключено автоматическое создание топиков регистрации и настройки Витрин.

[Таблица 3.2](#_0b7aa2920b6f03930b59789d23211012) содержит соответствие создаваемых топиков Apache Kafka параметрам конфигурационного файла.

Таблица 3.2 Соответствие параметров конфигурационного файла и создаваемых топиков

| № | Настройка | Параметр | Создаваемые топики [[3]](#footnote-3) |
| --- | --- | --- | --- |
| 1 | Топики для информационного обмена с использованием  Регламентированных SQL-запросов | query | * + Топики для обеспечения информационного обмена с использованием SQL-запросов;   + Топики для получения статистики по Витринам;   + Топики для получения событий Витрины. |
| 2 | Топики для информационного обмена с использованием  Рассылок | Replication,  ReplicationProvider | * + Топики для обеспечения информационного обмена с использованием подписок (для Поставщика);   + Топики для получения событий Витрины. |
| Replication, ReplicationConsumer | * + Топики для обеспечения информационного обмена с использованием подписок (для Потребителя);   + Топики для получения событий Витрины |
| 3 | Топики регистрации и настройки Витрин | config | Топики регистрации и настройки Витрин |

Для настройки создания топиков для обмена по Рассылкам только для Поставщика или Потребителя необходимо использовать настройки активного функционала Агента СМЭВ4 Replication, указанные в [Разделе 3.3.1](#_3.3.1_Общие_настройки).

Если инициатором обмена по Рассылке является Витрина или ИС Потребителя для корректного осуществления обмена необходимо задать один из видов настроек:

* + при использовании режима COMPATIBLE прописать Витрину в блоке datamarts:[]
  + установить режим ENABLED для создания общей группы топиков при старте Агента.

В случае отсутствия Витрин у Агента СМЭВ4 есть возможность отключить функционал в соответствии с [Разделом 3.3.1](#_3.3.1_Общие_настройки). В этом случае раздел datamart-registration может полностью отсутствовать в конфигурационном файле.

*# Общие настройки витрин*  
**datamart**:  
 *# автоматическое создание топиков витрины*  
 **create-topics**:  
 *# регистрация и настройка витрины*  
 **config**: false  
 *# информационный обмен с использованием SQL*  
 **query**: true  
 *# репликация*  
 **replication**: true  
 *# подключение к Kafka для взаимодействия с витринами*  
 **kafka-bootstrap-servers**: {{ kafka\_link }}  
  
*# Настройки регистрации витрин.*  
*# - Витрины могут регистрироваться в агенте двумя способами:*  
*# - статически - витрина прописывается в конфиге агента (блок datamarts:), в этом случае используются*  
*# прописанные для данной витрины настройки, топики витрины создаются и слушаются агентом при старте;*  
*# - динамически - автоматическая регистрация, в этом случае используется общий набор настроек (блок dynamic:);*  
*# - Если агенту приходит сообщение из ядра для незарегистрированной витрины, агент регистрирует её динамически.*  
*# - Регистрация витрины также может быть инициирована со стороны витрины, через специальный топик, в*  
*# этом случае витрина регистрируется динамически, если она не прописана статически. Это позволяет*  
*# получать профиль запросом с витрины при динамической регистрации.*  
*# - Через некоторый таймаут (inactive-cleanup-delay) если к витрине не приходят запросы, агент её*  
*# деактивирует (выключаются потребители и удаляются топики) для экономии ресурсов;*  
*# - Если агенту приходит сообщение из ядра для деактивированной витрины, агент её активирует обратно.*  
*# - Профиль витрины отсылается в ядро каждый раз при старте агента для всех динамически и статически*  
*# зарегистрированных витрин, а также во время динамической регистрации витрин;*  
  
**datamart-registration**:  
 *# Список статически регистрируемых витрин.*  
 *# Можно задать пустой список [], параметры витрины:*  
 *# id - \*\*\* ИДЕНТИФИКАТОР ВИТРИНЫ (мнемоника витрины ПОДД в нижнем регистре) \*\*\**  
 *# defined-profile - путь к файлу с предустановленным профилем витрины*  
 *# Например file:C:/profile.json, по умолчанию используется встроенный профиль datamart\_profile/postgresql.json;*  
 *# inactive-cleanup-delay - задержка перед деактивацией витрины, 0 - никогда не деактивировать, по умолчанию 0;*  
 *# topic-name-prefix - \*\*\* ЛИБО ИДЕНТИФИКАТОР ВИТРИНЫ (если не указывать, то по умолчанию id витрины) / ЛИБО ИДЕНТИФИКАТОР ГРУППЫ ВИТРИН \*\*\**  
 **datamarts**:  
 - **id**: {{ vitrine\_id1 }}  
 *# Предустановленный профиль. В данном примере используется профиль витрины по умолчанию, находящийся внутри исполняемого пакета Агента*  
 **definedProfile**: datamart\_profile/postgresql.json  
 - **id**: {{ vitrine\_id2 }}  
 *# Профиль витрины. Используется конфигурируемый пользователем файл postgresql.json.*  
 *# В данном примере файл находится в корневом каталоге Агента (там же, где конфигурационный файл application.yml).*  
 *# Возможно расположение файла профиля витрины по любому пути с любым названием.*  
 *# В этом случае исползуется формат file:/путь/к/файлу/имя.файла*  
 **definedProfile**: file:postgresql.json  
  
 *# Настройки для динамически регистрируемых витрин*  
 **dynamic**:  
 *# Режим работы динамической регистрации:*  
 *# - ENABLED - динамическая регистрация включена, общие топики создаются и слушаются агентом при старте;*  
 *# - COMPATIBLE - режим по умолчанию, для обратной совместимости. Если список статических витрин пуст (datamarts: [])*  
 *# то работает аналогично как в режиме ENABLED. Если список статических витрин не пуст, то общие топики создаются*  
 *# при первой динамической регистрации витрины;*  
 *# - DISABLED - динамическая регистрация отключена;*  
 **mode**: COMPATIBLE  
 *# Путь к файлу с предустановленным профилем витрины. Например file:C:/profile.json*  
 **defined-profile**: datamart\_profile/postgresql.json  
 *# Задержка перед деактивацией витрины, 0 - никогда не деактивировать*  
 **inactive-cleanup-delay**: 0  
 *# Префикс имен топиков, по умолчанию без префикса*  
 **topic-name-prefix**: ''

Если схема Витрины не прописана в блоке datamart-registration.datamarts, то она будет подключена через группу топиков, используемую по умолчанию.

Если прописать в конфиге несколько Витрин статически, а префикс оставить по умолчанию, то будет создана отдельная группа топиков для каждой из прописанных статически Витрин (с соответствующим префиксом).

Если прописать в конфиге несколько Витрин статически и задать префикс, то все Витрины, прописанные статически, будут общаться через общую группу с указанным префиксом.

Схемы Витрины, указанные в блоке datamart-registration.datamarts, могут быть сконфигурированы для общения через отдельную группу топиков или через группу топиков по умолчанию.

Например:

**datamart-registration**:  
 **datamarts**:  
  
*# подключение через группу топиков со значением префикса по умолчанию*  
 - **id**: {{ vitrine\_id1 }}  
 **topic-name-prefix**: 'vitrine\_id1'  
  
*# подключение нескольких схем Витрин через отдельную группу топиков*  
 - **id**: {{ vitrine\_id2 }}  
 **topic-name-prefix**: 'common'  
 - **id**: {{ vitrine\_id3 }}  
 **topic-name-prefix**: 'common'  
  
*# подключение через группу топиков по умолчанию, в соответствии с настройками*  
в блоке dynamic  
 - id: {{ vitrine\_id4 }}  
 **topic-name-prefix**: ''  
  
 **dynamic**:  
 **mode**: COMPATIBLE  
 **inactive-cleanup-delay**: 0  
 **topic-name-prefix**: ''

#### 3.3.3.2 Настройка параметров создаваемых топиков (опционально)

Для создаваемых топиков имеется возможность указывать их параметры: фактор репликации, количество партиций и т.п. Параметры влияют на все топики, создаваемые агентом

Пример:

**kafka**:  
 **topic**:  
 **property**:  
 **num.partitions**: 1 *# дефолтное значение 1*  
 **replication.factor**: 1 *# дефолтное значение 1*

Также можно задавать и другие параметры топиков, описание которых находится по адресу <https://kafka.apache.org/documentation/#topicconfigs>

Пример:

**kafka**:  
 **topic**:  
 **property**:  
 **cleanup.policy**: delete

Использование параметров не определенных в <https://kafka.apache.org/documentation/#topicconfigs> или num.partitions / replication.factor будет приводить к ошибке при создании топика

#### 3.3.3.3 Настройка взаимодействия через пользовательские топики (опционально)

Для настройки взаимодействия с Витриной через пользовательские топики необходимо:

1. Отключить автосоздание топиков Apache Kafka Агентом, указав следующие значения параметров в конфигурационном файле Агента СМЭВ4:

**datamart**:  
 *# автоматическое создание топиков витрины*  
 **create-topics**:  
 *# регистрация и настройка витрин*  
 **config**: false  
 *# информационный обмен с использованием SQL*  
 **query**: false  
 *# репликация*  
 **replication**: false

1. Отключить возможность автосоздания топиков на стороне kafka. Для этого в конфигурации Apache Kafka указать параметр auto.create.topics.enable=false в соответствии с <https://kafka.apache.org/documentation/>.
2. Создать в Apache Kafka необходимые топики вручную в соответствии с <https://kafka.apache.org/documentation/#basic_ops_add_topic>.
3. Если имена созданных топиков отличаются от имен по умолчанию, указать в конфигурационном файле Агента СМЭВ4 имена используемых топиков.

В примере указаны имена топиков, используемые по умолчанию:

**replication**:  
 **subscription**:  
 *# Топик запросов на регистрацию подписки (Агент -> Витрина)*  
 **registration-request-topic**: replication.rq  
 *# Топик ответов с успешным результатом регистрации подписки (Витрина -> Агент)*  
 **registration-result-topic**: replication.rs  
 *# Топик ответов с ошибками регистрации подписки (Витрина -> Агент)*  
 **registration-error-topic**: replication.err  
 *# Топик запросов на отмену подписки у поставщика (Агент -> Витрина)*  
 **cancel-request-topic**: replication.cancel.rq  
 *# Топик ответов с результатом отмены подписки у поставщика (Витрина -> Агент)*  
 **cancel-result-topic**: replication.cancel.rs  
 *# Топик запросов на отмену подписки у потребителя (Агент -> Витрина)*  
 **cancel-consumer-request-topic**: replication.cancel.in.rq  
 *# Топик ответов с результатом отмены подписки у потребителя (Витрина -> Агент)*  
 **cancel-consumer-result-topic**: replication.cancel.in.rs  
 *# Топик команд по репликации посылаемых от витрины в сторону ядра (Витрина -> Агент)*  
 **command-topic**: command.podd  
 *# Параметры конфигурирования топиков для запросов/ответов на создание хранилищ реплик (Агент <-> Витрина)*  
 **storage**:  
 *# Топик запросов на создание структуры для хранения реплик (Агент -> Витрина)*  
 **request-topic**: replication.in.rq  
 *# Топик ответов с ошибками создания структуры хранения реплик (Витрина -> Агент)*  
 **error-topic**: replication.in.err  
 *# Топик ответов с успешным результатом создания структуры хранения реплик (Витрина -> Агент)*  
 **response-topic**: replication.in.rs  
 *# Параметры конфигурирования топиков работы с дельтами (Агент <-> Витрина)*  
 **delta**:  
 *# Топик запросов на получение дельт от поставщиков (Агент -> Витрина)*  
 **request-topic**: delta.rq  
 *# Топик запросов на получение дельт от поставщиков (Агент -> Витрина)*  
 **request-tp-topic**: delta.tp  
 *# Топик чанков с дельтами (Витрина -> Агент)*  
 **response-topic**: delta.rs  
 *# Топик ответов с ошибками для реплик (Витрина -> Агент)*  
 **error-topic**: delta.err  
 *# Топик чанков на применение дельты потребителем (Агент -> Витрина).*  
 *# По умолчанию топик настроен под старую реализацию витрины. Для новой реализации витрины*  
 *# которая поддерживает распределенные подписки, не важно, используете вы распределенные*  
 *# подписки или обычные, в настройках агента за которым стоит новая реализация витрины*  
 *# надо поменять имя топика на delta.in.tp:*  
 **apply-request-topic**: delta.in.rq  
 *# Топик чанков на применение дельты потребителем (Агент -> Витрина)*  
 **apply-request-tp-topic**: delta.in.tp  
 *# Топик ответов с ошибками применения дельты (Витрина -> Агент)*  
 **apply-error-topic**: delta.in.err  
 *# Топик ответов с успешным результатом применения дельты (Витрина -> Агент)*  
 **apply-response-topic**: delta.in.rs  
 *# Топик уведомлений о новых данных по подпискам от поставщика (Витрина -> Агент)*  
 **notification-topic**: delta.notification  
 *# Топик уведомлений потребителя о новых данных по подпискам (Агент -> Витрина)*  
 **notification-datamart-topic**: delta.notification.in  
  
*# Настройки модуля обработки SQL подзапросов из ядра ПОДД к витрине данных*  
**sub-query**:  
 *# Настройки получения SQL подзапроса из ядра и отправки его в витрину*  
 **request**:  
 *# Топик отправки подзапросов к витрине (Агент -> Витрина)*  
 **request-topic-name**: query.rq  
 *# Топик подзапросов для вызова регламентированного запроса (хранимой процедуры) (Агент -> Витрина)*  
 **regulated-query-request-topic-name**: procedure.query.rq  
 *# Топик для передачи чанков табличного параметра (Агент -> Витрина)*  
 **table-param-topic-name**: query.tp  
 *# Топик для передачи чанков табличного параметра, нарезанных бинарно (Агент -> Витрина)*  
 **binary-table-param-topic-name**: query.tp.bin  
 **result**:  
 *# Топик получения результатов исполнения SQL подзапросов от витрины (Витрина -> Агент)*  
 **result-topic-name**: query.rs  
 *# Топик получения ошибок исполнения SQL подзапросов от витрины (Витрина -> Агент)*  
 **error-topic-name**: query.err  
 *# Топик ответов с оценкой (статистикой) по исполнению подзапросов (Витрина -> Агент)*  
 **query-estimation-topic-name**: query.estimation.rs  
  
*# Настройки модуля обработки SQL запросов отправляемых в ядро ПОДД*  
**query**:  
 *# Обработчик отмены SQL запросов*  
 **cancel**:  
 *# Топик нотификаций витрины об отмене SQL запроса (Агент -> Витрина)*  
 **request-topic-name**: cancel.rq  
 *# Топик передачи результата об отмене SQL запроса (Витрина -> Агент)*  
 **result-topic-name**: cancel.rs  
 *# Топик передачи ошибок отмены SQL запроса (Витрина -> Агент)*  
 **error-topic-name**: cancel.err  
 *# Настройки получения BLOB по ссылке*  
 **load-reference-data**:  
 *# Топик запроса по BLOB ссылке (Агент -> Витрина)*  
 **request-topic-name**: blob.rq  
 *# Ответный топик с данными (чанки) по BLOB ссылке (Витрина -> Агент)*  
 **result-topic-name**: blob.rs  
 *# Ответный топик с ошибками обработки запроса по BLOB ссылке (Витрина -> Агент)*  
 **error-topic-name**: blob.err  
  
*# Настройки модуля сбора Статистики*  
**statistic**:  
 *# Топик с запросами на сбор статистики (Агент -> Витрина)*  
 **requestTopicName**: statistic.rq  
 *# Топик с результатами сбора статистики (Витрина -> Агент)*  
 **responseTopicName**: statistic.rs  
  
*# Конфиг модуля регистрации профиля витрины в ядре*  
**datamart-profile**:  
 *# Топик с запросами профиля у витрины (Агент -> Витрина)*  
 **datamartRequestTopic**: profile.rq  
 *# Топик ответов за запросы профиля у витрины (Витрина -> Агент)*  
 **datamartResponseTopic**: profile.rs  
 *# Топик с неуспешными ответами на запросы профиля у витрины (Витрина -> Агент)*  
 **datamartErrorTopic**: profile.err  
  
**cls**:  
 **datamart-topic**: scl.signal

1. Если имена созданных топиков отличаются от имен по умолчанию, указать использование пользовательских топиков на стороне Витрины в конфигурации ПОДД-Адаптера – Модуль исполнения запросов, согласно разделу «7.1.1 Спецификация модуля ПОДД-адаптера – Модуль исполнения запросов» Руководства администратора Типового ПО «Витрина данных».

### 3.3.4 Настройка подключения к Ядру ПОДД СМЭВ, в том числе для работы в гео-распределенной конфигурации

*Предоставляемый шаблон конфигурационного файла имеет настройку по умолчанию для данного параметра. Применять изменения следует только в случае, если значения по умолчанию не подходят для данного Агента СМЭВ4.*

Для настройки Агентов необходимо перечислить все Ядра ПОДД СМЭВ (nodes), к которым подключается Агент СМЭВ4, с указанием адресов брокеров, ссылки на Pulsar и сервис авторизации Ядра ПОДД СМЭВ.

|  |
| --- |
| Внимание: |
| Масштабируемый Агент ([Раздел 3.3.10](#_a498c61ee11b980030e27df149bd7228)) должен работать только с одним Ядром ПОДД СМЭВ при использовании транспорта Pulsar, при использовании транспорта RSocket данного ограничения нет. Не масштабированный может работать с двумя Ядрами ПОДД СМЭВ через любой из транспортов (Pulsar, RSocket). |

Пример раздела конфигурации:

*# Настройки подключения ко всем ЦОД с установленным ПО ядра*  
**data-center**:  
…  
**nodes**:  
 - **node-id**: {{ node1\_name }}  
 *# Адреса брокеров (транспорт rsocket)*  
 **broker-addresses**:  
 - **host**: {{ broker1-host }}  
 **port**: {{ broker1-port }}  
 - **host**: {{ broker2-host }}  
 **port**: {{ broker2-host }}  
 *# Настройки подключения к Pulsar (транспорт pulsar)*  
 **pulsar**:  
 *# есть возможность указания нескольких адресов pulsar, для этого необходимо в переменную "serviceUrl" через запятую прописать все адреса*  
 *# прим–р - serviceUrl: pulsar://{{ address1:port }}, pulsar://{{ address2:port }}*  
 **client**:  
 **serviceUrl**: pulsar://{{ pulsar\_kernel1\_link }}  
 ...  
 **auth**:  
 **keycloak-oauth**:  
 **auth-server**:  
 *# список адресов серверов авторизации.*  
 *# Может быть указано несколько адресов списком.*  
 - **url**: {{ keycloak\_kernel1\_link\_1 }}  
 - **url**: {{ keycloak\_kernel1\_link\_2 }}  
 - **node-id**: {{ node2\_name }}  
 **broker-addresses**:  
 {...}  
 **pulsar**:  
 {...}  
 **client**:  
 **serviceUrl**: pulsar://{{ pulsar\_kernel2\_link }}  
 {...}  
 **keycloak-oauth**:  
 **auth-server**:  
 - **url**: {{ keycloak\_kernel2\_link }}  
 {...}

В блоке data-center.default-node описаны параметры, общие для подключения ко всем Ядрам ПОДД. Как правило, их изменение не требуется относительно значений по умолчанию.

### 3.3.5 Настройка модуля подписания печатных форм

Для настройки модуля подписания печатных форм необходимо перечислить используемые сертификаты для данного модуля и данные о них.

При отсутствии используемых печатных форм, данный раздел в конфигурации должен отсутствовать.

Пример раздела конфигурации:

**printable-form**:  
 *# Максимальный размер данных для подписания*  
 **max-content-length**: 268435456  
 *# Настройка каким сертификатом подписать результат какого запроса.*  
 *# Пары значений "название регламентированного запроса": "алиас сертификата"*  
 **forms**:  
 {{ form1\_name }}: {{ key1 }}  
 {{ form2\_name }}: {{ key2 }}  
 {...}  
 **signature**:  
 **printable-form-keys**:  
 -  
 **certificateAlias**: {{ key1 }}  
 **privateKeyAlias**: {{ key1 }}  
 **privateKeyPass**: {{ key1\_password }}  
  
 -  
 **certificateAlias**: {{ key2 }}  
 **privateKeyAlias**: {{ key2 }}  
 **privateKeyPass**: {{ key2\_password }}  
 {...}

### 3.3.6 Настройка приема и передачи БЛОБов (опционально)

#### 3.3.6.1 Настройка автоматического скачивания БЛОБ по ссылке Агентом СМЭВ4

*Раздел применим для Агента Потребителя. Предоставляемый шаблон конфигурационного файла имеет настройку по умолчанию для данного параметра. Применять изменения следует только в случае, если значения по умолчанию не подходят для данного Агента СМЭВ4.*

По умолчанию ссылка на скачивание БЛОБ возвращается ИС Потребителя. При необходимости настроить автоматическую выгрузку Агентом Потребителя БЛОБ по ссылке, полученной в ответе на запрос через REST-интерфейс, следует указать параметр в конфигурационном файле:

*# Настройки REST сервера исполнения SQL запросов*  
**rest-query-endpoint**:  
 *# Агент автоматически запрашивает блоб, при получении ссылки(на ЦА не влияет)*  
 **blobAutoresolve**: true

|  |
| --- |
| Примечание: |
| Настройка может быть задана при использовании передачи данных через Pulsar (раздел pulsar) и не распространяется на передачу данных с использованием брокеров (раздел broker-addresses). Описание указанных разделов приведено в [Разделе 3.3.4](#_3.3.4_Настройка_подключения). |

Примечание: механизм автоматической выгрузки БЛОБ по ссылке Агентом Потребителя поддерживается временно.

#### 3.3.6.2 Настройка использования S3 для передачи БЛОБов

*Раздел применим только при использовании S3 storage (на стороне Поставщика). В случае если хранилище S3 не используется, данный раздел в конфигурационном файле может отсутствовать.*

Для настройки использования S3 для передачи блобов следует указать адрес точки доступа и ссылку на файл с учётными данными для подключения к S3.

Bucket с соответствующим именем должен быть предварительно создан на стороне S3.

Также в файле s3\_creds.properties необходимо прописать корректные значения логина и пароля для подключения к хранилищу S3 согласно образцу в файле /distr/einfahrt/s3\_creds.properties.

В случае, если S3 не используется, адрес, bucket и путь могут быть любыми.

Пример раздела конфигурации:

**query**:  
 *# Настройки получения BLOB по ссылке*  
 **load-reference-data**:  
 *# Источник получения данных для BLOB ссылок,*  
 *# S3 - данные загружаются агентом из хранилища S3, DATAMART - запрос пересылается витрине*  
 **blob-source**: DATAMART  
 *# Настройки подключения к хранилищу S3*  
 **s3-storage**:  
 **endpoint**: http://{{ s3\_url }}/  
 *# Имя бакета*  
 **bucket-name**: {{ bucket name }}  
 *# Путь к файлу с данными для авторизации*  
 **pathToCredentialFile**: {{ /absolute/path/to/s3\_creds.properties }}

### 3.3.7 Настройки разбиения получаемой информации на чанки (опционально)

*Предоставляемый шаблон конфигурационного файла имеет настройку по умолчанию для данного параметра. Применять изменения следует только в случае, если значения по умолчанию не подходят для данного Агента СМЭВ4.*

Доступна возможность указать способ разбиения получаемой информации при выполнении Регламентированных SQL-запросов на чанки.

Для настройки разбиения получаемой информации на чанки при выполнении запроса через REST-интерфейс необходимо в конфигурационном файле Агента СМЭВ4 задать параметр tableParamChunkType, который может принимать значения:

* + EXACTLY\_CUT – позволяет разбивать информацию на чанки исходя из размера чанка (размер чанка указывается параметром tableParamChunkSize, значение по умолчанию 900 KB);
  + EVEN\_ROWS – запрещает разбиение информации между чанками (автономно десериализуемые чанки), не гарантируется соблюдение размера чанка.

Пример раздела конфигурации для настройки выполнения запросов через REST-интерфейс:

*# Настройки REST сервера исполнения SQL запросов*  
**rest-query-endpoint**:  
 ...  
 # Размер чанка пользовательского табличного параметра  
 tableParamChunkSize: 900KB  
 *# Способ разбиения пользовательского табличного параметра на чанки*  
 **tableParamChunkType**: EXACTLY\_CUT

Для настройки разбиения получаемой информации на чанки для JDBC драйвера необходимо добавить в свойства драйвера параметр tableParamChunkType, который может принимать значения:

* + EXACTLY\_CUT – позволяет разбивать информацию на чанки исходя из размера чанка (размер чанка указывается дополнительным свойством в настройках драйвера tableParamChunkSize, например tableParamChunkSize =100KB);
  + EVEN\_ROWS – запрещает разбиение информации между чанками (автономно десериализуемые чанки), не гарантируется соблюдение размера чанка.

### 3.3.8 Настройка организации информационного обмена через API Gateway (опционально)

Настройка информационного обмена через API Gateway для выполнения запросов к REST-сервису ИС Поставщика.

Все шаги опциональны, но если требуется настройка, то:

* + шаги 1-4 выполняются в рамках организации информационного обмена через API Gateway **по HTTPS**;
  + шаг 5 только для Агента Поставщика/ответчика;
  + шаг 6 только для Агента Потребителя/инициатора запроса.

1. Скопировать файл cacerts java в локальный каталог (java должна быть установлена, см. [Раздел 4.2.2](#_4.2.2_Предварительные_операции))

cp /distr/einfahrt/jdk-17.0.7/lib/security/cacerts /distr/einfahrt/certs/cacerts

1. Произвести импорт сертификата в java cacerts. Пример раздела конфигурации:

keytool -importcert -keystore /distr/einfahrt/certs/cacerts -storepass changeit -alias api-gateway -file cert.crt

* + changeit - пароль по умолчанию для cacerts;
  + cert.crt – файл с сертификатом используемым на стороне HTTPS сервера.

1. В параметры запуска агента добавить ключи -Djavax.net.ssl.keyStore=certs/cacerts и -Djavax.net.ssl.trustStore=certs/cacerts. При использовании systemd ([Раздел 4.2.3](#_4.2.3_Запуск_Агента)) данные параметры добавить в описание Environment="JDK\_JAVA\_OPTIONS=….
2. Произвести настройку модуля для работы по HTTPS. Пример раздела конфигурации:

# Настройка модуля API gateway  
api-gateway:  
 # Параметры HTTP-клиента для отправки запросов на стороне поставщика  
 client:  
 impl: APACHE  
 options:  
 # указать адрес и порт https сервера  
 default-host: \*\*\* адрес подключения к серверу \*\*\*  
 default-port: \*\*\* адрес подключения к серверу \*\*\*  
 ssl: true  
 verifyHost: false  
 maxPoolSize: 100

1. При необходимости настройки таймаутов указать опциональные параметры (ниже приведены дефолтные значения, которые используются если параметры не указаны явно):

*# Настройка модуля API gateway*  
**api-gateway**:  
 *# Параметры HTTP-клиента для отправки запросов на стороне поставщика*  
 **client**:  
 **options**:  
 **connectTimeout**: 10000 *#таймаут подключения, мс*  
 **idleTimeout**: 60000 *#таймаут бездействия, мс*  
 **maxPoolSize**: 100 *#размер пула соединений*  
 **maxWaitQueueSize**: 0 *#0 - не ждать, возвращает инициатору ошибку 503(service unavailable)*  
 *#для impl=VERTX - число ожидающих запросов при исчерпании*  
 *#пула соединений (-1 - неограниченная очередь),*  
 *#для impl=APACHE - таймаут ожидания соединения*  
 *#при исчерпании пула (-1 - неограниченное время*  
 *#ожидания), мс*

1. При необходимости изменения порта, используемого ИС Потребителя при обращении к Агенту СМЭВ4 по Регламентированным REST-запросам требуется указать значения следующих параметров:
   * при использовании транспорта pulsar (по умолчанию 8171):

*# Настройка модуля API gateway*  
**api-gateway**:  
 *# Параметры HTTP-сервера для приёма запросов на стороне потребителя (транспорт pulsar)*  
 **server**:  
 **port**: 8171

* + при использовании транспорта rsocket (по умолчанию 8172).

|  |
| --- |
| Внимание: |
| Версия Агента СМЭВ4 должна быть 3.8.0 или выше как у инициатора обмена, так и у ответчика |

*# Настройка модуля API gateway*  
**api-gateway**:  
 *# Параметры HTTP-сервера для приёма запросов на стороне потребителя (транспорт rsocket)*  
 **target-arch**:  
 **server-port**: 8172

### 3.3.9 Настройка параметров времени активации Агента СМЭВ4 (опционально)

Данные параметры применяются для обеспечения обновления масштабированного Агента СМЭВ4 с нулевым временем простоя.

В примере ниже указаны значения по умолчанию.

**agent-activation**:  
 *# Таймаут ожидания активации экземпляра Агента при получении запроса*  
 **component-activation-timeout**: 1s  
 *# Код ошибки HTTP при попытке выполнения SQL запроса на неактивированном экземпляре агента*  
 **inactive-query-http-error-code**: 501  
 *# Код ошибки HTTP при попытке выполнения APIGateway запроса на неактивированном экземпляре агента*  
 **inactive-api-gw-http-error-code**: 501

При последовательном обновлении экземпляров масштабированного Агента СМЭВ4 до новой мажорной версии, экземпляр Агента СМЭВ4 с новой версией не будет активирован до момента обновления других экземпляров.

Выполнение запроса к не активированному экземпляру Агента СМЭВ4 приведет к ошибке (коды ошибок в соответствии с примером конфигурации выше), в таком случае система - инициатор запроса должна перенаправить запрос на другой экземпляр Агента СМЭВ4.

### 3.3.10 Настройка подключения к масштабированному Агенту СМЭВ4 (опционально)

|  |
| --- |
| Внимание: |
| Масштабирование поддерживается для Агента Инициатора (Потребителя) при использовании любого из транспортов (Pulsar, RSocket). Для Агента Ответчика (Поставщика), т.е. в случае подключённой к Агенту Витрины, масштабирование Агента СМЭВ4 поддерживается только при использовании транспорта RSocket, в случае использования транспорта Pulsar Агент СМЭВ4 должен работать строго в одном экземпляре. |

1. Указать URL подключения к агентам.

Для масштабированного агента-потребителя(поставщика), пример раздела конфигурации:

*# Настройки REST сервера исполнения SQL запросов*  
**rest-query-endpoint**:  
 *# URL подключения к агентам по JDBC (только для implementation = JDBC)*  
 **jdbc-url**: jdbc:podd://<instance-1-ip-address>:${query-server.port},<instance-2-ip-address>:${query-server.port},<instance-N-ip-address>:${query-server.port}

где, <instance-\*-ip-address> - адреса всех экземпляров масштабированного агента.

Для немасштабированного Агента Потребителя, а также для Агента Поставщика, можно указать значение jdbc:podd://localhost:${query-server.port}.

1. Указать идентификатор экземпляра Агента СМЭВ4. В случае использования масштабируемого Агента ПОДД, значение параметра должно быть уникальным для каждого экземпляра Агента СМЭВ4.

Пример раздела конфигурации:

*# Настройки модуля "информация об агенте"*  
**agent-info**:  
 *# идентификатор экземпляра агента (HOSTNAME используется только при запуске под kubernetes, в остальных случаях следует использовать уникальные идентификаторы)*  
 **instanceId**: ${HOSTNAME:instance-1}

В случае запуска под **Kubernetes** с помощью **Helm chart**, данный параметр будет подставлен автоматически.

### 3.3.11 Настройка подключения к NTP

*Предоставляемый шаблон конфигурационного файла имеет настройку по умолчанию для данного параметра. Применять изменения следует только в случае, если значения по умолчанию не подходят для данного Агента СМЭВ4.*

В данном разделе необходимо указать IP адрес или HOSTNAME NTP сервера.

**ntp**:  
- **host**: {{ IP адрес или HOSTNAME NTP }}

В случае, если используется поставляемый в комплекте с Агентом СМЭВ4 пакет chrony, в данном параметре конфигурационного файла Агента СМЭВ4 следует указать ip адрес, на котором работает chrony.

### 3.3.12 Настройка типа аутентификации агента в ядре

Для получения токена Агентом СМЭВ4, позволяющим взаимодействовать с Ядром ПОДД СМЭВ, необходимо произвести настройку описанную ниже. В зависимости от использования либо неиспользования mTLS, должен быть выбран один из возможных способов аутентификации агента в ядре ([Раздел 2.2.2](#_2.2.2_СКЗИ_для))

**pulsar**:  
 **auth**:  
 **keycloak-oauth**:  
 *# Способ аутентификации в Keycloak:*  
 *# - TLS\_PUB\_KEY - проверка агента на сервере аутентификации выполняется по открытому ключу получаемому*  
 *# из сертификата используемого агентом при Mutual-TLS*  
 *# - SIGNED\_JWT - аутентификация через проверку подписи переданного агентом JWT, при данном способе*  
 *# использование Mutual-TLS опционально*  
 **auth-type**: SIGNED\_JWT  
 *# Протокол подключения*  
 *# - GOST\_TLS - Mutual-TLS по ГОСТ алгоритмам, с использованием ключа КриптоПро*  
 *# - PLAIN\_HTTP - обычный HTTP/HTTPS*  
 **auth-protocol**: GOST\_TLS

Значения по умолчанию: SIGNED\_JWT и GOST\_TLS

# 4 Настройка и запуск Агента СМЭВ4

## 4.1 Порядок загрузки данных и программ

Администратор УВ осуществляет развёртывание, запуск и настройку Агента СМЭВ4 с помощью данного руководства.

## 4.2 Подготовка и настройка системы для запуска Агента СМЭВ4 без использования docker

### 4.2.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Агента СМЭВ4 (/distr/einfahrt):

* + /distr/einfahrt/app/app.jar – исполняемый файл;
  + /distr/einfahrt/csp-5.0.11455.tar.gz – дистрибутив CryptoPro CSP;
  + /distr/einfahrt/java-csp-5.0.42119-A.zip – дистрибутив CryptoPro JСSP;
  + /distr/einfahrt/bellsoft-jdk17.0.7-linux-amd64.tar.gz – дистрибутив Java.

Путь /distr/einfahrt указан в качестве примера. Есть возможность использовать любой другой путь, скорректировав соответствующим образом упоминаемые ниже команды.

### 4.2.2 Предварительные операции (установка «пре-реквизитов»)

Перед запуском Агента СМЭВ4 выполнить от имени пользователя **root** либо используя команду sudo следующие действия:

1. Создать пользователя {{user}} и группу {{user\_group}}, под которым будет работать Агент СМЭВ4.
2. Установить java

cd /distr/einfahrt  
tar zxvf bellsoft-jdk17.0.7-linux-amd64.tar.gz

1. Установить системные переменные

export JAVA\_HOME=/distr/einfahrt/jdk-17.0.7  
export PATH=$PATH:$JAVA\_HOME/bin

Переменные должны устанавливаться автоматически также после перезагрузки сервера. Для этого рекомендуется внести данную настройку в **profile** пользователя либо в настройки ОС.

1. Установить пакет java-csp-5.0.42119-A:

cd /distr/einfahrt  
mkdir -p /distr/einfahrt/cryptopro  
unzip java-csp-5.0.42119-A.zip  
cd java-csp-5.0.42119-A  
./configure.sh  
cp -f \*.jar /distr/einfahrt/cryptopro/  
cd /distr/einfahrt  
rm -rf java-csp-5.0.42119-A

При наличии лицензионного кода CryptoPro JCP выполнить от имени пользователя {{user}} команду.

java -cp :/distr/einfahrt/cryptopro/\* ru.CryptoPro.JCP.tools.License -serial "{{ jcp\_serial }}" -store

В случае отсутствия лицензионного кода, CryptoPro JCP будет работать в режиме trial лицензии.

|  |
| --- |
| Внимание: |
| Срок действия trial лицензии – 90 дней с момента установки CryptoPro JCP. Для сохранения работоспособности Агента СМЭВ4 по окончании данного периода вам необходимо приобрести лицензию на CryptoPro JCP и внести её в систему как указано выше. |

1. Установить CryptoPro CSP:

cd /distr/einfahrt  
tar xzvf csp-5.0.11455.tar.gz  
rm -f csp-5.0.11455.tar.gz  
cd csp-5.0.11455 yum -y install lsb-cprocsp-base\*.rpm lsb-cprocsp-rdr-64\*.rpm lsb-cprocsp-kc1-64\*.rpm lsb-cprocsp-capilite-64\*.rpm lsb-cprocsp-devel\*.rpm lsb-cprocsp-kc2-64\*.rpm cprocsp-curl-64\*.rpm  
./install.sh  
cd ..

При наличии лицензионного кода CryptoPro CSP выполнить команду:

sudo /opt/cprocsp/sbin/amd64/cpconfig -license -set {{cprocsp\_license\_code}}

В случае отсутствия лицензионного кода, CryptoPro CSP будет работать в режиме trial лицензии.

|  |
| --- |
| Внимание: |
| Срок действия trial лицензии – 90 дней с момента установки CryptoPro CSP. Для сохранения работоспособности Агента СМЭВ4 по окончании данного периода, вам необходимо приобрести лицензию на CryptoPro CSP и внести её в систему как указано выше. |

1. Установить контейнер ключа CryptoPro в директорию /var/opt/cprocsp/keys/{{user}}/. Пользователь {{user}} должен быть владельцем данной директории и файлов в ней.
2. Для установки TLS соединения, который использует алгоритмы в соответствии с ГОСТ-2012, требуется использовать доверенное хранилище с корневыми сертификатами удостоверяющих центров (УЦ), которое находится в дистрибутиве (файл cp\_ca\_store).

|  |
| --- |
| Внимание: |
| Ключ CryptoPro должен содержать цепочку сертификатов промежуточных УЦ (кроме корневого). [Раздел 9](#_ec6a6ad768199c10ab1736d1a17ed224) настоящего документа содержит сведения о добавлении промежуточных сертификатов в ключ. |

1. Выложить в каталог /distr/enfahrt конфигурационный файл application.yml, подготовленный согласно [Разделу 3](#_3_Описание_конфигурационного).
2. В файл /etc/hosts добавить следующие записи:

172.20.59.5 podd.gosuslugi.ru  
172.20.59.5 podd-cross.gosuslugi.ru  
109.207.15.26 podd1.gosuslugi.ru  
109.207.15.58 podd2.gosuslugi.ru  
109.207.15.154 podd3.gosuslugi.ru  
109.207.15.186 podd4.gosuslugi.ru  
109.207.15.26 podd1-cross.gosuslugi.ru  
109.207.15.58 podd2-cross.gosuslugi.ru  
109.207.15.154 podd3-cross.gosuslugi.ru  
109.207.15.186 podd4-cross.gosuslugi.ru

### 4.2.3 Запуск Агента СМЭВ4

Убедитесь, что пользователь {{user}} имеет доступ к директории, в которой установлен Агент СМЭВ4 (/distr/einfahrt).

Пример раздела конфигурации скрипта для запуска Агента СМЭВ4 с использованием сервиса **systemd**:

[Unit]  
Description="Service for einfahrt"  
After=syslog.target  
  
[Service]  
Type=simple  
  
WorkingDirectory=/distr/einfahrt  
LimitNOFILE=1048576:1048576  
  
*# Важно! Запуск должен производиться от имени того пользователя, для которого ранее были выложены ключи КриптоПро!*  
User={{user}}  
Group={{user\_group}}  
  
Environment="JAVA\_HOME=/distr/einfahrt/jdk-17.0.7"  
Environment="JDK\_JAVA\_OPTIONS=--add-exports=java.base/sun.security.util=ALL-UNNAMED \  
 --add-exports=java.base/sun.security.x509=ALL-UNNAMED \  
 --add-exports=java.base/sun.security.pkcs=ALL-UNNAMED \  
 --add-exports=java.base/sun.security.provider=ALL-UNNAMED \  
 --add-exports=java.base/sun.security.tools.keytool=ALL-UNNAMED \  
 --add-exports=java.base/sun.net=ALL-UNNAMED \  
 --add-opens=java.base/jdk.internal.misc=ALL-UNNAMED \  
 --add-opens=java.base/java.lang=ALL-UNNAMED \  
 --add-opens=java.base/java.nio=ALL-UNNAMED \  
 --add-opens=java.xml/org.w3c.dom=ALL-UNNAMED \  
 --add-opens=java.base/java.util=ALL-UNNAMED \  
 -Dio.netty.tryReflectionSetAccessible=true \  
 -Dsaffron.default.charset=UTF-16LE \  
 -Dsaffron.default.collation.name='UTF-16LE$en\_US' \  
 -Dsaffron.default.nationalcharset=UTF-16LE \  
 -XX:MaxRAMPercentage=80.0"  
ExecStart=/distr/einfahrt/jdk-17.0.7/bin/java -cp app/\*:cryptopro/\* -jar app/app.jar  
  
[Install]  
WantedBy=multi-user.target

Соответствующий файл скрипта, для примера с названием einfahrt.service, необходимо сохранить в каталог /etc/systemd/system/.

Далее выполнить команды по включению, запуску сервиса и проверке его статуса:

sudo systemctl daemon-reload  
sudo systemctl enable einfahrt  
sudo systemctl start einfahrt  
sudo systemctl -l status einfahrt

### 4.2.4 Настройка ротации логов (опционально)

Во избежание переполнения диска лог-файлами, рекомендуется настроить ротацию лог-файлов **systemd** сервиса.

Настройка логирования осуществляется с помощью файлов конфигурации **logrotate** и **systemd** сервиса. Если этих файлов не существует, их необходимо создать. Первоначально необходимо установить пакет **logrotate**, для rpm-base дистрибутивов необходимо выполнить команду:

sudo yum install logrotate

Добавьте в файл **systemd** сервиса (/etc/systemd/system/einfahrt.service) следующие настройки логирования:

...  
[Service]  
Type=simple  
  
StandardOutput=append:/var/log/{{ file\_name }}  
StandardError=append:/var/log/{{ file\_name }}  
  
...

Создайте файл конфигурации **logrorate** /etc/logrotate.cron/einfahrt.conf и поместите в него следующее содержимое:

/var/log/{{ file\_name }} {  
 rotate {{ rotate }}  
 size {{ file\_size }}  
 create  
 nocompress  
 copytruncate  
}

где:

* + rotate – какое количество лог файлов оставлять,
  + file\_size – размер лог-файла при котором будет происходить ротация.

Создайте файл с скриптом запуска утилиты **logrotate**, поместите скрипт по пути /etc/logrotate.cron/einfahrt.sh

*#!/bin/bash*  
/usr/sbin/logrotate /etc/logrotate.cron/einfahrt.conf

Добавьте права на запуск командой:

chmod +x /etc/logrotate.cron/einfahrt.sh

Создайте правила cron, создайте файл /etc/cron.d/einfahrt и поместите в него содержимое ниже:

\*/1 \* \* \* \* root /etc/logrotate.cron/einfahrt\_logrotate.sh

Далее перезагрузите **systemd** сервис:

sudo systemctl daemon-reload  
sudo systemctl restart einfahrt

## 4.3 Настройка и запуск Агента СМЭВ4 с использованием docker

### 4.3.1 Предварительные условия

1. На сервере должен быть установлен docker версии не ниже 20.10.12.
2. Создан пользователь, который будет запускать Агент СМЭВ4.
3. Этот пользователь должен иметь права на загрузку докер-образов и запуск/остановку контейнеров (т.е. добавлен в группу docker).

### 4.3.2 Настройка ротации лог-файлов в docker (опционально)

Во избежание переполнения диска лог-файлами, рекомендуется настроить ротацию лог-файлов контейнеров в docker.

Настройка логирования в Docker осуществляется с помощью файла конфигурации /etc/docker/daemon.json. Если этого файла не существует, его необходимо создать. Добавьте в файл следующие настройки логирования:

{  
**"log-opts"**: {  
 **"max-file"**: "3",  
 **"max-size"**: "100m"  
 }  
}

где:

* + max-file – ограничение по количеству файлов (настройки ротации). Максимальное количество файлов журнала, которые могут быть созданы. При превышении количества самый старый файл удаляется. Действует только при установленном параметре max-size. Положительное целое число. По умолчанию 1;
  + max-size – устанавливает ограничение по размеру лог-файла (k, m или g). По умолчанию -1 (не ограничено).

### 4.3.3 Состав и содержание дистрибутивного пакета

Ниже приведён состав дистрибутива Агента СМЭВ4 для docker.

/distr/einfahrt – Агент СМЭВ4:

* + /distr/einfahrt/image.tgz – docker image для загрузки в систему. Включает в себя также все необходимые версии CryptoPro;
  + /distr/einfahrt/run\_agent.sh – скрипт для запуска и перезапуска агента;
  + /distr/einfahrt/stop.sh – скрипт для остановки агента;
  + /distr/einfahrt/log\_save.sh – скрипт для сохранения лога агента в файл;
  + /distr/einfahrt/log.sh – скрипт для просмотра лога агента в реальном времени;
  + /distr/einfahrt/diag.sh – скрипт для сбора диагностической информации при обращении в службу поддержки.

Путь /distr/einfahrt использован для примера, не является фиксированным и может быть изменен на любой другой по желанию пользователя, с соответствующим внесением корректировок при его упоминаниях ниже.

Ниже в качестве примера будет использоваться данный путь.

### 4.3.4 Подготовка к запуску

Для запуска Агента СМЭВ4 необходимо после распаковки пакета сформировать конфигурационный файл application.yml, как указано в [Разделе 3.3](#_3.3_Формирование_конфигурационного) , и выложить его в каталог /distr/einfahrt.

|  |
| --- |
| Внимание: |
| При использовании скрипта из пакета поставки для запуска Агента параметр trust-store.path в конфигурационном файле необходимо задать строго /egov/java/certs/cp\_ca\_store. |

Пример:

trust-store:  
 path: /egov/java/certs/cp\_ca\_store  
 password: \*\*\* ПАРОЛЬ К TRUST STORE \*\*\*

где:

* + path – фактический путь к файлу cp\_ca\_store из дистрибутива (в данном примере – /distr/einfahrt/certs/cp\_ca\_store);
  + password – пароль от cp\_ca\_store.

В каталоге /distr/einfahrt:

* + создать подкаталог keys, выложить в него полученный ключ CryptoPro **в распакованном виде** ;
  + создать подкаталог certs, выложить в него файл cp\_ca\_store из пакета поставки;
  + (только при использовании **HTTPS** API gateway) подготовить файл cacerts согласно [Разделу 3.3.8](#_3.3.8_Настройка_организации), сформированный файл выложить в каталог /distr/einfahrt/certs.
  + выложить файл postgresql.json из пакета поставки;

При наличии файла расширенных настроек логирования customLogLevels.xml выложить его в каталог /distr/einfahrt.

Для запуска Агента СМЭВ4 под docker полученный docker образ необходимо загрузить в локально установленный docker на машине, где будет работать Агент СМЭВ4.

Для этого необходимо выложить архив с образом на локальный диск этой машины и выполнить команду:

docker load < image.tgz

где image.tgz – имя полученного архива с docker image Агента СМЭВ4 из пакета поставки.

Загрузка должна завершиться без ошибок.

Проверить успешность загрузки можно командой:

docker images | grep einfahrt

Вывод будет содержать информацию вида:

einfahrt latest c7511824117e 5 days ago 1.2G

### 4.3.5 Запуск Агента СМЭВ4

Для запуска Агента СМЭВ4 используется скрипт run\_agent.sh, входящий в пакет поставки. Скрипт не требует указания параметров. При выполнении всех шагов, перечисленных в [Разделе 4.3.4](#_4.3.4_Подготовка_к), Агент СМЭВ4 будет успешно запущен, с сообщением о доступных портах. При повторном выполнении скрипта контейнер будет остановлен и запущен заново.

Для сохранения лога Агента СМЭВ4 в файл, запустите скрипт log-save.sh. Лог будет сохранен в файле log-дата-время.txt.

Для просмотра лога в режиме реального времени запустите скрипт log.sh.

В случае необходимости сбора диагностической информации для отправки в службу поддержки запустите скрипт diag.sh.

Остановка контейнера осуществляется скриптом stop.sh.

|  |
| --- |
| Примечание: |
| В ряде случаев может наблюдаться остановка контейнера через несколько секунд после запуска, с сообщением в логе java.lang.IllegalStateException: Ошибка вызова функции acquireContext: 0x8009001a. В этом случае следует изменить владельца каталога keys и вложенных подкаталогов и файлов на пользователя с id=1000 (потребуются root права): chown -R 1000 keys после чего повторить выполнение скрипта запуска контейнера. |

### 4.3.6 Информация по лицензированию CryptoPro

Входящие в поставку версии CryptoPro не имеют предустановленной лицензии, и могут работать как trial в течение трех месяцев с момента создания образа (не с момента первого запуска!)

**Для использования trial версии CryptoPro не требуется каких-либо дополнительных действий, касающихся лицензирования.**

В случае, если у Вас есть полная лицензия на CryptoPro CSP и CryptoPro JCP, предусмотрена возможность передачи номеров лицензий CSP и JCP при запуске контейнера, при передаче валидных лицензий соответствующие компоненты CryptoPro будут лицензированы на этапе запуска.

Для этого необходимо, чтобы текстовый файл, содержащий сроку с лицензией на CryptoPro CSP, был при запуске контейнера доступен внутри контейнера по пути /egov/csp.lic. Аналогично, лицензия для CryptoPro JCP должна быть доступна внутри контейнера в текстовом файле /egov/jcp.lic.

При запуске под docker-ом можно для этого монтировать внешние файлы, содержащие номера лицензий, по указанным выше путям.

Для того, чтобы прилагаемый скрипт запуска применил лицензии CryptoPro, при их наличии, их необходимо поместить в текстовые файлы licenses/jcp.txt и licenses/csp.txt соответственно. При отсутствии лицензии и использовании trial версий CryptoPRO не создавайте указанные файлы.

|  |
| --- |
| Внимание: |
| Срок действия trial лицензии – 90 дней с момента создания docker image используемого Вами Агента. Для сохранения работоспособности Агента СМЭВ4 по окончании данного периода необходимо приобрести лицензии на CryptoPro CSP и JCP и внести их в систему, как указано выше. |

## 4.4 Настройка предустановленного профиля Витрины в Агенте СМЭВ4

Раздел применим только при использовании Витрины и заданной настройке использования предустановленного профиля Витрины в Агенте СМЭВ4 (см. [Раздел 3.3.3](#_3.3.3_Настройка_регистрации)).

*Файл профиля имеет настройки по умолчанию. Вносить изменения следует только в том случае, если значения по умолчанию не подходят для данной Витрины.*

Настройки задаются после установки Агента ПОДД в файле postgresql.json, расположенном в директории:

1. при установке без использования docker (см. [Раздел 4.2](#_4.2_Подготовка_и)): /директория\_установленного\_Агента\_СМЭВ4/postgresql.json. По умолчанию /distr/einfahrt/postgresql.json

1. при установке с использованием docker (см. [Раздел 4.3](#_4.3_Настройка_и)): /egov/java/postgresql.json

Пример предустановленного профиля Витрины в Агенте ПОДД:

{  
 "sqlDialect": "POSTGRESQL",  
 "parameterNotionType": "QUESTION",  
 "aggFunctions": [  
 ...  
 ],  
 "otherFunctions": [  
 ...  
 ],  
 "forSystemTimeParameterSupport": false,  
 "subQueryParamSupport": "DYNAMIC\_PARAM\_SUPPORT"  
}

где:

1. subQueryParamSupport – способ передачи подзапроса при выполнении РЗ с параметрами на сторону Витрины, возможные значения:
   * NOT\_SUPPORTED - отправка подзапроса с параметрами, подставленными в SQL-выражение;
   * DYNAMIC\_PARAM\_SUPPORT - отправка подзапроса с блоком динамических параметров, подстановка осуществляется на стороне Адаптера Витрины;
   * NAMED\_PARAM\_SUPPORT - отправка подзапроса с блоком именованных параметров, подстановка осуществляется на стороне Адаптера Витрины.
2. forSystemTimeParameterSupport – поддержка системного параметра РЗ для запроса ак-туальных на заданный момент времени данных из Витрины:
   * false - Адаптер Витрины не поддерживает обработку параметра;
   * true - Адаптер Витрины поддерживает обработку параметра.

## 4.5 Настройка сбора метрик Агента СМЭВ4 (опционально)

### 4.5.1 Настройка Агента СМЭВ4 для передачи метрик в Prometheus

Агент поддерживает возможность передачи метрик работы во внешнюю систему сбора метрик **Prometheus**.

Для включения возможности передачи необходимо добавить в конфигурационный файл следующие параметры:

**metrics**:  
 **implementation**: PROMETHEUS  
 *# порт, при обращении к которому Агент отдаёт значения метрик*  
 **endpointPort**: 8381

**Prometheus** следует настроить на опрос адреса, на котором запущен Агент СМЭВ4, по указанному порту.

При запуске Агента под docker также необходимо добавить указанный порт в список **expose ports** в скрипте запуска Агента.

Полный список метрик приведен в [Приложении B "Список метрик Агента СМЭВ4"](#_10_Приложение_B).

# 5 Настройка и запуск NTP сервера

## 5.1 Порядок загрузки данных и программ

Администратор УВ осуществляет развёртывание, запуск и настройку NTP сервиса с помощью данного руководства.

## 5.2 Настройка и запуск NTP сервиса БЕЗ использования docker

### 5.2.1 Состав и содержание дистрибутивного пакета

* + /distr/chrony/chrony.rpm – установочный пакет для ОС CentOS 7.x;
  + /distr/common/einfahrt-chrony.service — unit для systemd;
  + /distr/config/prodConfig.conf – конфигурационный файл для использования в ПРОД среде;
  + /distr/config/testConfig.conf – конфигурационный файл для использования в ТЕСТ среде.

Путь /distr/ указан в качестве примера.

Есть возможность использовать любой другой путь, скорректировав соответствующим образом упоминаемые ниже команды.

### 5.2.2 Предварительные операции (установка «пре-реквизитов»)

Перед запуском NTP сервиса выполнить следующие действия:

1. Установить пакет с сервисом chrony:

sudo cd /distr/chrony  
sudo yum install chrony.rpm

1. Скопировать конфигурационный файл в /etc/chrony.conf:

sudo cp /distr/config/{{ stand }}Config.conf /etc/einfahrt-chrony.conf

где {{ stand }} – название среды, к которой подключается агент (prod/test)

### 5.2.3 Запуск NTP сервиса

Файл системного сервиса /distr/common/einfahrt-chrony.service необходимо положить в каталог /etc/systemd/system/ (потребуются root права)

Далее выполнить команды по включению, запуску сервиса и проверке его статуса:

sudo systemctl daemon-reload  
sudo systemctl enable einfahrt-chrony  
sudo systemctl start einfahrt-chrony  
sudo systemctl -l status einfahrt-chrony

## 5.3 Настройка и запуск NTP сервиса с использованием docker

### 5.3.1 Предварительные условия

1. На сервере должен быть установлен docker версии не ниже 20.10.12.
2. Создан пользователь, который будет запускать NTP сервис.
3. Этот пользователь должен иметь права на загрузку докер-образов и запуск/остановку контейнеров (т.е. добавлен в группу docker).

### 5.3.2 Состав и содержание дистрибутивного пакета

Ниже приведён состав дистрибутива NTP сервиса для docker.

* + /distr/chrony/chrony.tgz – docker image для загрузки в систему;
  + /distr/scripts/run\_chrony.sh – скрипт для запуска и перезапуска NTP сервиса;
  + /distr/scripts/stop.sh – скрипт для остановки NTP сервиса;

Путь /distr/chrony использован для примера, не является фиксированным и может быть изменен на любой другой по желанию пользователя, с соответствующим внесением корректировок при его упоминаниях ниже. Ниже, в качестве примера, будет использоваться данный путь.

### 5.3.3 Подготовка к запуску

Для запуска NTP сервиса под docker полученный docker образ необходимо загрузить в локально установленный docker на машине, где будет работать NTP. Для этого необходимо выложить архив с образом на локальный диск этой машины и выполнить команду:

cd /distr/chrony  
docker load < chrony.tgz

где chrony.tgz – имя полученного архива с docker image Агента ПОДД из пакета поставки.

Загрузка должна завершиться без ошибок.

Проверить успешность загрузки можно командой:

docker images | grep einfahrt-chrony

Вывод будет содержать информацию вида:

einfahrt-chrony latest c7511824117e 5 days ago 13MB

### 5.3.4 Запуск NTP

Для запуска NTP сервиса используется скрипт run\_chrony.sh (предварительно раскомментировать нужную строку с NTP серверами для используемой среды prod/test), входящий в пакет поставки.

Скрипт не требует указания параметров.

При выполнении всех шагов, перечисленных в [Разделе 5.3.3](#_5.3.3_Подготовка_к), NTP сервис будет успешно запущен, с сообщением о доступных портах.

При повторном выполнении скрипта контейнер будет остановлен и запущен заново.

Остановка контейнера осуществляется скриптом stop.sh.

# 6 Типовые вопросы и проблемы

Также сведения о типовых ошибках приведены на [портале ЕСКС](https://info.gosuslugi.ru/articles/Типовые_ошибки_Агента_СМЭВ4/).

Таблица 6.1 Типовые вопросы и проблемы

| № | Вопрос/Проблема | Возможная причина |
| --- | --- | --- |
| 1 | Как скачать актуальный JDBC драйвер? | 1. Драйвер можно получить по адресу http://<ваш\_хост>:8192/api/v1/jdbc-driver. |
| 2 | Как проверить соединение Агента СМЭВ4 с Ядром ПОДД СМЭВ? | 1. Воспользуйтесь запросом «SELECT 1». 2. Воспользуйтесь командой для проверки через REST с использованием утилиты curl:   curl -X POST -H "Accept-Version:1" -H "Content-Type: application/json" -d '{"sql": {"sql": "select 1"}}' |
| 3 | В лог-файле присутствует ошибка:  «Ошибка вызова функции acquireContext: 0x80090016» | 1. При запуске Агента СМЭВ4 без использования docker убедитесь, что контейнер с ключами выложен в /var/opt/cprocsp/keys/{{user}}/  * пользователь {{user}} имеет доступ на чтение к /var/opt/cprocsp/keys/{{user}}/.  1. Убедитесь, что Агент СМЭВ4 запускается от пользователя {{user}}.   При использовании docker убедитесь, что при запуске указан ключ --user=1000. |
| 4 | В лог-файле присутствует ошибка  «Ошибка вызова функции acquireContext: 0x8009001a» | 1. При использовании docker, установите владельца id=1000 на каталог keys рекурсивно chown -R 1000 keys. 2. При запуске без использования docker, сделайте пользователя {{user}} владельцем каталога /var/opt/cprocsp/keys/{{user}}/ рекурсивно. 3. При запуске без использования docker на платформе CentOS/RedOS, убедитесь что SELinux находится в режиме permissive или diasbled. |
| 5 | В логе присутствуют сообщения «No such provider: JCP» | Убедитесь, что CryptoPro JCP и CryptoPro CSP установлены корректно (согласно данного руководства),  а также путь к jar файлам СryptoPro JCP присутствует в classpath при запуске java. |
| 6 | В логе присутствуют сообщения «No required SSL certificate was sent» | 1. Убедитесь, что используется верный ключ. 2. Убедитесь, что указан корректный адрес {{ gost\_nlb }}. 3. Убедитесь, что используется cp\_ca\_store, содержащий необходимые цепочки для подключения к используемому Ядру ПОДД. |
| 7 | При выполнении запроса, запрос не проходит, в логе агента появляются сообщения  «java.lang.IllegalStateException: Ошибка вызова функции signHash: 0x65b» | Используемая trial лицензия CryptoPro истекла.  Необходимо приобрести лицензии на CryptoPro CSP и JCP и внести информацию о них в систему, как описано в [Разделе 4.3.6](#_4.3.6_Информация_по) настоящего документа |
| 8 | Агент не подключается к Ядру, сообщения об ошибке в логах содержат текст «invalid\_client\_credentials» | 1. Убедитесь, что используется корректный ключ CryptoPro, соответствующий данной информационной системе. 2. Убедитесь, что мнемоника Агента СМЭВ4 в конфигурационном файле указана корректно. Параметр agent.id   **Регистр учитывается!** Например, «agentMnemonic» и «agentmnemonic» - две различные мнемоники.   1. Обратитесь в службу поддержки для проверки корректности сертификата данного Агента СМЭВ4, загруженного в Ядро ПОДД СМЭВ.   У вас будут запрошены дополнительные данные о подключении, необходимо будет их предоставить согласно инструкции от службы поддержки. |

# 7 Термины и определения

| Термин | Определение |
| --- | --- |
| Агент ПОДД СМЭВ, также Экземпляр ПО Агент (ПОДД СМЭВ) | Экземпляр ПО «Агент (ПОДД СМЭВ)», установленный в контуре ИС УВ и обеспечивающее сопряжение Экземпляров ПО «Витрина данных» и ИС УВ с Ядром ПОДД СМЭВ |
| Витрина (данных), также: Экземпляр ПО «Витрина данных» | Комплекс программных и технических средств в составе информационно-телекоммуникационной инфраструктуры участника взаимодействия, обеспечивающий хранение и предоставление данных другим участникам взаимодействия в соответствии с критериями, установленными Министерством цифрового развития, связи и массовых коммуникаций |
| ГБ | Гигабайт |
| ГОСТ-2012 | ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» |
| Запрос к REST-сервису ИС Ответчика (Регламентированный REST-запрос) | Регламентированный запрос, представляющий из себя REST-сервис в инфраструктуре Ответчика, обеспечивающий предоставление данных другим Участникам взаимодействия с использованием ПОДД СМЭВ в соответствии с загруженной в ПОДД СМЭВ спецификацией OpenAPI |
| Инициатор (запроса) | Участник взаимодействия, который формирует исходный запрос к REST-сервису ИС Ответчика для передачи через ПОДД СМЭВ и может являться источником данных |
| ИС | Информационная система |
| ИЭП | Инфраструктура электронного правительства |
| КСЗ | Комплекс средств защиты |
| МинЦифры | Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации |
| Мнемоника | Короткое символическое имя объектов модели данных (Витрин, сущностей, атрибутов) для использования в Запросах. Имеет более строгие правила формирования, чем наименования объектов (нельзя использовать пробелы, специальные символы и т. д.), что облегчает чтение Запросов человеком и позволяет изменять наименования объектов без влияния на работоспособность систем Потребителей |
| Мнемоника Витрины | Уникальное строковое значение, однозначно определяющее Витину данных |
| НСУД | Национальная система управления данными |
| ОС | Операционная система |
| Ответчик | Участник взаимодействия, на стороне которого развернут REST-сервис ИС Ответчика и который является получателем запроса |
| ПОДД | Подсистема обеспечения доступа к данным |
| ПОДД СМЭВ | Подсистема обеспечения доступа к данным — подсистема СМЭВ, предназначенная для обеспечения взаимодействия СМЭВ с Витринами данных |
| Подзапрос (данных) | SQL-запрос, который отправляется Ядром ПОДД СМЭВ в адрес Поставщика данных |
| Поставщик (данных ПОДД) | Участник взаимодействия, являющийся источником данных для других участников и использующий ПОДД СМЭВ для передачи данных |
| Потребитель (данных ПОДД) | Участник взаимодействия, получающий данные от Поставщиков данных для дальнейшей их обработки и использующий для передачи запросов и получения данных ПОДД СМЭВ |
| Регламентированный SQL-запрос (РЗ) | SQL-запрос, выраженный в терминах Модели данных, загруженной в ПОДД, и зарегистрированный в Ядре ПОДД под символической мнемоникой, используемой ИС Потребителя ПОДД для выполнения регламентированного запроса. Может иметь параметры, значения которых задаются Потребителем данных ПОДД при выполнении регламентированного запроса |
| РЦОД | Резервный Центр обработки данных |
| СКЗИ | Средство криптографической защиты информации |
| СМЭВ | Единая система межведомственного электронного взаимодействия и Единая система нормативной справочной информации |
| СЦЛ | Система централизованного логирования |
| УВ | Участник взаимодействия – федеральный орган исполнительной власти, государственный внебюджетный фонд и иной орган или организация, участвующие в предоставлении государственных и муниципальных услуг (функций) |
| УЦ | Удостоверяющий центр |
| ФЦОД | Федеральный Центр обработки данных |
| ЦПУ | Центральное процессорное устройство |
| Ядро ПОДД СМЭВ | Централизованная часть ПОДД, предназначенная для маршрутизации запросов и контроля полномочий УВ |
| API | (англ. Application Programming Interface) — набор классов, процедур, функций, структур или констант, которыми одна компьютерная программа может взаимодействовать с другой программой |
| JDBC | (англ. Java DataBase Connectivity) — платформенно независимый промышленный стандарт взаимодействия Java-приложений с различными СУБД |
| JWT | (англ. JSON Web Token) — открытый стандарт (RFC 7519) для создания токенов доступа, основанный на формате JSON |
| OpenAPI, спецификация OpenAPI | Формализованная спецификация и экосистема множества инструментов, предоставляющая интерфейс между front-end системами, кодом библиотек низкого уровня и коммерческими решениями в виде API |
| REST | (англ. Representational State Transfer) — Архитектурный стиль взаимодействия компонентов распределённого приложения в сети |
| REST-сервис ИС Ответчика | Сервис в инфраструктуре Ответчика, зарегистрированный в ПОДД СМЭВ и обеспечивающий обмен данными с другими Участниками взаимодействия с использованием ПОДД СМЭВ в соответствии с загруженной в ПОДД СМЭВ спецификацией OpenAPI |
| SQL | (англ. Structured Query Language) — декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных |

# 8 История изменений документа

|  |
| --- |
| Примечание: |
| Изменения отражены начиная с версии 3.4.0. |

Таблица 8.1 История изменений документа

| Версия | Доработки | Изменения документа |
| --- | --- | --- |
| 3.4.0 | Task:   1. [PODD-5470] - Обеспечить поддержку времени жизни запроса (таймаут) 2. [PODD-5577] - Метрики по трафику APIGateway 3. [PODD-5646] - Метрики по трафику SQL запросов   BugFix:   1. [PODD-5551] - Blastoff подставляет некорректный адрес брокера в конфиг агента 2. [PODD-5639] - После падения и простоя агента потребителя упали подписки 3. [PODD-5634] - Некорректная остановка агентов 4. [PODD-5635] - Массовое логирование ошибок с уровнем ERROR 5. [PODD-5756] - Ошибка подписания больших печатных форм | 1. Скорректирована команда, используемая при установке CryptoPro JCSP при наличии лицензионного кода CryptoPro JCSP:  * [Раздел 4.2.2](#_4.2.2_Предварительные_операции)  1. Расширено описание решения типовых проблем для ошибки Ошибка вызова функции acquireContext: 0x8009001a:  * [Раздел 6](#_6_Типовые_вопросы)  1. Расширено описание настроек групп топиков при использовании нескольких схем Витрин данных  * [Раздел 3.3.3](#_3.3.3_Настройка_регистрации) |
| 3.5.0 | Task:   1. [PODD-5459] - Конфигурирование функций агента ПОДД 2. [PODD-5496] - [ЦА] Миграция Рассылок 3. [PODD-5604] - Обновить образ JDK: 17.0.6 4. [PODD-5649] - События СЦЛ для запроса Blob по ссылке 5. [PODD-5735] - Дедлайн должен срабатывать и при передаче результата 6. [PODD-5745] - Запрос BLOB по ссылке при взаимодействии ИС Потребителя с Агентом через REST-интерфейс 7. [PODD-5749] - События СЦЛ для РЗ типа «REST-сервис» (Api GW) 8. [PODD-5598] - Сквозная идентификация запросов 9. [PODD-5868] - События СЦЛ для обменов с РЗ типа «Рассылка»   Bugfix:   1. [PODD-5827] - Пересоздание агентом соединения до балансировщика 2. [PODD-5651] - ЦА. Ошибка при выполнении РЗ с ТП | 1. Расширено описание настроек создания топиков в разрезе видов обмена и добавлена информация о подключении пользовательских топиков:  * 3.3.3. Настройка регистрации Витрин данных и подключения к kafka (только при использовании Витрин) * 3.3.1. Общие настройки Агента СМЭВ4  1. Добавлено описание настроек логирования для запуска Агента без использования docker:  * 4.2.4. Настройка ротации логов (опционально)  1. Добавлена настройка передачи событий Витрины в СЦЛ при подключении только через Pulsar:  * 3.3.10. Настройка передачи событий Витрины в СЦЛ  1. Добавлена настройка автоматического скачивания БЛОБ по ссылке Агентом СМЭВ4 при выполнении запроса через REST-интерфейс:  * 3.3.6.1 Настройка автоматического скачивания БЛОБ по ссылке Агентом СМЭВ4 |
| 3.6.0 | Task:   1. [PODD-5721]- DEV::хранить в Зукипере максимальный таймаут запроса 2. [PODD-5781] - DEV:: События СЦЛ для асинхронного вызова SQL-запросов 3. [PODD-6212] - DEV События СЦЛ: почанковая передача объёма данных 4. [PODD-6256] - DEV: Удалить состояние в оперативной памяти на поставщике 5. [PODD-6408] - Переконфигурирование сервисов в рамках 3.6.0 6. [PODD-6025] - [DEV] Миграция произвольных запросов на ЦА 7. [PODD-5848] - Резервирование broker. Не выполняется подключение к брокеру на ЦОД2 при недоступности брокеров на ЦОД1 8. [PODD-5922] - При динамической регистрации витрин, не создаются топики при отправке запроса 9. [PODD-5965]- ЦА. Результат запроса, отмененного по таймауту, передается потребителю 10. [PODD-6015] - Сквозной идентификатор. РЗ получение блоба по ссылке. В логах clientRequestId не во всех сообщениях 11. [PODD-6460] - [ПОДД] - копящиеся клозвейты на агентах | 1. Обновлена версия агента 2. Внесены изменения в описание конфигурационного файла |
| 3.7.0 | 1. [PODD-6020] - [DEV] Миграция произвольных запросов на ЦА :: доработка Агента ПОДД 2. [PODD-6023]- [DEV] Миграция произвольных запросов на ЦА :: выбор группы и Агента ПОДД 3. [PODD-6431] - [DEV] Миграция произвольных запросов на ЦА :: strom, Этап 2 4. [PODD-6624] - DEV:: Логирование, метрики и аудит для Гостех 5. [PODD-6830] - DEV:: метрики по длине очереди сервисов ПОДД 6. [PODD-6414] - [3ЛП][ПОДД] - Корректировка отправленных события от ПОДД в СЦЛ 7. [PODD-6588] - ТПОДД: На ТПОДД завис репликатор | 1. Раздел 2.3: Обновлена таблица точек подключения к Агенту СМЭВ4 2. Раздел 3.2: Обновлена таблица реестра изменений файлов конфигурирования 3. Добавлен раздел 3.3.9 Настройка параметров времени активации Агента СМЭВ4 4. Обновлен раздел 3.3.10. Настройка подключения к Агентам ПОДД при использовании масштабированного Агента СМЭВ4, запускаемого более чем в одном экземпляре (опционально) 5. Обновлен раздел 4.5.1 Настройка Агента СМЭВ4 для передачи метрик в Prometheus 6. Обновлены версии Агента СМЭВ4 7. В приложение В обновлена таблица «Список метрик Агента СМЭВ4» 8. Обновлены примеры конфигураций 9. Исправлены ошибки |
| 3.8.0. | 1. [PODD-7379] Метрики подписок: фильтрация по атрибутам подписок 2. [PODD-7186] После обновления ПОДД до 3.7.0 подписки зависли в DELTA\_REQUEST 3. [PODD-7104] [ЗЛП][ПОДД] ЕПГУ после работ с агентом и потерей коннекта кафкой перестал слать акки по дельтам (среда ПРОД) 4. [PODD-7039] Доработка Notarius для ПФ 5. [PODD-6977] [DEV] Отказ от mTLS при получении JWT. Доработки в ядре 6. [PODD-6977] [DEV] Отказ от mTLS при получении JWT. Доработки на агенте 7. [PODD-6973] Проверка цепочки сертификатов | 1. Изменен раздел 2.2 Требования к среде развертывания Агента СМЭВ4:  * добавлен подраздел «2.2.1 Минимальные требования к серверу»; * добавлен подраздел «2.2.2 СКЗИ для работы Агента СМЭВ4».  1. Обновлен раздел 3. Описания конфигурационного файла 2. Обновлены примеры конфигураций. 3. Исправлены ошибки. |
| 3.9.0 | 1. PODD-7330 - DEV:: Формирование событий СЦЛ с кодом INTERNAL\_ERROR 2. PODD-7561 [DEV] Периодическая очистка очереди на основе deadline 3. PODD-7680 Удаление Databank 4. PODD-7834 Лимитирование - перенос лимитов по скачиванию блобов по ссылкам в Redis | 1. Добавлен раздел «3.3.12 Настройка типа аутентификации агента в ядре». 2. Обновлены примеры конфигураций. 3. Исправлены ошибки. |
| 3.9.1 | 1. PODD-8327 Анализ задержек при чтении сообщений агентом 3.9.0 из Pulsar | Изменений нет |
| 3.10.0 | 1. PODD-7995 Настройка Партиций и Фактора репликации для топиков Агента | 1. Обновлен раздел (см. [Раздел 3.3.3.2](#_3.3.3.2_Настройка_параметров)) описания конфигурационного файла |
| 3.11.0 | Изменений нет | 1. Уточнены требуемые лицензии CryptoPro в разделе «2.2.2 СКЗИ для работы Агента СМЭВ4»:  * CryptoPro CSP 5.0; * CryptoPro JCP 2.0. |

# 9 Приложение А Добавление промежуточных сертификатов в ключ CryptoPro

## 9.1 А.1 С использованием графического интерфейса

Для добавления промежуточных сертификатов в ключ CryptoPro следует:

1. Поместить контейнер ключа в папку пользователя, под которым далее будут исполняться команды, например /var/opt/cprocsp/keys/<user> или C:/Users/<user>/Local Settings/Application Data/Crypto Pro/.
2. Создать запрос на сертификат с помощью Java утилиты **keytool**. Для подписи запроса ГОСТ алгоритмом в Java должно быть установлено CryptoPro JCP или JCSP (см. документацию на CryptoPro).

Пример команды для Java17 с установленным CryptoPro JCSP (где «cryptopro/» - имя каталога, в котором находятся jar файлы CryptoPro JCSP):

keytool -J-Dkeytool.compat=true -J-Duse.cert.stub=true -provider ru.CryptoPro.JCP.JCP -providerpath cryptopro/JCSP.jar:cryptopro/JCP.jar: cryptopro/JCPRequest.jar:cryptopro/JCPRevCheck.jar:cryptopro/asn1rt.jar:cryptopro/ASN1P.jar -certreq -alias client\_01 -keysize 256 -sigalg GOST3411\_2012\_256withGOST3410\_2012\_256 -storetype HDImageStore -keystore NONE -storepass 1 -keypass 1234567890 -file client\_01.csr -ext KeyUsage=keyEncipherment,keyAgreement -ext ExtendedkeyUsage=clientAuth

* + Для ключей длиной 256 указывается «-sigalg GOST3411\_2012\_256withGOST3410\_2012\_256», для ключей длиной 512 указывается «-sigalg GOST3411\_2012\_512withGOST3410\_2012\_512».
  + Если контейнер ключа имеет кириллицу в алиасе, утилита keytool не увидит его, тогда контейнер можно переименовать, изменив алиас обычным редактором в файле контейнера «name.key». При этом целостность ключа не нарушится.

1. Запрос на сертификат передать в соответствующий УЦ для выпуска сертификата. Например, тестовый УЦ CryptoPro выдает сертификат на Web-форме <https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp>.
2. Полученный сертификат импортировать в контейнер ключа. Для этого в первую очередь подготовить файл в формате PKCS#7 (\*.p7b). Данную операцию можно сделать через GUI утилиту CryptoPro Tools (cptools) либо через Windows GUI утилиту «certmgr». Сертификат устанавливается в персональное хранилище пользователя, далее экспортируется в файл PKCS#7 (\*.p7b). Подробнее на [Рисунок - 9.1](#_d4e1a5f0e07e29a672d266a195c283cf) - [Рисунок - 9.5](#_cab974cf589adbe16f596992a2df49ce).

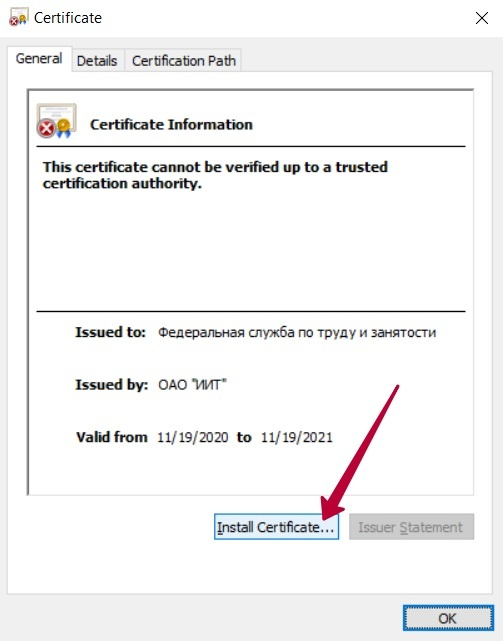


Рисунок - 9.1 Установка сертификата

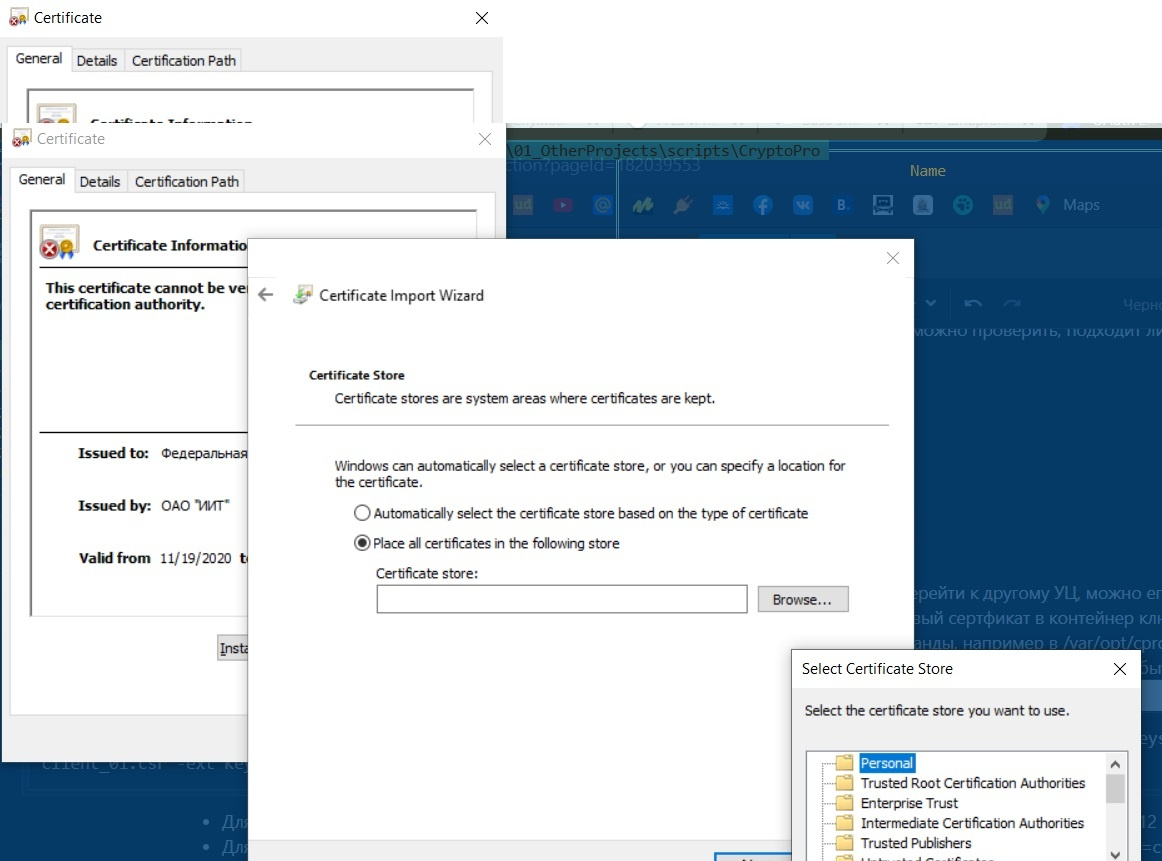


Рисунок - 9.2 Установка сертификата в персональное хранилище пользователя

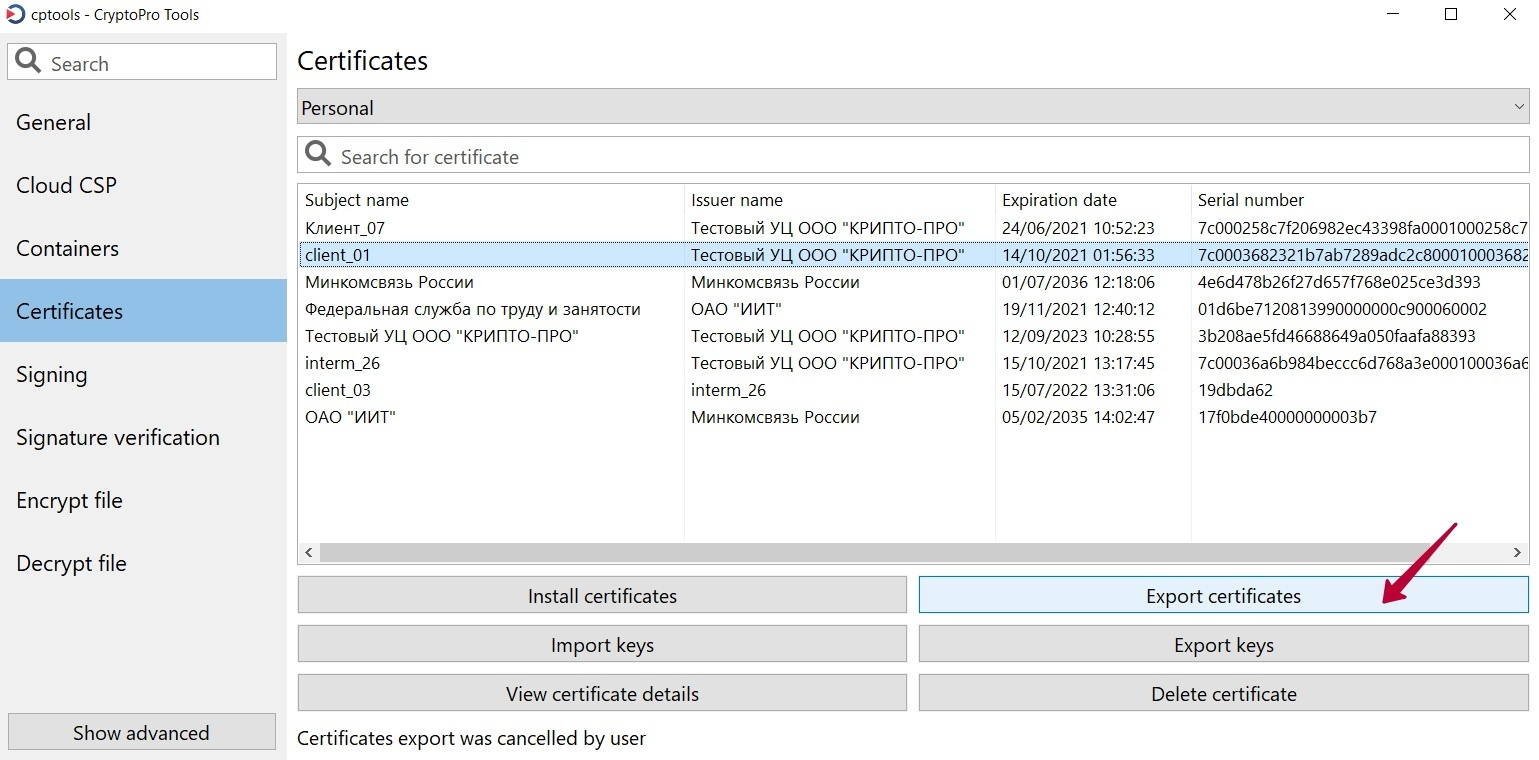


Рисунок - 9.3 Экспорт сертификата в CryptoPro Tools

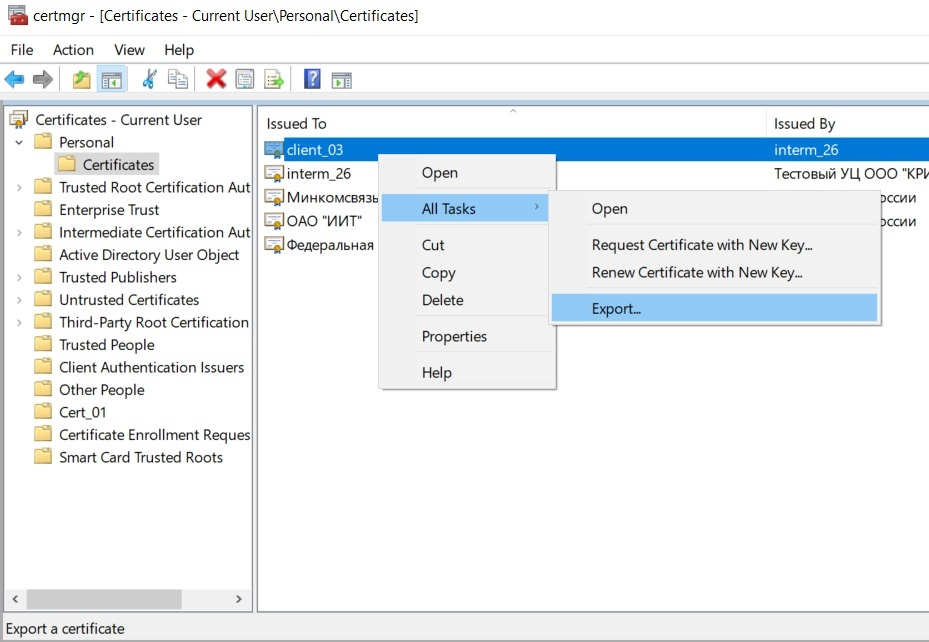


Рисунок - 9.4 Экспорт сертификата в certmgr

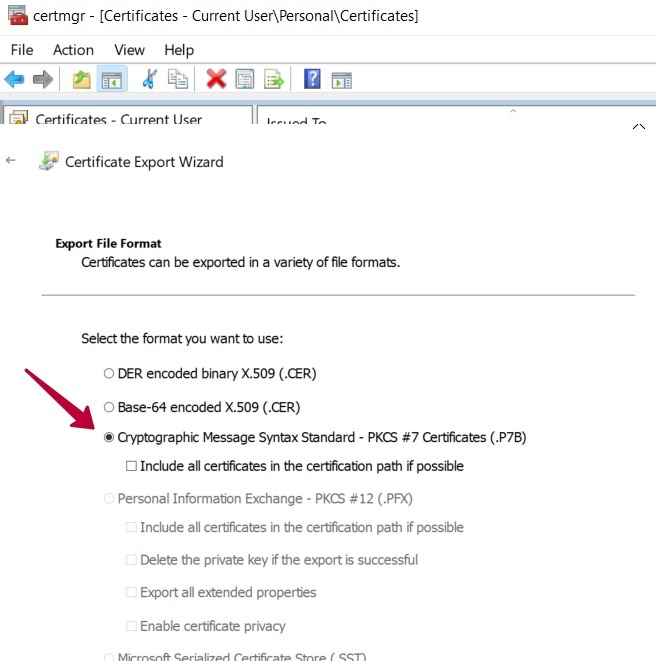


Рисунок - 9.5 Выбор формата PKCS#7 (\*.p7b) в certmgr

1. Импортировать файл \*.p7b в контейнер ключа командой (где «cryptopro/» - имя каталога, в котором находятся jar файлы CryptoPro JCSP):

keytool -J-Dkeytool.compat=true -J-Duse.cert.stub=true -provider ru.CryptoPro.JCP.JCP -providerpath cryptopro/JCSP.jar:cryptopro/JCP.jar: cryptopro/JCPRequest.jar:cryptopro/JCPRevCheck.jar:cryptopro/asn1rt.jar:cryptopro/ASN1P.jar -importcert -alias client\_01 -storetype HDImageStore -keystore NONE -storepass 1 -keypass 1234567890 -file client\_01.p7b

Аналогичным образом можно выгрузить несколько сертификатов (цепочку) в файл PKCS#7 (\*.p7b), чтобы потом загрузить их в контейнер.

Сертификаты из контейнера ключа передаются другой стороне для проверки при установке TLS соединения, соответственно, если в доверенном хранилище второй стороны (сервера или клиента) не хватает промежуточных сертификатов для проверки подписи по цепочке, сертификаты могут быть переданы из контейнера ключа.

При этом в контейнер можно класть не всю цепочку, а только сертификаты, которых не хватает у второй стороны для построения всей цепочки.

Стороны посылают сертификаты для проверки только из контейнера своего ключа и проверяют подпись по цепочке для полученных от второй стороны сертификатов по сертификатам в своём хранилище доверенных. Проверить наличие цепочки в контейнере можно через утилиты CryptoPro ([Рисунок - 9.6](#_e18281b08ac7264882a8ecfc5ee1839c), [Рисунок - 9.7](#_19863f2cbe431508842a92677c7aed9c)).

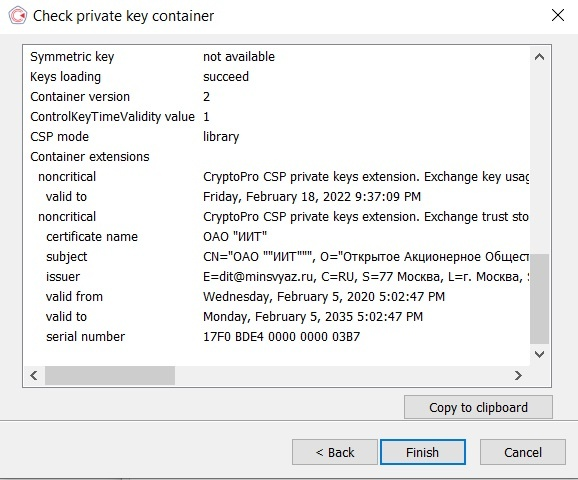


Рисунок - 9.6 Проверка наличия нескольких сертификатов в контейнере

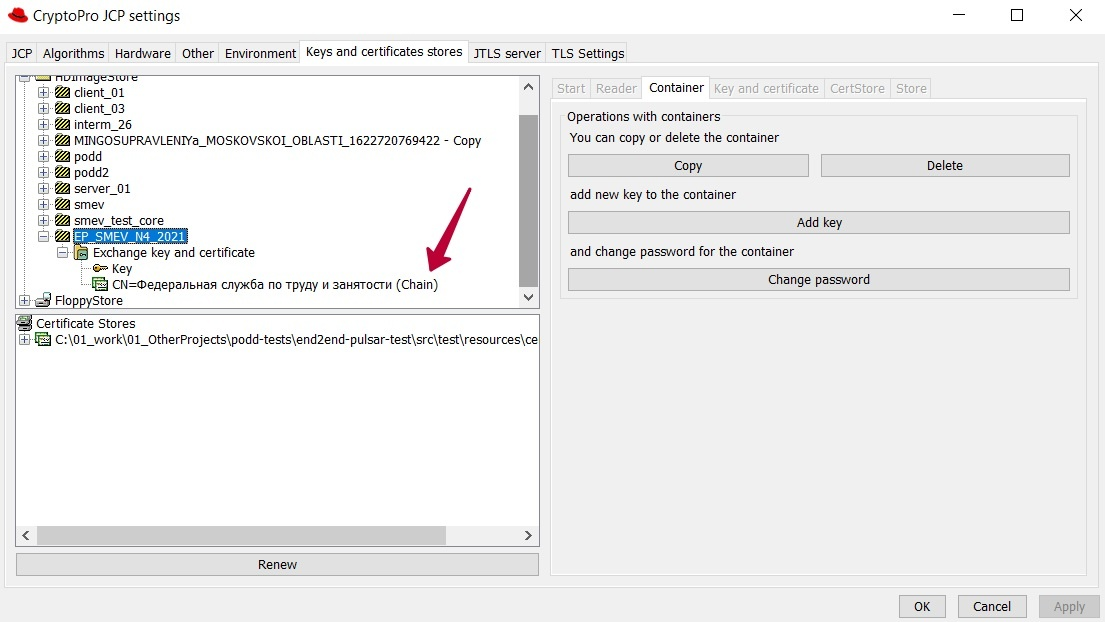


Рисунок - 9.7 Проверка наличия нескольких сертификатов в контейнере

Для промежуточных сертификатов сервер делает проверку атрибута BasicConstraints=ca:true, если атрибут отсутствует, сервер отклонит соединение с ошибкой в логе: client SSL certificate verify error: (24:invalid CA certificate).

## 9.2 А.2 С использованием командной строки ОС Linux

Для установки сертификата используется две основные команды: openssl и keytool.

Первая команда предназначена для формирования файла сертификата, закодированного в Base64-формате.

Инструмент **keytool** используется от java, установленной вместе с Агентом СМЭВ4. Этот инструмент можно найти в директории $JAVA\_HOME/bin/keytool.

Особое внимание стоит обратить на директорию приложения CryptoPro, полный путь до которого понадобится при указании необходимых библиотек для утилиты **keytool** в параметре -providerpath. Более подробный пример использования будет приведён ниже.

В случае запуска Агента СМЭВ4 в docker, перед проверкой или добавлением цепочки сертификатов необходимо будет зайти в запущенный контейнер и в нем продолжить работу с сертификатом. Следующая команда может служить примером входа в контейнер Агента СМЭВ4:

docker exec -it einfahrt bash

Все последующие команды будут выполняться в домашней директории Агента СМЭВ4. Там же находится установленное в директории cryptopro/ приложение **CryptoPro JCSP**.

Этот путь используется для явного указания зависимостей крипто провайдера.

Для установки цепочки сертификатов:

1. Убедиться в наличии контейнера в директории /var/opt/cprocsp/keys/{user} с именем пользователя, под которым выполняется проверка/изменение сертификата, где {user} – имя пользователя, под которым запускается агент (‘app’ в случае запуска в docker).
2. Если не известно имя или псевдоним/alias контейнера, то его можно узнать следующей командой:

less /var/opt/cprocsp/keys/{user}/{container}/name.key

где:

* user – имя пользователя, под которым запускается агент (‘app’ в случае запуска в docker),
* container – имя контейнера ключа cryptoPro.

1. Для проверки наличия цепочки сертификатов у контейнера, можно выполнить в домашней директории Агента СМЭВ4 команду, приведенную ниже. Обратите внимание на путь расположения в параметре –providerpath, его следует заменить на директорию расположения «Крипто ПРО», в нашем случае cryptopro/. {alias} в команде следует заменить на имя контейнера, известное или полученное на предыдущем шаге.

$JAVA\_HOME/bin/keytool **\**  
-v -list **\**  
-keystore NONE -storepass 1 -storetype HDImageStore **\**  
-provider ru.CryptoPro.JCP.JCP **\**  
-providerpath cryptopro/JCSP.jar:cryptopro/JCP.jar:cryptopro/JCPRevCheck.jar:cryptopro/asn1rt.jar:cryptopro/ASN1P.jar **\**  
-alias {alias}

В самом начале выведенных данных необходимо найти строчку, начинающуюся с Certificate chain length.

Этот параметр может принимать значения от единицы и выше. Если в результате стоит число «1», то цепочка отсутствует и необходимо переходить к следующему пункту.

Пример:

Alias name: certificate  
Creation date: 01.01.2022  
Entry type: PrivateKeyEntry  
Certificate chain length: 1

Если значение равно двум или выше, то в контейнере присутствуют сертификаты промежуточных удостоверяющих центров (УЦ).

1. Скачать необходимые сертификаты, используя информацию из предыдущего пункта. Для начала нужно найти строчки accessLocation: URIName и выбрать первую ссылку с расширением .crt, с помощью которой можно скачать сертификат УЦ.

Пример:

accessMethod: caIssuers  
accessLocation: URIName: http://url.ru/certificate.crt

Создать временную директорию для хранения сертификатов:

mkdir certs/

И скачать сертификат УЦ по ссылке: wget {полученный адрес} -O certs/center.crt

Чтобы получить сам сертификат из контейнера, можно воспользоваться командой, указав псевдоним контейнера в параметре -alias:

$JAVA\_HOME/bin/keytool **\**  
-exportcert **\**  
-keystore NONE -storepass 1 -storetype HDImageStore **\**  
-provider ru.CryptoPro.JCP.JCP **\**  
-providerpath cryptopro/JCSP.jar:cryptopro/JCP.jar:cryptopro/JCPRevCheck.jar:cryptopro/asn1rt.jar:cryptopro/ASN1P.jar **\**  
-file certs/local.cer **\**  
-alias {alias}

1. Необходимо сформировать файл, который будет содержать информацию о сертификатах. Для этого поочередно выполнить следующие команды:

openssl x509 -inform der -in certs/local.cer -out certs/local.pem  
openssl x509 -inform der -in certs/center.crt -out certs/center.pem  
cat certs/local.pem certs/center.pem > certs/chain.pem

1. Для добавления сгенерированной цепочки выполнить следующую команду:

$JAVA\_HOME/bin/keytool **\**  
-importcert -keystore NONE -storepass 1 -storetype HDImageStore **\**  
-provider ru.CryptoPro.JCP.JCP **\**  
-providerpath cryptopro/JCSP.jar:cryptopro/JCP.jar:cryptopro/JCPRevCheck.jar:cryptopro/asn1rt.jar:cryptopro/ASN1P.jar **\**  
-file certs/chain.pem **\**  
-alias {alias}

1. Выполнить команду из пункта 2 и убедиться, что значение Certificate chain length увеличилось на единицу, и контейнер содержит добавленные сертификаты.
2. Повторить добавление сертификатов для всех промежуточных УЦ.

# 10 Приложение B Список метрик Агента СМЭВ4

Таблица 10.1 Список метрик Агента

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Тема | Метрика Prometheus | Тип | Доп. метрики | Описание |
| 1 | Api Gateway | api\_gateway\_execution\_time\_seconds | Histogram |  | Время выполнения запроса API Gateway на стороне Агента Инициатора |
| 2 | Api Gateway | api\_gateway\_request\_handle\_time\_seconds | Histogram |  | Время выполнения запроса API Gateway на стороне Агента Ответчика |
| 3 | SQL-подзапрос | subquery\_request\_handle\_time\_seconds | Histogram | quantile | Время выполнения SQL подзапроса Поставщиком (Агент Поставщика - Витрина - Агент Поставщика) |
| 4 | Трафик агента | req\_time | Histogram | quantile  kind | Время обработки входящего запроса с указанием типа в kind |
| 5 | Трафик агента | req\_count | Counter | result  kind | Количество обработанных запросов с указанием типа запроса в kind |

Таблица 10.2 Описание меток

|  |  |  |
| --- | --- | --- |
|  | Метка | Описание |
| 1 | quantile | Возможные значения: 0.75, 0.9, 0.95, 0.99 |
| 2 | result | * «success»; * «cancel» (отмена по дедлайну); * «limit\_error» (блокировка по лимитам); * «error» |
| 3 | kind | Для рассылок:   * + запрос на получение дельты - subscription\_delta\_request   + уведомление Ядро -> Витрина Потребителя о новых данных в подписке - subscrip-tion\_delta\_notification\_in\_event   + уведомление о новых данных от Витрины Поставщика - subscrip-tion\_delta\_notification\_event   + запрос на передачу дельты: ответ с ошибкой - subscription\_delta\_error   + запрос на передачу дельты: ключ чанка с данными дельты - subscription\_delta\_result\_chunk   + статус применения дельты: подтверждение применения дельты - subscription\_delta\_apply\_result   + статус применения дельты: ошибка применения дельты - subscription\_delta\_apply\_error   + запрос дельты от ИС Потребителя подписки - subscription\_request\_delta   Для РЗ-SQL:   * + РЗ-SQL, произвольные запросы и подзапросы - query\_request   + ответ на РЗ-SQL, произвольный запрос - query\_result   + ошибочный ответ на РЗ-SQL от Витрины - query\_error   + SQL-подзапросы: sub\_query\_request, sub\_query\_result, sub\_query\_error   + запрос на загрузку ТП - table\_param   + запрос BLOB по ссылке - blob\_request   + успешный ответ на запрос BLOB по ссылке - blob\_result   + ошибочный ответ на запрос BLOB по ссылке - blob\_error   Для РЗ-REST:   * + чанк мета запроса РЗ-REST - api\_gw\_meta\_request   + чанк тела запроса РЗ-REST - api\_gw\_payload\_request   + ответ на РЗ-REST - api\_gw\_response |

1. Перечисленные документы размещены на [технологическом портале СМЭВ3](https://smev3.gosuslugi.ru/portal/) [↑](#footnote-ref-1)
2. Данные порты могут быть переопределены посредством конфигурационного файла [↑](#footnote-ref-2)
3. В соответствии с разделами 2.3 и 2.5 документа «Методические рекомендации по работе с ПОДД СМЭВ», размещенном на портале ЕСКС – <https://info.gosuslugi.ru/> [↑](#footnote-ref-3)