ИНФРАСТРУКТУРА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Руководство администратора Агента СМЭВ4

Версия 3.22.0

**СМЭВ4**

Листов 72

Москва, 2025

Содержание

[1 Введение 7](#_Toc202873147)

[1.1 Область применения 7](#_Toc202873148)

[1.2 Краткое описание возможностей 7](#_Toc202873149)

[1.3 Уровень подготовки пользователя 7](#_Toc202873150)

[1.4 Перечень документации для работы с СМЭВ4 7](#_Toc202873151)

[2 Назначение и условия применения 8](#_Toc202873152)

[2.1 Назначение 8](#_Toc202873153)

[2.2 Требования к среде для развертывания Агента СМЭВ4 8](#_Toc202873154)

[2.2.1 Минимальные требования к серверу 8](#_Toc202873155)

[2.2.2 Перечень стороннего ПО, необходимого для работы Агент СМЭВ4 9](#_Toc202873156)

[2.2.3 СКЗИ для работы Агента СМЭВ4 9](#_Toc202873157)

[2.3 Точки подключения к Агенту СМЭВ4 10](#_Toc202873158)

[3 Настройка и запуск Агента СМЭВ4 11](#_Toc202873159)

[3.1 Порядок загрузки данных и программ 11](#_Toc202873160)

[3.2 Подготовка и настройка системы для запуска Агента СМЭВ4 без использования Docker 11](#_Toc202873161)

[3.2.1 Состав и содержание дистрибутивного пакета 11](#_Toc202873162)

[3.2.2 Предварительные операции (установка «пре-реквизитов») 11](#_Toc202873163)

[3.2.3 Запуск Агента СМЭВ4 13](#_Toc202873164)

[3.2.4 Проверка работоспособности Агента СМЭВ4 после включения и запуска сервиса 14](#_Toc202873165)

[3.2.5 Настройка ротации логов (опционально) 15](#_Toc202873166)

[3.3 Настройка логирования в формате «Гостех» (опционально) 16](#_Toc202873167)

[3.4 Включение протоколирования тел запросов/ответов с сохранением с БД Clickhouse (опционально) 17](#_Toc202873168)

[3.5 Настройка и запуск Агента СМЭВ4 с использованием Docker 17](#_Toc202873169)

[3.5.1 Предварительные условия 17](#_Toc202873170)

[3.5.2 Настройка ротации лог-файлов в Docker (опционально) 17](#_Toc202873171)

[3.5.3 Состав и содержание дистрибутивного пакета 18](#_Toc202873172)

[3.5.4 Подготовка к запуску 18](#_Toc202873173)

[3.5.5 Запуск Агента СМЭВ4 19](#_Toc202873174)

[3.6 Обновление Агента СМЭВ4 21](#_Toc202873175)

[3.6.1 Информация по лицензированию CryptoPro 21](#_Toc202873176)

[4 Описание конфигурационного файла Агента СМЭВ4 23](#_Toc202873177)

[4.1 Состав и содержание файлов конфигурирования 23](#_Toc202873178)

[4.2 Реестр изменений файлов конфигурирования 23](#_Toc202873179)

[4.3 Формирование конфигурационного файла Агента СМЭВ4 27](#_Toc202873180)

[4.3.1 Общие настройки Агента 27](#_Toc202873181)

[4.3.2 Настройка ключей CryptoPro 27](#_Toc202873182)

[4.3.3 Настройка регистрации Витрин данных и подключения к Apache Kafka (только при использовании Витрин) 28](#_Toc202873183)

[4.3.3.1 Настройка создания топиков Агентом СМЭВ4 28](#_Toc202873184)

[4.3.4 Настройка возможности выполнения SQL-РЗ при взаимодействии Агента СМЭВ4 с Витриной по HTTP (опционально) 31](#_Toc202873185)

[4.3.5 Настройка организации информационного обмена с blob adapter (требуется только при включенном профайле QueryProvider) 31](#_Toc202873186)

[4.3.5.1 Настройка параметров создаваемых топиков (опционально) 31](#_Toc202873187)

[4.3.5.2 Настройка взаимодействия через пользовательские топики (опционально) 32](#_Toc202873188)

[4.3.6 Настройка подключения к Ядру СМЭВ4, в том числе для работы в гео-распределенной конфигурации 34](#_Toc202873189)

[4.3.7 Настройка модуля подписания печатных форм 35](#_Toc202873190)

[4.3.7.1 Настройка использования S3 для передачи БЛОБов (опционально) 36](#_Toc202873191)

[4.3.8 Настройки разбиения получаемой информации на чанки (опционально) 36](#_Toc202873192)

[4.3.9 Настройка организации информационного обмена через API Gateway (опционально) 37](#_Toc202873193)

[4.3.10 Настройка параметров времени активации Агента СМЭВ4 (опционально) 39](#_Toc202873194)

[4.3.11 Настройка Агента СМЭВ4 для работы в масштабированном варианте (опционально) 39](#_Toc202873195)

[4.3.12 Настройка подключения к NTP 39](#_Toc202873196)

[4.3.12.1 Настройка подключения к сервису криптографии (опционально) 40](#_Toc202873197)

[4.3.13 Настройка передачи информации аудита в ГосТех (опционально) 40](#_Toc202873198)

[4.3.14 Настройка параметров Сервиса проверки полномочий (опционально) 40](#_Toc202873199)

[4.3.15 Настройка таймаутов исполнения запросов по умолчанию (опционально) 41](#_Toc202873200)

[4.4 Настройка сбора метрик Агента СМЭВ4 (опционально) 41](#_Toc202873201)

[4.4.1 Настройка Агента СМЭВ4 для передачи метрик в Prometheus 41](#_Toc202873202)

[4.5 Переопределение значений портов REST и JDBC интерфейсов Агента СМЭВ4 (опционально, в случае необходимости) 41](#_Toc202873203)

[5 Настройка и запуск NTP сервера (опционально) 43](#_Toc202873204)

[5.1 Порядок загрузки данных и программ 43](#_Toc202873205)

[5.2 Настройка и запуск NTP сервиса БЕЗ использования Docker 43](#_Toc202873206)

[5.2.1 Состав и содержание дистрибутивного пакета 43](#_Toc202873207)

[5.2.2 Предварительные операции (установка «пре-реквизитов») 43](#_Toc202873208)

[5.2.3 Запуск NTP сервиса 44](#_Toc202873209)

[5.3 Настройка и запуск NTP сервиса с использованием Docker 44](#_Toc202873210)

[5.3.1 Предварительные условия 44](#_Toc202873211)

[5.3.2 Состав и содержание дистрибутивного пакета 44](#_Toc202873212)

[5.3.3 Подготовка к запуску 44](#_Toc202873213)

[5.3.4 Запуск NTP 45](#_Toc202873214)

[6 Типовые вопросы и проблемы 46](#_Toc202873215)

[Приложение A «Список используемых метрик Агента СМЭВ4» 48](#_Toc202873216)

[Приложение Б «Настройка и Установка Сервиса проверки полномочий Prohibitor» (опционально) 50](#_Toc202873217)

[1 Описание конфигурационных файлов Сервиса проверки полномочий 50](#_Toc202873218)

[1.1 Состав и содержание дистрибутивного пакета 50](#_Toc202873219)

[1.2 Реестр изменений конфигурационного файла 50](#_Toc202873220)

[2 Настройка и запуск Сервиса проверки полномочий 51](#_Toc202873221)

[2.1 Порядок загрузки данных и программ 52](#_Toc202873222)

[2.1.1 Состав и содержание дистрибутивного пакета 52](#_Toc202873223)

[2.2 Предварительные операции (установка «пре-реквизитов») 52](#_Toc202873224)

[2.3 Настройка БД для работы Сервиса проверки полномочий 52](#_Toc202873225)

[2.4 Запуск Сервиса проверки полномочий 53](#_Toc202873226)

[2.5 Формирование конфигурационного файла Сервиса проверки полномочий 54](#_Toc202873227)

[2.5.1 Общие настройки конфигурационного файла 54](#_Toc202873228)

[2.5.2 Настройка подключения к базе данных: 54](#_Toc202873229)

[2.5.3 Настройка подключения к сервису подписания и верификации сообщений (Опционально) 54](#_Toc202873230)

[2.5.4 Настройка параметров, связанных с настройками времени жизни и блокировки пользовательских учетных записей 55](#_Toc202873231)

[2.5.5 Настройка передачи информации аудита в ГосТех (Опционально) 55](#_Toc202873232)

[2.6 Создание пользователя для работы с Сервисом проверки полномочий 56](#_Toc202873233)

[3 Запуск консольной утилиты TOTP 56](#_Toc202873234)

[3.1 Порядок загрузки данных и программ 56](#_Toc202873235)

[3.1.1 Состав и содержание дистрибутивного пакета 56](#_Toc202873236)

[3.2 Предварительные операции 56](#_Toc202873237)

[3.3 Запуск TOTP CLI 56](#_Toc202873238)

[4 Настройка и запуск Сервиса проверки полномочий с использованием Docker 57](#_Toc202873239)

[Приложение В «Настройка и Установка Сервиса подписания и верификации сообщений Notarius» (опционально) 58](#_Toc202873240)

[1 Описание конфигурационных файлов Сервиса подписания и верификации сообщений 58](#_Toc202873241)

[1.1 Состав и содержание дистрибутивного пакета 58](#_Toc202873242)

[1.2 Реестр изменений конфигурационного файла 58](#_Toc202873243)

[2 Настройка и запуск Сервиса подписания и верификации сообщений 58](#_Toc202873244)

[2.1 Порядок загрузки данных и программ 58](#_Toc202873245)

[2.1.1 Состав и содержание дистрибутивного пакета 59](#_Toc202873246)

[2.2 Предварительные операции (установка «пре-реквизитов») 59](#_Toc202873247)

[2.3 Запуск Сервиса подписания и верификации сообщений 59](#_Toc202873248)

[2.4 Формирование конфигурационного файла Сервиса подписания и верификации сообщений 60](#_Toc202873249)

[2.4.1 Общие настройки конфигурационного файла 60](#_Toc202873250)

[2.5 Настройка ключей CryptoPro CSP 60](#_Toc202873251)

[2.6 Настройка модуля подписания печатных форм 60](#_Toc202873252)

[2.7 Настройка порта сервиса приема запросов 61](#_Toc202873253)

[2.8 Настройка Notarius для передачи метрик в Prometheus 61](#_Toc202873254)

[3 Настройка и запуск подписания и верификации сообщений с использованием Docker 61](#_Toc202873255)

[Приложение Г Подготовка Docker образов для возможности запуска приложений под Docker (podman) 63](#_Toc202873256)

[1 Подготовительные действия 63](#_Toc202873257)

[2 Создание Docker образов 63](#_Toc202873258)

[Термины и определения 67](#_Toc202873259)

[История изменений документа 70](#_Toc202873260)

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 1 «Введение» указаны область применения подсистемы, краткое описание ее возможностей, уровень необходимой подготовки пользователей подсистемы и перечень документации для работы со СМЭВ4.

В разделе 2 «Назначение и условия применения» описано назначение подсистемы и требования к среде развертывания подсистемы.

В разделе 3 «Настройка и запуск Агента СМЭВ4» приведено описание порядка подготовки, настройки и запуска Агента СМЭВ4.

В разделе 4 «Описание конфигурационного файла Агента СМЭВ4» приведен состав и содержание файлов конфигурации, а также описание действий по формированию конфигурационного файла Агента СМЭВ4.

В разделе 5 «Настройка и запуск NTP сервера (опционально)» приведено описание настройки и запуска опционального сервера NTP.

В разделе 6 «Типовые вопросы и проблемы» приведены типовые ошибки, причины и решения данных ошибок.

Приложение А «Список метрик Агента СМЭВ4» содержит таблицы с метриками и метками Агента СМЭВ4 и их описанием.

Приложение Б «Настройка и установка Сервиса проверки полномочий Prohibitor (опционально)» приведены:

* описание конфигурационных файлов Сервиса проверки полномочий;
* описание настроек и запуска данного сервиса;
* запуск консольной утилиты TOTP;
* настройка и запуск Сервиса с использованием Docker.

Приложение В «Настройка и установка Сервиса подписания и верификации сообщений Notarius (опционально)» приведены:

* описание конфигурационных файлов Сервиса подписания и верификации сообщений;
* описание настроек и запуска данного сервиса;
* настройка и запуск Сервиса с использованием Docker.

Приложение Г «Подготовка Docker образов для возможности запуска приложения под Docker» описаны настройки Docker образов для запуска приложения.

В разделе «Термины и определения» приведена таблица с терминами, используемыми в данном документе, и их определения.

В разделе «История изменений документа» приведена таблица с изменениями данного документа.

# 1 Введение

## 1.1 Область применения

СМЭВ4 — единый сервис доступа к данным СМЭВ, предназначенный для автоматизации 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

СМЭВ4 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 ОС Linux, версии применяемой для развертывания агента;
	+ администрирование CryptoPro;
	+ администрирование Docker (при его использовании).

## 1.4 Перечень документации для работы с СМЭВ4

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

* + Методические рекомендации по работе с СМЭВ4;
	+ Регламент «Правила и процедуры работы в СМЭВ4»

# 2 Назначение и условия применения

## 2.1 Назначение

СМЭВ4 состоит из следующих компонентов:

* + Ядро СМЭВ4 – центральный компонент СМЭВ4, размещенный в ИЭП.
	+ Агент СМЭВ4 – компонент СМЭВ4, устанавливаемый в контуре участника взаимодействия.
	+ Notarius (опциональный компонент) - модуль Агента СМЭВ4, сервис подписания и верификации сообщений предназначен для проверки подписи и подписания сообщений;
	+ Prohibitor (опциональный компонент) – модуль Агента СМЭВ4, сервис проверки полномочий предназначен для контроля и блокировки Поставщиком обращений к данным своей Витрины с использованием Регламентированных SQL-запросов (РЗ), устанавливаемый в контуре участника взаимодействия.

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

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 серверная | * ALT 8 SP Server 10
* RedOS 7.3
* Astra Linux 1.7 SE
 |
| ЦПУ | 2-х ядерный процессор |
| Оперативная память | 4 Гб |
| Дисковое пространство | 20 Гб |

[Таблица 2.2](#_080c788c472e83609f002d27f43fff2f) содержит минимальные требования к характеристикам сервера для развертывания сервиса «Prohibitor».

Таблица 2.2 Минимальные требования к характеристикам сервера для развертывания Prohibitor

|  |  |
| --- | --- |
| Характеристики | Prohibitor |
| ОС серверная | * ALT 8 SP Server 10
* RedOS 7.3
* Astra Linux 1.7 SE
 |
| ЦПУ | 2-х ядерный процессор |
| Оперативная память | 4 Гб |
| Дисковое пространство | 20 Гб |

[Таблица 2.3](#_3118fbcb68be2e2c03f9f99f1cf2b180) содержит минимальные требования к характеристикам сервера для развертывания сервиса «Notarius».

Таблица 2.3 Минимальные требования к характеристикам сервера для развертывания Notarius

|  |  |
| --- | --- |
| Характеристики | Notarius |
| ОС серверная | * ALT 8 SP Server 10
* RedOS 7.3
* Astra Linux 1.7 SE
 |
| ЦПУ | 2-х ядерный процессор |
| Оперативная память | 4 Гб |
| Дисковое пространство | 20 Гб |

### 2.2.2 Перечень стороннего ПО, необходимого для работы Агент СМЭВ4

Для обеспечения работоспособности Агента СМЭВ4 рекомендуется приобрести следующее стороннее ПО:

* + JDK версии 17.0, рекомендуется JDK 17 LTS Axiom сертифицированный дистрибутив JDK, а также лицензия, cоответствующей операционной системе, приобретается пользователем самостоятельно на сайте производителя <https://axiomjdk.ru/pages/downloads/#/java-17-lts>.
	+ СКЗИ CryptoPro CSP версии 5.0 R3 (см. [Раздел 2.2.3](#_860b8e2f18ebcc1403f16b6905d288f1)). Сертифицированный дистрибутив CryptoPro, cоответствующий операционной системе, приобретается пользователем самостоятельно на сайте производителя <https://cryptopro.ru/products/csp/downloads#latest_csp50r3_linux>.

|  |
| --- |
| Внимание: |
| В целях безопасности, на данных серверах должно отсутствовать любое стороннее ПО, не требующееся непосредственно для работы компонентов Агента СМЭВ4 |

### 2.2.3 СКЗИ для работы Агента СМЭВ4

Канал связи между Агентом СМЭВ4 и Ядром СМЭВ4 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:

* + CryptoPro CSP.

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

Криптография в Агенте обеспечивается CryptoPro CSP.

Помимо защиты канала сертифицированными средствами, для защиты канала, а именно авторизации Агента в Ядре СМЭВ4, используются токены доступа JWT.

Для этого используется односторонний TLS, через СКЗИ с помощью подписанного запроса в Ядро СМЭВ4.

* + для обеспечения защиты класса KC1 – СКЗИ «CryptoPro CSP» Версия 5.0 KC1 в исполнении 1-Base (CryptoPro CSP 5.0);
	+ для обеспечения защиты класса KC2 – СКЗИ «CryptoPro CSP» Версия 5.0 KC2 в исполнении 2-Base (CryptoPro CSP 5.0).

Агент СМЭВ4 является сервером для всех его клиентов и при этом является клиентом для Ядра СМЭВ. Криптографические функции в Агенте обеспечивается CryptoPro CSP 5.0.

Таким образом, для обеспечения работоспособности Агента СМЭВ4 необходимо приобретение серверной лицензии для CryptoPro CSP 5.0 R3 на официальном сайте поставщика: <https://cryptopro.ru/products/csp/downloads#latest_csp50_linux>. Рекомендации о приобретении лицензии указано в [Разделе 2.2.2](#_2.2.2_Перечень_стороннего).

Количество необходимых лицензий требуется рассчитать, ознакомившись с рекомендациями на сайте CryptoPro.

## 2.3 Точки подключения к Агенту СМЭВ4

[Таблица 2.4](#_87c82fc79b8df105548e3fef0d53c1b6) содержит точки подключения к Агенту СМЭВ4 и их назначение

Таблица 2.4 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; ссылка на скачивание актуальной версии драйвера указана в [Разделе 6](#_6_Типовые_вопросы).
 |
| 8171 (протокол 1)8172 (протокол 2) | Обмены по Регламентированным REST-запросам (API Gateway).Потребитель, в зависимости от используемого Поставщиком протокола, должен направлять запросы в соответствующий этому протоколу порт Агента ([Раздел 4.3.9](#_4.3.9_Настройка_организации)). Для уточнения используемого Поставщиком протокола требуется обратиться в службу эксплуатации СМЭВ4.Примечания:Для использования протокола 2, версия Агента должна быть 3.8.0 или выше как на стороне Потребителя, так и на стороне Поставщика.При использовании протокола 1 поддерживается максимальный объем запросов не более 5 мегабайт.При использовании протокола 2 поддерживается максимальный объем запросов не более 30 гигабайт. |

# 3 Настройка и запуск Агента СМЭВ4

## 3.1 Порядок загрузки данных и программ

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

## 3.2 Подготовка и настройка системы для запуска Агента СМЭВ4 без использования Docker

### 3.2.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Агента СМЭВ4 в архиве с бинарными файлами (/distr/einfahrt):

* /distr/einfahrt/app/app.jar – исполняемый файл;

Для установки Агента необходим CryptoPro CSP 5.0 R3, предназначенный для установки в используемую ОС. Его необходимо загрузить с сайта производителя <https://cryptopro.ru/products/csp/downloads#latest_csp50r3_linux>

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

Необходимо приобрести и загрузить с сайта <https://axiomjdk.ru/pages/downloads/#/java-17-lts> Axiom JDK 17-й версии, соответствующую используемой ОС

### 3.2.2 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. Создать каталог /distr/einfahrt, владельцем каталога назначить пользователя {{user}}. Создать каталог /distr/einfahrt/app, скопировать в него исполняемый файл Агента app.jar из дистрибутивного пакета.

|  |
| --- |
| Примечание: |
| Для того, чтобы пользователь мог перезапускать Агента и смотреть системный лог нужно указать: {{ user }} ALL=NOPASSWD:/bin/journalctl,/bin/systemctl. Если убрать «NOPASSWD:», то пароль будет запрашиваться каждый раз. |

1. Установить JDK (версия в примере ниже может отличаться для загруженного пакета)

Для ALT 8 SP Server 10

apt install axiomjdk-jdk-certified17.0.6+11-linux-amd64.\*\*alt8\*\*.rpm

Для RedOS 7.3

yum install axiomjdk-jdk-certified17.0.6+11-linux-amd64.rpm

Для Astra Linux 1.7 SE

apt-get install axiomjdk-jdk-certified17.0.6+11-linux-amd64.deb

1. Установить системные переменные

export JAVA\_HOME=/usr/lib/jdk/axiomjdk-java17.x86\_64
export PATH=$PATH:$JAVA\_HOME/bin

Переменные должны устанавливаться автоматически также после перезагрузки сервера.

Для этого рекомендуется внести данную настройку в **profile** ОС (/etc/profile.d).

1. Установить CryptoPro CSP, используя загруженный с сайта производителя пакет

|  |
| --- |
| Внимание: |
| Не требуется устанавливать отдельный экземпляр CryptoPro CSP для Агента или опционального компонента Prohibitor, если используется сервис подписания и верификации сообщений, установленный на отдельном сервере (см. [Раздел 4.3.12.1](#_4.3.12.1_Настройка_подключения) и [Раздел 2.5.3 Приложения Б](#_2.5.3_Настройка_подключения)) В этом случае CryptoPro CSP требуется установить на сервер, на котором разворачивается сервис подписания и верификации сообщений (см. [Приложение Г](#_Приложение_Г_Подготовка)) |

При установке на RedOS 7.3:

tar -xzvf linux-amd64.tgz
cd linux-amd64
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 установке на Astra Linux 1.7 SE:

cd /distr/einfahrt
tar -xzvf linux-amd64\_deb.tgz
cd linux-amd64\_deb
apt -y install lsb-cprocsp-base\*.deb lsb-cprocsp-rdr-64\*.deb lsb-cprocsp-kc1-64\*.deb lsb-cprocsp-capilite-64\*.deb lsb-cprocsp-devel\*.deb lsb-cprocsp-kc2-64\*.deb cprocsp-curl-64\*.deb
./install.sh
cd ..

При установке на ALT 8 SP Server 10:

tar -xzvf linux-amd64.tgz
cd linux-amd64
apt-get -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, 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.

|  |
| --- |
| Примечание: |
| Установка ключа CryptoPro требуется только на серверы, на которых устанавливается CryptoPro. Т.е. в случае использования сервиса подписания и верификации сообщений, (см. [Раздел 4.3.12.1](file:///C%3A%5CUsers%5CDStarkov%5CAppData%5CLocal%5CTemp%5C57c06f01-1d5a-4ea7-996f-9538e7c10e00_artifacts%20%288%29.zip.e00%5C_build%5Cdocx%5C%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0%20%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0%20%D0%A1%D0%9C%D0%AD%D0%924.docx#_4.3.12.1_Настройка_подключения) и [Раздел 2.5.3 Приложения Б](file:///C%3A%5CUsers%5CDStarkov%5CAppData%5CLocal%5CTemp%5C57c06f01-1d5a-4ea7-996f-9538e7c10e00_artifacts%20%288%29.zip.e00%5C_build%5Cdocx%5C%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0%20%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0%20%D0%A1%D0%9C%D0%AD%D0%924.docx#_2.5.3_Настройка_подключения)), установка ключей производится только на сервере сервиса подписания и верификации сообщений (notarius) |

1. В файл /etc/hosts добавить записи, соответствующие адресам серверов аутентификации:

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

**Или** выполнить команды:

echo -e “**\n\n***# Адреса сервиса аутентификации Агента СМЭВ4”*
echo -e “**\n\n**172.20.59.5 podd.gosuslugi.ru” >> /etc/hosts
echo -e “172.20.59.5 podd-cross.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.26 podd1.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.58 podd2.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.154 podd3.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.186 podd4.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.26 podd1-cross.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.58 podd2-cross.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.154 podd3-cross.gosuslugi.ru” >> /etc/hosts
echo -e “109.207.15.186 podd4-cross.gosuslugi.ru” >> /etc/hosts

1. Выложить в каталог /distr/enfahrt конфигурационный файл application.yml, подготовленный согласно описанию в [Разделе 4](#_4_Описание_конфигурационного). Установить пользователя {{user}} владельцем данного файла.

### 3.2.3 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** Данный файл, с названием einfahrt.service, необходимо сохранить в каталог /etc/systemd/system/, указав, при необходимости, корректные пути к файлам:

[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 CryptoPro!*
User={{user}} *# указать пользователя*
Group={{user\_group}} *# указать группу*

Environment="JAVA\_HOME=/usr/lib/jdk/axiomjdk-java17.x86\_64"
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=/usr/lib/jdk/axiomjdk-java17.x86\_64/bin/java -jar app/app.jar

[Install]
WantedBy=multi-user.target

Далее от имени пользователя **root** или используя sudo выполнить команду 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

### 3.2.4 Проверка работоспособности Агента СМЭВ4 после включения и запуска сервиса

Для проверки соединения Агента с Ядром СМЭВ4 необходимо выполнить команду с использованием утилиты curl.

Если утилита Curl не установлена необходимо ее установить из базового репозитория для Astra Linux 1.7 SE командой:

sudo apt-get install curl

для RedOS 7.3

sudo dnf install curl

Проверка корректной установки Агента СМЭВ4 осуществляется командой:

curl -X POST 'http://agent-ip-address:8192/query?async=false' -H "Accept-Version: 1" -H "Content-Type: application/json" -d '{"sql": {"sql": "select 1"}}'

Вывод должен быть следующим:

{
 "created\_at": "YYYY-MM-DD HH-MM-SS",
 "query\_id": "<identifier>",
 "meta": [
 {
 "name": "EXPR$0",
 "type": "INTEGER"
 }
 ],
 "rows": [
 [
 "1"
 ]
 ]
}

### 3.2.5 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** (поместить файл в /etc/logrotate.cron/einfahrt.conf) и поместите в него следующие строки:

/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 со 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 приведенную ниже строку:

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

Далее перезагрузите **systemd** сервис:

sudo systemctl daemon-reload
sudo systemctl restart einfahrt

## 3.3 Настройка логирования в формате «Гостех» (опционально)

Агент СМЭВ4 поддерживает запись логов в формате «Гостех». Для включения данного варианта логирования, необходимо в параметры запуска добавить значение параметра GOSTECH\_LOG\_ENABLED=true Данный параметр передается через указание дополнительного ключа «-D» в переменной JDK\_JAVA\_OPTIONS

Дополнительно могут быть заданы следующие опциональные параметры (в примере указаны значения по умолчанию):

* Имя лог-файла: GOSTECH\_LOG\_FILE\_NAME=log
* Имя каталога с лог-файлами: GOSTECH\_LOG\_DIR=/fluent-bit/logs/

|  |
| --- |
| Примечание: |
| Каталог, указанный в параметре GOSTECH\_LOG\_DIR, должен существовать, и быть доступным на запись для пользователя под которым запущен Агент СМЭВ4 |

|  |
| --- |
| Внимание: |
| Значение параметра GOSTECH\_LOG\_DIR должно заканчиваться символом «/» |

Пример определения переменной JDK\_JAVA\_OPTIONS в файле einfahrt.service с включенным логированием в формате «Гостех»:

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 \
 -DGOSTECH\_LOG\_ENABLED=true \
 -DGOSTECH\_LOG\_DIR=/fluent-bit/logs/ \
 -DGOSTECH\_LOG\_FILE\_NAME=log"

## 3.4 Включение протоколирования тел запросов/ответов с сохранением с БД Clickhouse (опционально)

Для протоколирования тел запросов/ответов с сохранением с БД Clickhouse, в параметрах запуска следует добавить параметры:

Для включения протоколирования:

-DAUDIT\_REQ\_RESP\_ENABLED=true

Для указания настроек подключения к БД:

-DAUDIT\_REQ\_RESP\_JDBC\_URL="jdbc:clickhouse://\*clickhouse\_host\*:8123/database\_name?user=database\_login&password=database\_password"

Также нужно указать путь к каталогу с JDBC драйвером clickhouse, либо положить драйвер в папку из которой уже настроена загрузка в classpath.

Для указания каталога с драйвером clickhouse указывается параметр:

-Dloader.path=/external\_libs/\*

Для подробного логирования парсера конфигурации logback:

-Dlogback.debug=true

Для проверки загрузки классов:

-verbose:class

Для включения протоколирования тел запросов/ответов с сохранением с файл:

-DAUDIT\_REQ\_RESP\_FILE\_ENABLED=true

Дополнительно возможно указать параметры (приведены значения по умолчанию):

* Имя лог-файла: -DAUDIT\_REQ\_RESP\_FILE\_NAME=gostech
* Имя папки с лог-файлами: -DAUDIT\_REQ\_RESP\_FILE\_LOG\_DIR=/fluent-bit/logs/

|  |
| --- |
| Примечание: |
| Каталог, указанный в параметре AUDIT\_REQ\_RESP\_FILE\_LOG\_DIR, должен существовать и быть доступным на запись для пользователя под которым запущен Агент СМЭВ4 |

|  |
| --- |
| Внимание: |
| Значение параметра AUDIT\_REQ\_RESP\_FILE\_LOG\_DIR должно заканчиваться символом «/» |

## 3.5 Настройка и запуск Агента СМЭВ4 с использованием Docker

### 3.5.1 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).

### 3.5.2 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:

для Astra Linux 1.7 SE:

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

для RedOS 7.3:

{
**"log-driver"**: "json-file",
**"live-restore"**: **true**,
**"icc"**: **false**,
**"disable-validation"**: **true**,
**"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).

### 3.5.3 Состав и содержание дистрибутивного пакета

Для запуска Агента под Docker необходимо самостоятельно собрать Docker образы, согласно описания в [Приложении Г](#_Приложение_Г_Подготовка)

### 3.5.4 Подготовка к запуску

Для запуска Агента СМЭВ4 необходимо после распаковки пакета сформировать конфигурационный файл application.yml, как указано в [Разделе 4.3](#_4.3_Формирование_конфигурационного) , и сохранить его в каталог /distr/einfahrt.

В каталоге /distr/einfahrt:

* создать подкаталог keys, сохранить в него полученный ключ CryptoPro **в распакованном виде** ;

|  |
| --- |
| Примечание: |
| создание подкаталога keys и сохранение в него ключа не требуется в случае использования сервиса подписания и верификации сообщений, (см. см. [Раздел 4.3.12.1](file:///C%3A%5CUsers%5CDStarkov%5CAppData%5CLocal%5CTemp%5C57c06f01-1d5a-4ea7-996f-9538e7c10e00_artifacts%20%288%29.zip.e00%5C_build%5Cdocx%5C%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0%20%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0%20%D0%A1%D0%9C%D0%AD%D0%924.docx#_4.3.12.1_Настройка_подключения) и [Раздел 2.5.3 Приложения Б](file:///C%3A%5CUsers%5CDStarkov%5CAppData%5CLocal%5CTemp%5C57c06f01-1d5a-4ea7-996f-9538e7c10e00_artifacts%20%288%29.zip.e00%5C_build%5Cdocx%5C%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0%20%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0%20%D0%A1%D0%9C%D0%AD%D0%924.docx#_2.5.3_Настройка_подключения)), в таком случае установка ключей производится только на сервере сервиса подписания и верификации сообщений (notarius) |

* + (только при использовании **HTTPS** API gateway) создать подкаталог certs, подготовить файл **cacerts** согласно [Разделу 4.3.9](#_4.3.9_Настройка_организации), сформированный файл сохранить в каталог /distr/einfahrt/certs.

При наличии файла расширенных настроек логирования customLogLevels.xml сохранить 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 сохранить архив с образом на локальный диск этой машины и выполнить команду:

docker load < einfahrt.tgz

где einfahrt.tgz – имя полученного архива с Docker образом Агента СМЭВ4.

Загрузка должна завершиться без ошибок.

Проверить успешность загрузки можно командой:

docker images | grep einfahrt

Вывод будет содержать информацию следующего вида:

einfahrt latest c7511824117e 5 days ago 1.2G

### 3.5.5 Запуск Агента СМЭВ4

Для запуска Агента СМЭВ4 используется скрипт run\_agent.sh

*#!/bin/bash*

*# Название docker image указать здесь*
IMAGE=einfahrt:latest
*# Список используемых портов приложения, указывается в круглых скобках*
PORT\_LIST=(8183 8192 8171 8172)

*###### DO NOT EDIT BELOW THIS LINE ###### НЕ РЕДАКТИРОВАТЬ НИЖЕ ######*
stop()
{
 echo $1
 exit 1
}

*#*
IMG=**$(**echo *${*IMAGE*}* |cut -d: -f1**)**
TAG=**$(**echo *${*IMAGE*}* |cut -d: -f2**)**
[ ! -f application.yml ] && stop "File application.yml not found; exiting" || chmod 0666 application.yml

DIR=**$(**pwd**)**

[ ! -d keys ] && stop "\"keys\" directory not found; exiting"

MOUNTS=" --mount type=bind,source=*${*DIR*}*/application.yml,target=/egov/java/application.yml,readonly"
[ -d keys ] && MOUNTS="*${*MOUNTS*}* --mount type=bind,source=*${*DIR*}*/keys,target=/var/opt/cprocsp/keys/app"
[ -d certs ] && MOUNTS="*${*MOUNTS*}* --mount type=bind,source=*${*DIR*}*/certs,target=/egov/java/certs,readonly"

*# check exisence of mandatory objects; set permissions*
**for** OBJECT **in** certs keys; **do**
 [ -d *${*OBJECT*}* ] && find *${*OBJECT*}* **\(** -type f -exec chmod 0666 {} + **\)** -o **\(** -type d -exec chmod 0777 {} + **\)**
**done**

*# Если есть лицензия КриптоПро CSP, она должна находиться в текстовом виде в файле licenses/csp.lic*
*# При отсутствии внешнего файла с лицензией, будет использовано trial лицензирование CryptoPro*
[ -f licenses/csp.txt ] && MOUNTS="*${*MOUNTS*}* --mount type=bind,source=*${*DIR*}*/licenses/csp.txt,target=/egov/csp.lic,readonly"

*# custom logger configuration, if exists*
**if** [ -f customLogLevels.xml ]; **then**
 chmod 0666 customLogLevels.xml
 MOUNTS="*${*MOUNTS*}* --mount type=bind,source=*${*DIR*}*/customLogLevels.xml,target=/chgCfgTmp/customLogLevels.xml"
**fi**

*# expose ports*
unset PORTS
**for** OBJECT **in** *${*PORT\_LIST[@]*}*; **do**
 PORTS="*${*PORTS*}* -p *${*OBJECT*}*:*${*OBJECT*}*"
**done**

echo "Checking for already started container, stop it if running"
[ ! -z **$(**docker ps |awk '{print $NF}'|grep "^*${*IMG*}*$"**)** ] && docker stop *${*IMG*}* >/dev/null
[ ! -z **$(**docker ps -a |awk '{print $NF}'|grep "^*${*IMG*}*$"**)** ] && docker rm *${*IMG*}* >/dev/null

echo "Starting docker container"
*# Важно! Для корректного использования ключей CryptoPro,*
*# процесс в контейнере docker должен выполняться пользователем app (id=1000)*
*# использование ключа «--user=1000» обязательно!*
docker run **\**
 -d **\**
 --user=1000 **\**
 --name *${*IMG*}* **\**
 --add-host podd.gosuslugi.ru:172.20.59.5 **\**
 --add-host podd1.gosuslugi.ru:109.207.15.26 **\**
 --add-host podd2.gosuslugi.ru:109.207.15.58 **\**
 --add-host podd3.gosuslugi.ru:109.207.15.154 **\**
 --add-host podd4.gosuslugi.ru:109.207.15.186 **\**
 --add-host podd-cross.gosuslugi.ru:172.20.59.5 **\**
 --add-host podd1-cross.gosuslugi.ru:109.207.15.26 **\**
 --add-host podd2-cross.gosuslugi.ru:109.207.15.58 **\**
 --add-host podd3-cross.gosuslugi.ru:109.207.15.154 **\**
 --add-host podd4-cross.gosuslugi.ru:109.207.15.186 **\**
 *${*PORTS*}* **\**
 --env LANG=en\_US.UTF-8 **\**
 --env LC\_ALL=en\_US.UTF-8 **\**
 --env JDK\_JAVA\_OPTIONS="" **\**
 *${*MOUNTS*}* **\**
 *${*IMG*}*:*${*TAG*}*

[ $? -eq 0 ] && echo "Application started. Container name: *${*IMG*}*. " || echo "Error starting docker."

Скрипт не требует указания параметров. При выполнении всех шагов, перечисленных в [Разделе 3.5.4](#_3.5.4_Подготовка_к), Агент СМЭВ4 будет успешно запущен. При повторном выполнении скрипта контейнер будет остановлен и запущен заново.

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

*#!/bin/bash*

NAME="einfahrt"

LOGFILE="log-**$(**date +%Y%m%d-%H%M%S**)**.txt"

echo "Check for container presence, gathering log"
**if** [ ! -z **$(**docker ps -a |awk '{print $NF}'|grep "^*${*NAME*}*$"**)** ]; **then**
 docker logs *${*NAME*}* >*${*LOGFILE*}* 2>&1
 echo "Log file gathered; See *${*LOGFILE*}* for details"
**else**
 echo "ERROR: No container process found"
 exit 1
**fi**

Остановка контейнера осуществляется командой docker stop einfahrt.

|  |
| --- |
| 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. |

## 3.6 Обновление Агента СМЭВ4

Для обновления версии Агента СМЭВ4 необходимо выполнить следующие шаги:

1. Скачать с [портала ЕСКС](https://info.gosuslugi.ru/docs/section/%D0%A1%D0%9C%D0%AD%D0%92_4_%28%D0%9F%D0%9E%D0%94%D0%94%29/) образцы файлов конфигурирования нужной версии.
2. Заполнить файл конфигурации application.yaml актуальными данными в соответствии с описанием в [Разделе 4.3](#_4.3_Формирование_конфигурационного).
3. Из пакета с дистрибутивом скопировать новую версию исполняемого файла Агента app.jar в каталог /distr/einfahrt/app, как указано в [Разделе 3.2.2](#_3.2.2_Предварительные_операции).
4. Проверить файл einfahrt.service на соответствие с описанием в [Разделе 3.2.3](#_3.2.3_Запуск_Агента)
5. Перезапустить Агент СМЭВ4.

Для обновления версии Агента СМЭВ4 с использованием Docker необходимо выполнить шаги описанные в [Разделе 3.5.4](#_3.5.4_Подготовка_к) и [Разделе 3.5.5](#_3.5.5_Запуск_Агента).

### 3.6.1 Информация по лицензированию CryptoPro

Входящий в поставку дистрибутив CryptoPro не имеет предустановленной лицензии, и может работать в «пробном режиме» в течение трех месяцев с момента создания образа (**не с момента первого запуска!**)

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

В случае, если имеется в наличии полная серверная лицензия на CryptoPro CSP, предусмотрена возможность передачи номера лицензий CSP при запуске контейнера. При передаче валидной лицензии CryptoPro будет лицензирована на этапе запуска.

Для этого необходимо, чтобы текстовый файл, содержащий строку с лицензией на CryptoPro CSP, был при запуске контейнера доступен внутри контейнера по пути /egov/csp.lic.

При запуске под Docker можно для этого монтировать внешние файлы, содержащие номера лицензии, по указанным выше путям.

**Для того, чтобы прилагаемый скрипт запуска применил имеющуюся лицензию CryptoPro, её необходимо поместить в текстовый файл ``licenses/csp.txt``. При отсутствии лицензии и использовании пробной версии CryptoPro не создавайте указанные файлы.**

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

# 4 Описание конфигурационного файла Агента СМЭВ4

## 4.1 Состав и содержание файлов конфигурирования

Состав дистрибутива Агента СМЭВ4 в архиве с конфигурационными файлами (/distr/einfahrt):

* + /distr/einfahrt/customLogLevels.xml – файл описания настроек логирования;
	+ /distr/einfahrt/conf/\*.yml – заготовки конфигурационных файлов для Потребителя и Поставщика, для тестовой и продуктивной среды.

В директории /distr/einfahrt/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 (Подключение только к одному ЦОД):
		- conf/prod-singleDC-consumer-application.yml – для Потребителя.
		- conf/prod-singleDC-producer-application.yml – для Поставщика.
	+ шаблоны конфигурационного файла Агента для тестовой среды:
		- conf/test-consumer-application.yml – для Потребителя.
		- conf/test-producer-application.yml – для Поставщика.

После распаковки дистрибутива необходимо 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 приведено в разделах ниже.

## 4.2 Реестр изменений файлов конфигурирования

[Таблица 4.1](#_1590441ee0ce88eec9ac24c6874db5a5) содержит Реестр изменений.

Таблица 4.1 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 4.3.9](#_4.3.9_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 4.3.9](#_4.3.9_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 СМЭВ4.
 |
| 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 CryptoPro, содержащих пробелы в алиасе;
	+ Изменён systemd unit для запуска агента, (см. [Раздел 3.2.3](#_9c5cea83061bcdd1d28eaa25440ed4b0))
 |
| 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 4.3.10](#_4.3.10_Настройка_параметров));
	+ Добавлен параметр управления используемым транспортом (pulsar/rsocket): agent.use-ca (см. [Раздел 4.3.1](#_4.3.1_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 4.3.1](#_4.3.1_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 4.3.1](#_4.3.1_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 4.3.5.1](#_4.3.5.1_Настройка_параметров)) |
| 3.11.0 | Изменений нет |
| 3.12.0 | Исключен параметр:* query.metadata.storeToDb
 |
| 3.13.0 | Исключены параметры:* datamart-registration.datamarts.registrationFlow
* datamart-registration.datamarts.definedProfile

Исключен файл postgresql.json |
| 3.14.0 | Исключены параметры:* trust-store.path
* trust-store.password
* data-center.default-node.pulsar.auth.keycloak-oauth.auth-type
* data-center.default-node.pulsar.auth.keycloak-oauth.auth-protocol
* data-center.signature.keystoreType
 |
| 3.15.0 | Добавлены параметры:* datamart.integration.blobAdapter.host;
* datamart.integration.blobAdapter.port;
* datamart.integration.prostore.host;
* datamart.integration.prostore.port;
* datamart.integration.type;

Параметр datamart.kafka-bootstrap-servers изменен на datamart.integration.kafka.kafka-bootstrap-servers. |
| 3.16.0 | Добавлены опциональные параметры:* notarius.target-host;
* notarius.target-port;
 |
| 3.17.0 | Изменений нет |
| 3.18.0 | Исключены параметры:* agent.use-ca;
* nodes.\*node\*.pulsar.\*;
* rest-query-endpoint.blobAutoresolve;
* rest-query-endpoint.jdbc-url;

Добавлен параметр:* nodes.\*node\*.auth.\*
 |
| 3.19.0 | Изменений нет |
| 3.20.1 | Исключен параметр datamart.zero-base-chunk-numЗначение параметра query.default-query-timeout по умолчанию установлено в 20 секундИзменены способ включения и настройки логирования для платформы Гостех (см. [Раздел 3.3](#_3.3_Настройка_логирования))Добавлена возможность сохранения тел запросов во внешнюю систему (clickhouse) (см. [Раздел 3.4](#_3.4_Включение_протоколирования)) |
| 3.21.0 | Исключены параметры* core.mnemonic
* core.broadcast-tenant
 |
| 3.22.0 | Изменений нет |

## 4.3 Формирование конфигурационного файла Агента СМЭВ4

### 4.3.1 Общие настройки Агента

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.

В предлагаемых шаблонах конфигурационных файлов указаны профайлы **QueryConsumer**, **ApiGwConsumer**, **ApiGwProvider** только для файлов конфигурации prod/\*-consumer-\*.yml.

Для файлов \*-producer-\*.yml данный блок отсутствует.

*# 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:
	* идентификатор агента (мнемоника соответствующей ИС из ЛК УВ);
	* ОГРН Агента (ОГРН организации владельца ИС из ЛК УВ)

**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 \*\*\*'

### 4.3.2 Настройка ключей CryptoPro

Указать идентификатор и пароль контейнера ключа CryptoPro:

Подробнее об идентификаторе ключа и о том, как получить контейнер закрытого ключа электронной подписи [на портале ЕСКС](https://info.gosuslugi.ru/articles/%D0%A0%D0%B0%D0%B1%D0%BE%D1%82%D0%B0_%D1%81_%D0%AD%D0%9F_%D0%B2_%D0%A1%D0%9C%D0%AD%D0%92/).

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

|  |
| --- |
| Примечание: |
| Указывать параметр password не требуется, если используется сервис подписания и верификации сообщений (см. [Раздел 4.3.12.1](#_4.3.12.1_Настройка_подключения)) |

В случае, если идентификатор ключа CryptoPro содержит пробелы, его следует заключить в одинарные кавычки.

### 4.3.3 Настройка регистрации Витрин данных и подключения к Apache Kafka (только при использовании Витрин)

|  |
| --- |
| Внимание: |
| указание адреса сервера(серверов) Apache Kafka (параметр datamart.integration.kafka.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. |

#### 4.3.3.1 Настройка создания топиков Агентом СМЭВ4

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

Доступна настройка взаимодействия нескольких схем Витрины данных 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 4.2](#_6b69a89d6d0e9a382603e81c5828b17c) содержит соответствие создаваемых топиков Apache Kafka параметрам конфигурационного файла.

Таблица 4.2 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 4.3.1](#_4.3.1_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 4.3.1](#_4.3.1_Общие_настройки). В этом случае раздел datamart-registration может полностью отсутствовать в конфигурационном файле.

*# Общие настройки витрин*
**datamart**:
 **integration**:
 *# подключение к Kafka для взаимодействия с витринами*
 **kafka**:
 **kafka-bootstrap-servers**: {{ kafka\_link }}
 *# автоматическое создание топиков витрины*
 **create-topics**:
 *# регистрация и настройка витрины*
 **config**: false
 *# информационный обмен с использованием SQL*
 **query**: true
 *# репликация*
 **replication**: true

*# 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 в нижнем регистре) \*\*\**
 *# 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 }}
 - **id**: {{ vitrine\_id2 }}

 *# 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
 *# 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**: ''

### 4.3.4 Настройка возможности выполнения SQL-РЗ при взаимодействии Агента СМЭВ4 с Витриной по HTTP (опционально)

Для обеспечения прямого взаимодействия Агента СМЭВ4 с Prostore на стороне Витрины, необходимо скопировать данный блок в файл application.yml и заполнить параметры datamart.integration.prostore.\* актуальными данными:

**datamart**:
 **integration**:
 **type**: HTTP
 **prostore**:
 **host**: '\*\*\* prostore\_host \*\*\*'
 **port**: '\*\*\* prostore\_port \*\*\*'

### 4.3.5 Настройка организации информационного обмена с blob adapter (требуется только при включенном профайле QueryProvider)

Для обеспечения прямого взаимодействия Агента СМЭВ4 с blob-адаптером на стороне Витрины, необходимо скопировать данный блок в файл application.yml и заполнить параметры datamart.integration.blobAdapter.\* актуальными данными:

|  |
| --- |
| Примечание: |
| Указание данного параметра требуется только при включенном профайле QueryProvder, см. [Раздел 4.3.1](#_4.3.1_Общие_настройки) |

**datamart**:
 **integration**:
 **blobAdapter**:
 **host**: '\*\*\* blob\_adapter\_host \*\*\*'
 **port**: '\*\*\* blob\_adapter\_port \*\*\*'

#### 4.3.5.1 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.

#### 4.3.5.2 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 Apache 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 СМЭВ4 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 СМЭВ4*
**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 имён по умолчанию, указать использование пользовательских топиков на стороне Витрины в конфигурации СМЭВ4-Адаптера – Модуль исполнения запросов, согласно разделу «7.1.1 Спецификация модуля СМЭВ4-адаптера – Модуль исполнения запросов» Руководства администратора Типового ПО «Витрина данных».

### 4.3.6 Настройка подключения к Ядру СМЭВ4, 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 СМЭВ4 (nodes), к которым подключается Агент СМЭВ4, с указанием адресов брокеров и сервиса авторизации Ядра СМЭВ4.

Пример раздела конфигурации:

*# Настройки подключения ко всем ЦОД с установленным ПО Ядра СМЭВ4*
**data-center**:
…
**nodes**:
 - **node-id**: {{ node1\_name }}
 *# Адреса брокеров*
 **broker-addresses**:
 - **host**: {{ broker1-host }}
 **port**: {{ broker1-port }}
 - **host**: {{ broker2-host }}
 **port**: {{ broker2-host }}
 **auth**:
 **oauth**:
 **auth-server**:
 *# список адресов серверов авторизации.*
 *# Может быть указано несколько адресов списком.*
 - **url**: {{ authentication\_kernel1\_address\_1 }}
 - **url**: {{ authentication\_kernel1\_address\_2 }}
 - **node-id**: {{ node2\_name }}
 **broker-addresses**:
 {...}
 **auth**:
 **oauth**:
 **auth-server**:
 *# Может быть указано несколько адресов списком.*
 - **url**: {{ authentication\_kernel2\_address\_1 }}
 - **url**: {{ authentication\_kernel2\_address\_2 }}
 {...}

В блоке data-center.default-node описаны параметры, общие для подключения ко всем Ядрам СМЭВ4. Как правило, их изменение не требуется относительно значений по умолчанию.

### 4.3.7 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 }}
 {...}

#### 4.3.7.1 Настройка использования S3 для передачи БЛОБов (опционально)

*Раздел применим только при использовании хранилища типа S3 (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. Данный файл создается вручную, при наличии необходимости в нем.

Формат указания учетных данных в файле s3\_creds.properties:

accessKey = '\*\*\* логин \*\*\*'
secretKey = '\*\*\* пароль \*\*\*'

В случае, если S3 не используется (т.е. параметр blob-source имеет значение «DATAMART»), адрес, bucket и путь могут быть указаны любые, либо отсутствовать.

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 }}

### 4.3.8 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 rest-query-endpoint.tableParamChunkType, который может принимать значения:

* + EXACTLY\_CUT – позволяет разбивать информацию на чанки исходя из размера чанка (размер чанка указывается параметром rest-query-endpoint.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.

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

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

|  |
| --- |
| Внимание: |
| Данная настройка опциональна, применяется только при использовании API Gateway; Некоторые шаги выполняются только при использовании **HTTPS** для коммуникации, подробнее см. в описании шагов |

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 3.2.2](#_3.2.2_Предварительные_операции))

cp /usr/lib/jvm/axiomjdk-java17.x86\_64/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 поставщика данных.
1. В параметры запуска агента добавить ключи -Djavax.net.ssl.keyStore=certs/cacerts и -Djavax.net.ssl.trustStore=certs/cacerts. При использовании systemd ([Раздел 3.2.3](#_3.2.3_Запуск_Агента)) данные параметры добавить в строку описания переменных окружения: 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 http(s) сервера*
 **default-host**: '\*\*\* адрес подключения к серверу \*\*\*'
 **default-port**: '\*\*\* адрес подключения к серверу \*\*\*'
 **ssl**: true *# false при использовании http*
 **verifyHost**: false
 **maxPoolSize**: 100

1. При необходимости настройки таймаутов указать опциональные параметры (ниже приведены дефолтные значения, которые используются в случае, 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 протокола 1 (по умолчанию 8171):

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

* при использовании протокола 2 (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*
 **target-arch**:
 **server-port**: 8172

### 4.3.10 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.

### 4.3.11 Настройка Агента СМЭВ4 для работы в масштабированном варианте (опционально)

1. Указать идентификатор экземпляра Агента СМЭВ4. В случае использования масштабируемого Агента СМЭВ4, 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}

1. При создании отказоустойчивого кластера каждый экземпляр КриптоПро CSP 5 R3 должен работать под лицензией и не нарушать лицензионных условий производителя ([Раздел 2.2.3](#_2.2.3_СКЗИ_для)).

### 4.3.12 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 один или более 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**.

#### 4.3.12.1 Настройка подключения к сервису криптографии (опционально)

Агент СМЭВ4 может работать как использовать встроенные средства криптографии, так и предоставляемые опциональным компонентом Notarius. В случае использования Notarius для средств криптографии, необходимо добавить блок notarius в файл application.yml и заполнить параметр notarius.target-host.

Пример раздела конфигурации (номер порта должен соответствовать указанному в конфигурационном файле Notarius, см. [Раздел 2.4 Приложения В](#_2.4_Формирование_конфигурационного)):

**notarius**:
 **enabled**: true
 **endpoints**:
 - **target-host**: '\*\*\* IP АДРЕС ПЕРВОГО СЕРВЕРА ПОДПИСАНИЯ И ВЕРИФИКАЦИИ СООБЩЕНИЙ СМЭВ4 \*\*\*'
 **target-port**: 8696
 - **target-host**: '\*\*\* IP АДРЕС ВТОРОГО СЕРВЕРА ПОДПИСАНИЯ И ВЕРИФИКАЦИИ СООБЩЕНИЙ СМЭВ4 (при наличии) \*\*\*'
 **target-port**: 8696
 {...}

|  |
| --- |
| Внимание: |
| При использовании более одного экземпляра сервера подписания и верификации сообщений (notarius), каждый экземпляр должен быть указан в вышеуказанном списке явным образом. НЕ ДОПУСКАЕТСЯ использование любого вида прокси и балансировщиков между Агентом СМЭВ4 и Сервером подписания и верификации сообщений СМЭВ4 (notarius) |

При указании данного параметра внутренние криптографические функции в Агенте СМЭВ4 **не задействуются**.

### 4.3.13 Настройка передачи информации аудита в ГосТех (опционально)

Для активации передачи информации аудита при работе Агента СМЭВ4 на платформе ГосТех, необходимо скопировать данный блок в файл application.yml и заполнить параметры gostech.audit.\* актуальными данными:

**gostech**:
 **enabled**: true
 **audit**:
 **host**: '\*\*\* audit\_server\_host \*\*\*'
 **port**: '\*\*\* audit\_server\_port \*\*\*'

### 4.3.14 Настройка параметров Сервиса проверки полномочий (опционально)

Для активации работы функций Сервиса проверки полномочий ([Приложение Б](%D0%9D%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0#_Приложение_Б_)), необходимо скопировать данный блок в файл application.yml и заполнить параметры allowance.prohibitor-client.\* актуальными данными:

**allowance**:
 **enabled-sql**: true
 **enabled-api-gateway**: true
 **prohibitor-client**:
 **default-host**: '\*\*\* prohibitor\_server\_host \*\*\*'
 **default-port**: '\*\*\* prohibitor\_server\_port \*\*\*'

### 4.3.15 Настройка таймаутов исполнения запросов по умолчанию (опционально)

Для изменения таймаутов по умолчанию (применяются при отсутствии таймаута в запросе) требуется добавить в конфигурацию агента дополнительные параметры. (Примеры значений: 15s, 5m, 1h).

При отсутствии параметра в конфигурации применяется значение по молчанию, указанное ниже.

**query**:

…
 *# Таймаут для SQL-запросов, включая запросы блобов через JDBC*

 **default-query-timeout:** 20s
 *# Таймаут для запросов блобов по ссылке через REST*
 **default-blob-query-timeout**: 20s

**api-gateway**:

…
 *# Таймаут для API Gateway запросов*

 **default-apigw-query-timeout:** 20s

## 4.4 Настройка сбора метрик Агента СМЭВ4 (опционально)

### 4.4.1 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.

Список используемых метрик приведен в [Приложение А](%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA#_Приложение_A_).

## 4.5 Переопределение значений портов REST и JDBC интерфейсов Агента СМЭВ4 (опционально, в случае необходимости)

Порты REST и JDBC интерфейсов при необходимости можно изменить указанием следующих параметров в конфигурационном файле.

Для REST интерфейса (по умолчанию 8192):

**rest-query-endpoint**:
 **port**: 8192

Для JDBC интерфейса (по умолчанию 8183):

**query-server**:
 **port**: 8183

В случае запуска Агента СМЭВ4 под Docker, необходимо также изменить значения портов в скрипте run\_agent.sh (см. [Раздел 3.5.5](#_3.5.5_Запуск_Агента))

# 5 Настройка и запуск NTP сервера (опционально)

## 5.1 Порядок загрузки данных и программ

|  |
| --- |
| Внимание: |
| Данный дистрибутивный пакет находится в открытом доступе на портале ЕСКС по адресу <https://info.gosuslugi.ru/download.php?id=1342> В него включен rpm пакет chrony для установки на ОС RedOS, а также примеры конфигурационных файлов. В случае использования ОС Astra Linux, соответствующий deb пакет устанавливается из официального репозитория Astra Linux. Находящиеся в дистрибутивном пакете конфигурационные файлы применимы вне зависимости от версии операционной системы. |

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 RedOS 7.3;
	+ /distr/common/einfahrt-chrony.service — unit файл 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 приведенные ниже команды.

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

|  |
| --- |
| Примечание: |
| До запуска сервера необходимо убедиться, что время на сервере выставлено корректно. |

Перед запуском NTP сервиса выполнить от имени пользователя **root** следующие действия:

1. Установить пакет с сервисом chrony:

**Для Astra Linux 1.7 SE**

apt-update && apt-get install -y chrony

**Для RedOS 7.3**

cd /distr/chrony
yum localinstall chrony.rpm

**Для ALT 8 SP Server 10**

apt-get install chrony

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

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

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

### 5.2.3 Запуск NTP сервиса

Файл системного сервиса /distr/common/einfahrt-chrony.service необходимо скопировать в каталог /etc/systemd/system/, при необходимости скорректировав в нем пути к файлам.

Далее, от имени пользователя **root** выполнить команду по включению, и 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 скопировать 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 СМЭВ4 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/%D0%A2%D0%B8%D0%BF%D0%BE%D0%B2%D1%8B%D0%B5_%D0%BE%D1%88%D0%B8%D0%B1%D0%BA%D0%B8_%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0_%D0%A1%D0%9C%D0%AD%D0%924/)

Таблица 6.1 Типовые вопросы и проблемы

|  |  |  |
| --- | --- | --- |
| № | Вопрос/Проблема | Возможная причина |
| 1 | Как узнать версию установленного Агента СМЭВ4 | Проверка версии установленного Агента СМЭВ4 осуществляется командой:curl -X GET 'http://<agent-ip>:8192/api/v1/agent-info/version' |
| 2 | Как скачать актуальный JDBC драйвер? | Драйвер можно получить по адресу http://<agent-ip>:8192/api/v1/jdbc-driver. |
| 2 | 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. |
| 3 | 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.
 |
| 4 | В логе присутствуют сообщения «No required SSL certificate was sent» | Убедитесь, что используется верный ключ, и в нем присутствует необходимый сертификат |
| 5 | 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 лицензию на CryptoPro CSP и внести информацию о лицензии в систему, согласно инструкции в [Разделе 3.6.1](#_3.6.1_Информация_по) настоящего документа |
| 6 | 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 СМЭВ4 СМЭВ.

У вас будут запрошены дополнительные данные о подключении, необходимо будет их предоставить согласно инструкции от службы поддержки. |

# Приложение A «Список используемых метрик Агента СМЭВ4»

В таблице ниже приведен список используемых метрик Агента СМЭВ4. Отображаемые, но не описанные в данной таблице метрики не рекомендуются к использованию.

Таблица 7.1 Список метрик Агента

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Тема | Метрика Prometheus | Тип | Метка | 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 | quantilekind | Время обработки входящего запроса с указанием типа в kind |
| 5 | Трафик агента | req\_count | Counter | resultkind | Количество обработанных запросов с указанием типа запроса в kind |
| 6 | Трафик агента | agent2broker\_connection | Gauge | nodeIdtypeaddress | Соединение с брокеромметрика показывает кол-во соединений:* 1 - cсоединение установлено;
* 0 - соединение разорвано.
 |

Таблица 7.2 Описание меток, приведенных в [Таблица 7.1](#_00b782d1f764974793a66bf774e877a2).

|  |  |  |
| --- | --- | --- |
| № | Метка | Описание |
| 1 | address | Адрес брокера |
| 2 | 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.
 |
| 3 | nodeId | Идентификатор ноды |
| 4 | quantile | Возможные значения: 0.75, 0.9, 0.95, 0.99 |
| 5 | result | Успешность результата обработки запроса* «success»;
* «cancel» (отмена по дедлайну);
* «limit\_error» (блокировка по лимитам);
* «error»
 |
| 6 | type | Тип соединения |

# Приложение Б «Настройка и Установка Сервиса проверки полномочий Prohibitor» (опционально)

## 1 Описание конфигурационных файлов Сервиса проверки полномочий

### 1.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Сервиса проверки полномочий.

* + /distr/prohibitor – Сервис проверки полномочий:
		- /distr/prohibitor/customLogLevels.xml – файл описания настроек логирования;
		- /distr/prohibitor/conf/\*.yml – заготовки конфигурационного файла;

В директории conf/ пакета находятся типовые заготовки конфигурационного файла.

Необходимо взять заготовку конфигурационного файла в соответствии с потребностями:

* + шаблон конфигурационного файла Сервиса проверки полномочий для продуктивной среды (2-х ЦОДовая конфигурация: ФЦОД, РЦОД):
		- conf/prod-prohibitor-application.yml.
	+ шаблон конфигурационного файла Сервиса проверки полномочий для продуктивной среды (1-на ЦОДовая конфигурация: ФЦОД):
		- conf/prod-singleDC-prohibitor-application.yml.
	+ шаблон конфигурационного файла Сервиса проверки полномочий для тестовой среды:
		- conf/test-prohibitor-application.yml.

Скопировать выбранный файл в каталог /distr/prohibitor 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.

### 1.2 Реестр изменений конфигурационного файла

[Таблица 8.1](#_0a4ecc06753dec3b86c13a64ccacb898) содержит реестр изменений.

Таблица 8.1 Реестр изменений конфигурационного файла

|  |  |
| --- | --- |
| Версия | Перечень изменений (относительно предыдущей версии) |
| 3.5.4 | Добавлен компонент Prohibitor |
| 3.8.1 | * + удалены параметры подключения к pulsar:
		- data-center.default-node.pulsar.auth.keycloak-oauth.realm
		- data-center.default-node.pulsar.auth.keycloak-oauth.grant\_type
		- data-center.default-node.pulsar.auth.keycloak-oauth.client\_id
	+ добавлены параметры ([Раздел 4.3.12.1](#_4.3.12.1_Настройка_подключения)) выбора способа аутентификации:
		- data-center.default-node.pulsar.auth.keycloak-oauth.auth-typee
		- data-center.default-node.pulsar.auth.keycloak-oauth.auth-protocol
	+ добавлен параметр ([Раздел 2.5 Приложения Б](#_2.5_Формирование_конфигурационного)) выбора транспорта (pulsar/RSocket)
 |
| 3.14.0 | Исключены параметры:* trust-store.path
* trust-store.password
* data-center.default-node.pulsar.auth.keycloak-oauth.auth-type
* data-center.default-node.pulsar.auth.keycloak-oauth.auth-protocol
 |
| 3.15.0 | Изменений нет |
| 3.16.0 | Добавлены параметры:* notarius.target-host
* notarius.target-port
 |
| 3.17.0 | Изменений нет |
| 3.18.0 | Исключен параметр:* agent.use-ca
 |
| 3.19.0 | Добавлены параметра:* agent.host
* agent.port
 |
| 3.20.1 | Изменений нет |
| 3.21.0 | Изменений нет |
| 3.22.0 | Изменений нет |

## 2 Настройка и запуск Сервиса проверки полномочий

**Prohibitor** - Сервис проверки полномочий предназначен для контроля и блокировки Поставщиком обращений к данным своей Витрины с использованием Регламентированных SQL-запросов (РЗ).

Установка Prohibitor опциональна, если Агент СМЭВ4 используется исключительно в качестве ПО, обеспечивающего доступ к данным посредством СМЭВ.

Действия (успешные и неуспешные), совершенные пользователями Сервиса проверки полномочий, логируются для передачи в систему сбора событий Аудита (SIEM) на стороне Поставщика данных. Перечень логируемых действий:

* создание пользователя;
* удаление пользователя;
* блокировка и разблокировка пользователя;
* блокировка и подтверждение полномочия на выполнение РЗ.

|  |
| --- |
| Внимание: |
| Для соблюдения требований безопасности к сертифицированному Агенту СМЭВ4 в контуре Поставщика рекомендуется:* развернуть систему сбора событий Аудита (SIEM);
* хранить во внешней системе сбора событий Аудита (SIEM) данные аудита Сервиса проверки полномочий минимум один год.
 |

### 2.1 Порядок загрузки данных и программ

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

#### 2.1.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Сервиса проверки полномочий (/distr/prohibitor):

* + /distr/prohibitor/app/app.jar – исполняемый файл;
	+ /distr/prohibitor/prohibitor-cli/prohibitor-cli.jar – исполняемый файл;
	+ /distr/prohibitor/totp-cli/totp\_cli – исполняемый файл утилиты двухфакторной аутентификации;

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

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

В случае, если Prohibitor устанавливается на машине, отличной от той где установлен Агент, перед запуском Prohibitor необходимо выполнить действия, описанные в [Разделе 3.2.2](#_3.2.2_Предварительные_операции):

|  |
| --- |
| Внимание: |
| Не требуется устанавливать отдельный экземпляр CryptoPro CSP для сервиса проверки полномочий, в следующих случаях:* если Сервис проверки полномочий установлен на том же сервере, что и Агент СМЭВ4 в варианте «без использования Docker», в такой ситуации на данном сервере уже имеется установленная CryptoPro CSP;
* если Сервис проверки полномочий настроен на использование Агента СМЭВ4 для проверки подписи, согласно см. [Раздел 2.5.3 Приложения Б](file:///C%3A%5CUsers%5CDStarkov%5CAppData%5CLocal%5CTemp%5C57c06f01-1d5a-4ea7-996f-9538e7c10e00_artifacts%20%288%29.zip.e00%5C_build%5Cdocx%5C%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0%20%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0%20%D0%A1%D0%9C%D0%AD%D0%924.docx#_2.5.3_Настройка_подключения).
 |

Выложить в каталог /distr/prohibitor конфигурационный файл application.yml, подготовленный согласно [Разделу 2.5 Приложения Б](#_2.5_Формирование_конфигурационного), в /distr/prohibitor/config выложить подготовленный файл logback.xml.

Доступ к админ-консоли Prohibitor необходимо проксировать с помощью внешних инфраструктурных решений. Указанный прокси должен поддерживать работу клиента с ним только по ГОСТ TLS. Прямой доступ к порту админ-консоли Prohibitor необходимо ограничить средствами ОС или инфраструктуры, для недопущения прямого доступа к нему пользователей по нешифрованному протоколу.

Установить СУБД Postgres 15

### 2.3 Настройка БД для работы Сервиса проверки полномочий

1. Подключится к БД PostgreSQL с административным аккаунтом и выполнить SQL команды ниже. Используйте собственные имя БД, имя пользователя и пароль, эти же данные должны быть указаны в конфигурационном файле сервиса Prohibitor: (см. [Раздел 2.5 Приложения Б](#_2.5_Формирование_конфигурационного))

**CREATE** **DATABASE** prohibitor;
**CREATE** **USER** dbadmin\_prohibitor **WITH** **ENCRYPTED** PASSWORD '<postgres\_pass>' NOSUPERUSER CREATEROLE **CREATEDB** INHERIT LOGIN NOREPLICATION;
**ALTER** **DATABASE** prohibitor **OWNER** **TO** dbadmin\_prohibitor;

Следующие команды следует выполнять от имени пользователя, подключенного к БД Prohibitor с административным аккаунтом:

**GRANT** **ALL** **PRIVILEGES** **ON** **ALL** TABLES **IN** **SCHEMA** **public** **TO** dbadmin\_prohibitor;
**GRANT** **ALL** **PRIVILEGES** **ON** **ALL** SEQUENCES **IN** **SCHEMA** **public** **TO** dbadmin\_prohibitor;

### 2.4 Запуск Сервиса проверки полномочий

Убедитесь, что пользователь {{user}} имеет доступ к директориям, в которой установлен Prohibitor: /distr/prohibitor.

Пример раздела конфигурации скрипта для запуска **Prohibitor** с использованием сервиса **systemd** Данный файл, с названием prohibitor.service, необходимо сохранить в каталог /etc/systemd/system/, скорректировав, при необходимости, пути к файлам

[Unit]
Description="Service for prohibitor"
After=syslog.target

[Service]
Type=simple

WorkingDirectory=/distr/prohibitor
User={{user}} *#указать пользователя*
Group={{user\_group}} *#указать группу*

Environment="JAVA\_HOME=/usr/lib/jdk/axiomjdk-java17.x86\_64"
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 \
 -Dsaffron.default.charset=UTF-16LE \
 -Dsaffron.default.collation.name='UTF-16LE$en\_US' \
 -Dsaffron.default.nationalcharset=UTF-16LE \
 -XX:MaxRAMPercentage=80.0 \
 -XX:+UnlockExperimentalVMOptions \
 -XX:InitiatingHeapOccupancyPercent=16 \
 -XX:+UseStringDeduplication \
 -XX:+G1EagerReclaimHumongousObjects \
 -XX:+G1EagerReclaimHumongousObjectsWithStaleRefs \
 -XX:G1HeapWastePercent=2 \
 -XX:G1MaxNewSizePercent=25 \
 -XX:G1MixedGCLiveThresholdPercent=15 \
 -XX:+UseG1GC"
ExecStart=/usr/lib/jdk/axiomjdk-java17.x86\_64/bin/java -jar app/app.jar
[Install]
WantedBy=multi-user.target

Далее от имени пользователя **root** необходимо выполнить команду по включению, запуску сервиса и проверке его статуса:

systemctl daemon-reload
systemctl enable prohibitor
systemctl start prohibitor
systemctl -l status prohibitor

### 2.5 Формирование конфигурационного файла Сервиса проверки полномочий

#### 2.5.1 Общие настройки конфигурационного файла

В конфигурационном файле application.yml задать:

* + идентификатор агента (мнемоника соответствующей ИС из ЛК УВ);
	+ ОГРН Агента (ОГРН организации владельца ИС из ЛК УВ);
	+ Идентификатор ключа CryptoPro: алиас контейнера CryptoPro. Необходимо использовать тот же ключ, что и на Агенте, с которым работает данный сервис проверки полномочий ([Раздел 4.3.2](#_4.3.2_Настройка_ключей));
	+ Хост и порт Агента СМЭВ4, с которым работает данный сервис проверки полномочий;

Значения agent.id, agent.ogrn должны совпадать с параметрами в конфигурационном файле Агента СМЭВ4 ([Раздел 4.3.1](#_4.3.2_Настройка_ключей)) agent.port должен иметь значение 8192, если не был переопределен в конфигурационном файле Агента СМЭВ4 ([Таблица 2.4](#_87c82fc79b8df105548e3fef0d53c1b6))

*# Общие настройки агента*
**agent**:
 *# Идентификатор агента*
 **id**: '\*\*\* ИДЕНТИФИКАТОР (МНЕМОНИКА) АГЕНТА \*\*\*'
 **ogrn**: '\*\*\* ОГРН АГЕНТА \*\*\*'
 **host**: '\*\*\* Адрес инстанса агента СМЭВ4 \*\*\*'
 **port**: '\*\*\* Порт инстанса агента СМЭВ4 \*\*\*'

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

|  |
| --- |
| Примечание: |
| Указывать параметр password не требуется, если используется сервис подписания и верификации сообщений (см [Раздел 2.5.3 Приложения Б](file:///C%3A%5CUsers%5CDStarkov%5CAppData%5CLocal%5CTemp%5C57c06f01-1d5a-4ea7-996f-9538e7c10e00_artifacts%20%288%29.zip.e00%5C_build%5Cdocx%5C%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B0%20%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D0%B0%20%D0%A1%D0%9C%D0%AD%D0%924.docx#_2.5.3_Настройка_подключения)) |

#### 2.5.2 Настройка подключения к базе данных:

Переменные db.\* указываются в разделе настроек подключения к PostgreSQL:

*# параметры подключения к базе и настройки пулла коннектов*
**db**:
 **host**: '\*\*\* hostname \*\*\*'
 **port**: '\*\*\* port \*\*\*'
 **user**: '\*\*\* username \*\*\*'
 **password**: '\*\*\* password \*\*\*'
 **database**: '\*\*\* database name \*\*\*'

#### 2.5.3 Настройка подключения к сервису подписания и верификации сообщений (Опционально)

Сервис проверки полномочий может работать как с локально установленным CryptoPro, так и без него, в этом случае за подписанием и верификацией сообщений он обращается к Агенту СМЭВ4. Для этого необходимо скопировать блок notarius в файл application.yml и заполнить параметр(ы) notarius.endpoints.target-host.

Пример раздела конфигурации:

**notarius**:
 **enabled**: true
 **endpoints**:
 - **target-host**: '\*\*\* IP АДРЕС СЕРВЕРА Агента СМЭВ4, либо Серера подписания и верификации сообщений (notarius) СМЭВ4 \*\*\*'
 **target-port**: 8696

#### 2.5.4 Настройка параметров, связанных с настройками времени жизни и блокировки пользовательских учетных записей

Пример раздела конфигурации:

**user**:
*# Задание повторного логина невозможно в течении конфигурируемого периода*
**login-uniq-period**: P3Y
*# Время бездействия пользователя, после которого, он будет разлогинен*
**inactive-timeout**: 5m
**password**:
 *# Максимальное время жизни пароля пользователя*
 **max-password-lifetime**: 60d
 *# Минимальное время жизни пароля пользователя*
 **min-password-lifetime**: 1d
 *# Период, в который нужно уведомлять пользователя об истечения срока действия пароля*
 **password-expire-notification-period**: 5d
**block**:
 *# Количество попыток аутентификации, после превышения которого пользователь временно блокируется*
 **max-failed-login-attempts**: 3
 *# Время блокировки при превышении разрешенного числа попыток аутентификации*
 **block-period**: 60m
 *# Период не активности, после которого пользователь блокируется*
 **inactive-period**: 45d
 *# Частота актуализации статусов пользователей в БД*
 **status-actualize-period**: 1m
**totp**:
 *# Размер секрета в байтах, на основе которого генерируется дополнительный код.*
 *# Размер секрета и алгоритм хэширования связаны:*
 *# - для SHA1 рекомендуется размер не менее 20 байт (160 бит);*
 *# - для SHA256 рекомендуется размер не менее 32 байт (256 бит);*
 *# - для SHA512 рекомендуется размер не менее 64 байт (512 бит).*
 **secretSize**: 20
 *# Алгоритм хэширования. Возможные значения: SHA1, SHA256, SHA512.*
 **hashingAlgorithm**: SHA1
 *# Количество цифр дополнительного кода (длина дополнительного кода).*
 **digits**: 8
 *# Период актуальности дополнительного кода.*
 **period**: PT30S

#### 2.5.5 Настройка передачи информации аудита в ГосТех (Опционально)

Для активации передачи информации аудита при работе Агента СМЭВ4 на платформе ГосТех, необходимо скопировать данный блок в файл application.yml и заполнить параметры gostech.audit.\* актуальными данными:

**gostech**:
 **enabled**: true
 **audit**:
 **host**: '\*\*\* audit\_server\_host \*\*\*'
 **port**: '\*\*\* audit\_server\_port \*\*\*'

### 2.6 Создание пользователя для работы с Сервисом проверки полномочий

Для создания пользователя в Сервисе проверки полномочий используется консольная утилита prohibitor-cli.jar входящая в состав дистрибутивного пакета. Для этого необходимо выполнить на сервере команду:

java -jar /distr/prohibitor/prohibitor-cli/prohibitor-cli.jar -l {{user\_login}} -p {{user\_password}} --db\_host {{db\_host}} --db\_port {{db\_port}} --db\_user {{db\_user}} --db\_password {{db\_password}} --db\_name {{db\_name}}

Где:

* {{user\_login}} - логин создаваемого пользователя;
* {{user\_password}} - пароль создаваемого пользователя;
* {{db\_host}} - IP адрес СУБД Postgres для Сервиса проверки полномочий;
* {{db\_port}} - порт СУБД Postgres для Сервиса проверки полномочий;
* {{db\_user}} - пользователь БД от Сервиса проверки полномочий;
* {{db\_password}} - пароль для БД от Сервиса проверки полномочий;
* {{db\_name}} - имя БД от Сервиса проверки полномочий.

## 3 Запуск консольной утилиты TOTP

**TOTP CLI** - это консольная утилита, предназначенная для генерации одноразовых паролей (TOTP, Time-based One-Time Passwords) на основе секретного ключа и текущего времени. Эта утилита необходима для аутентификации в сервисе проверки полномочий (Prohibitor).

### 3.1 Порядок загрузки данных и программ

Администратор УВ осуществляет развёртывание и настройку totp\_cli с помощью данного руководства.

#### 3.1.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Сервиса проверки полномочий (/distr/prohibitor/totp-cli):

* /distr/prohibitor/totp-cli/totp\_cli – исполняемый файл;

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

### 3.2 Предварительные операции

Перед запуском **totp\_cli** выполнить от имени пользователя **root** следующие действия:

1. Создать пользователя {{user}} и группу {{user\_group}}, под которым будет запускаться **totp\_cli**.
2. В домашней директории пользователя {{user}} создать поддиректорию local/bin
3. Переместить исполняемный файл **totp\_cli** в **/home/{{user}}/local/bin/**

mkdir -p /home/{{user}}/local/bin
cp /distr/prohibitor/totp-cli/totp\_cli /home/{{user}}/local/bin/totp\_cli
chmod +x /home/{{user}}/local/bin/totp\_cli

### 3.3 Запуск TOTP CLI

Для запуска TOTP CLI необходимо предварительно получить URL от Сервиса проверки полномочий. После получения URL запустить totp\_cli утилиту командой представленной ниже. Выполнять запуск необходимо от ранее созданного пользователя {{user}}

totp\_cli "{{URL}}"

## 4 Настройка и запуск Сервиса проверки полномочий с использованием Docker

Действия, требуемые для запуска Prohibitor под Docker, аналогичны действиям описанным в [Разделе 3.5](#_3.5_Настройка_и), за исключением следующих отличий:

* В качестве базового каталога используется /distr/prohibitor, либо любой другой, не совпадающий с уже используемым /distr/einfahrt
* Файл application.yml должен быть подготовлен согласно [Раздел 2.5 Приложения Б](#_2.5_Формирование_конфигурационного)
* Загружается подготовленный согласно [Приложению Г](#_Приложение_Г_Подготовка) образ Prohibitor
* В файле run\_agent.sh указываются следующие значения:

*# Название docker image указать здесь*
IMAGE=prohibitor:latest
*# Список используемых портов приложения, указывается в круглых скобках*
PORT\_LIST=(8692)

* В файле log-save.sh указывается

NAME="prohibitor"

* В командах docker start|stop указывается prohibitor вместо einfahrt

# Приложение В «Настройка и Установка Сервиса подписания и верификации сообщений Notarius» (опционально)

## 1 Описание конфигурационных файлов Сервиса подписания и верификации сообщений

**Notarius** - Сервис подписания и верификации сообщений предназначен для проверки подписи и подписания сообщений.

### 1.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Сервиса подписания и верификации сообщений.

* + /distr/notarius – Сервис подписания и верификации сообщений:
		- /distr/notarius/conf/customLogLevels.xml – файл описания настроек логирования;
		- /distr/notarius/conf/application.yml – заготовка конфигурационного файла.

Необходимо скопировать данные файлы в каталог /distr/notarius.

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.

### 1.2 Реестр изменений конфигурационного файла

[Таблица 9.1](#_bb50e14c87c176502e0110c055bba62c) содержит реестр изменений.

Таблица 9.1 Реестр изменений конфигурационного файла

|  |  |
| --- | --- |
| Версия | Перечень изменений (относительно предыдущей версии) |
| 3.16.0 | Начальная версия |
| 3.17.0 | Изменений нет |
| 3.18.0 | Изменений нет |
| 3.19.0 | Изменений нет |
| 3.20.1 | Изменений нет |
| 3.21.0 | Изменений нет |
| 3.22.0 | Изменений нет |

## 2 Настройка и запуск Сервиса подписания и верификации сообщений

Установка **Notarius** опциональна, требуется только если по требованиям ИБ Агенту СМЭВ4 не разрешается использовать встроенные средства криптографии.

### 2.1 Порядок загрузки данных и программ

Администратор УВ осуществляет развёртывание, запуск и настройку **Notarius** с помощью данного руководства.

#### 2.1.1 Состав и содержание дистрибутивного пакета

Состав дистрибутива Сервиса подписания и верификации сообщений (/distr/notarius):

* /distr/notarius/app/app.jar – исполняемый файл;

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

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

В случае, если Notarius устанавливается на машине, отличной от той где установлен Агент, перед запуском Notarius необходимо выполнить действия, описанные в [Разделе 3.2.2](#_3.2.2_Предварительные_операции):

|  |
| --- |
| Внимание: |
| Не требуется устанавливать отдельный экземпляр CryptoPro CSP для сервиса подписания и верификации сообщений, в следующих случаях:* Если Сервис подписания и верификации сообщений установлен на том же сервере, что и Агент СМЭВ4 в варианте «без использования Docker», в такой ситуации на данном сервере уже имеется установленная CryptoPro CSP;
 |

1. Выложить в каталог /distr/notarius конфигурационный файл application.yml, подготовленный согласно notaruis\_config.

### 2.3 Запуск Сервиса подписания и верификации сообщений

Убедитесь, что пользователь {{user}} имеет доступ к директориям, в которой установлен notarius: /distr/notarius.

Пример раздела конфигурации скрипта для запуска Notarius с использованием сервиса **systemd** Данный файл, с названием notarius.service, необходимо сохранить в каталог /etc/systemd/system/, скорректировав, при необходимости, пути к файлам.

[Unit]
Description="Service for notarius"
After=syslog.target

[Service]
Type=simple

WorkingDirectory=/distr/notarius
User={{user}} *#указать пользователя*
Group={{user\_group}} *#указать группу*

Environment="JAVA\_HOME=/usr/lib/jdk/axiomjdk-java17.x86\_64"
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 \
 -Dsaffron.default.charset=UTF-16LE \
 -Dsaffron.default.collation.name='UTF-16LE$en\_US' \
 -Dsaffron.default.nationalcharset=UTF-16LE \
 -XX:MaxRAMPercentage=80.0 \
 -XX:+UnlockExperimentalVMOptions \
 -XX:InitiatingHeapOccupancyPercent=16 \
 -XX:+UseStringDeduplication \
 -XX:+G1EagerReclaimHumongousObjects \
 -XX:+G1EagerReclaimHumongousObjectsWithStaleRefs \
 -XX:G1HeapWastePercent=2 \
 -XX:G1MaxNewSizePercent=25 \
 -XX:G1MixedGCLiveThresholdPercent=15 \
 -XX:+UseG1GC"
ExecStart=/usr/lib/jdk/axiomjdk-java17.x86\_64/bin/java -jar app/app.jar
[Install]
WantedBy=multi-user.target

Далее от имени пользователя **root** необходимо выполнить команду по включению, запуску сервиса и проверке его статуса:

systemctl daemon-reload
systemctl enable notarius
systemctl start notarius
systemctl -l status notarius

### 2.4 Формирование конфигурационного файла Сервиса подписания и верификации сообщений

#### 2.4.1 Общие настройки конфигурационного файла

В конфигурационном файле application.yml задать идентификатор ключа CryptoPro: **alias** контейнера CryptoPro.

Необходимо использовать тот же идентификатор ключа, что и на Агенте, с которым работает данный сервис проверки полномочий.

### 2.5 Настройка ключей CryptoPro CSP

Указать идентификатор и пароль контейнера ключа CryptoPro:

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

В случае, если идентификатор ключа CryptoPro содержит пробелы, его следует заключить в одинарные кавычки.

### 2.6 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 }}
 {...}

### 2.7 Настройка порта сервиса приема запросов

При необходимости изменения порта, на котором принимает запросы Notarius, измените номер порта в блоке параметров

*# Настройка Web-сервера*
**http**:
 **port**: 8696

### 2.8 Настройка Notarius для передачи метрик в Prometheus

Notarius 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 notarius отдаёт значения метрик*
 **endpointPort**: 8381

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

Изменение номера порта может потребоваться, например, в случае если порт уже занят каким-либо другим ПО.

## 3 Настройка и запуск подписания и верификации сообщений с использованием Docker

Действия, требуемые для запуска Notarius под Docker, аналогичны действиям описанным в [Разделе 3.5](#_3.5_Настройка_и), за исключением следующих отличий:

* + В качестве базового каталога используется /distr/notarius, либо любой другой, не совпадающий с уже используемым /distr/einfahrt;
	+ Файл application.yml должен быть подготовлен согласно [Раздел 2.4 Приложения В](#_2.4_Формирование_конфигурационного);
	+ Загружается подготовленный согласно [Приложению Г](#_Приложение_Г_Подготовка) образ Notarius;
	+ В файле run\_agent.sh указываются следующие значения:

*# Название docker image указать здесь*
IMAGE=notarius:latest
*# Список используемых портов приложения, указывается в круглых скобках*
PORT\_LIST=(8696 8381)

* В файле log-save.sh указывается

NAME="notarius"

* В командах docker start|stop указывается notarius вместо einfahrt

# Приложение Г Подготовка Docker образов для возможности запуска приложений под Docker (podman)

## 1 Подготовительные действия

Для создания Docker образов необходимы соблюдение следующих требований:

* + Рабочая станция, на которой установлена одна из сертифицированных ОС (ALT 8 SP Server 10, RedOS 7.3, Astra Linux 1.7 SE).
	+ Docker либо podman из дистрибутива ОС.
	+ Приобретенная пользователем лицензия на одну из указанных выше ОС; загруженный локально базовый Docker образ этой ОС, предоставленный производителем.
	+ Доступ с данной рабочей станции к репозиторию ОС, выбранной в качестве базовой для Docker образа, либо доступная в локальной сети копия репозитория. (В случае локальной копии необходимо внести изменения в указанный ниже пример Dockerfile. Подобная настройка делается администратором и выходит за рамки данного Руководства).
	+ Приобретенная пользователем лицензия на Axiom JDK 17-й версии, загруженный на локальный диск пакет Axiom JDK, соответствующий операционной системе базового Docker образа.
	+ Загруженный с сайта cryptopro.ru установочный пакет CryptoPro CSP 5R3, соответствующий операционной системе базового Docker образа.

## 2 Создание Docker образов

Для создания необходимых Docker образов выполняются следующие действия в указанном ниже порядке:

1. Распаковать полученный архив с дистрибутивом Агента СМЭВ4 в каталог /distr (имя каталога может быть другим, далее данное имя используется в качестве примера). В результате распаковки должна создаться следующая файловая структура:

distr
├── einfahrt
│   └── app
│   └── app.jar
├── notarius
│   └── app
│   └── app.jar
└── prohibitor
 ├── app
 │   └── app.jar
 ├── prohibitor-cli
 │   ├── application.yml
 │   ├── prohibitor-cli-x.xx.x-SNAPSHOT.jar
 │   └── README.md
 └── totp-cli
 └── totp\_cli

1. В каталоге distr создать подкаталог files; В подкаталог files выложить дистрибутив **Axiom JDK** и **CryptoPro CSP**. В примерах ниже используются пакеты, применяемые для ALT 8 SP Server 10, для других ОС имена пакетов, а также версии, могут отличаться.

distr
├── files
│   ├── linux-amd64.tgz # дистрибутив CryptoPro CSP
│   └── axiomjdk-jdk-certified17.0.6+11-linux-amd64.alt8.rpm # установочный пакет Axiom JDK
├── einfahrt
 ...

1. В каталоге distr создать файл с именем Dockerfile, содержащий приведенную ниже информацию.

|  |
| --- |
| Примечание: |
| Приведенный ниже пример Dockerfile использует ALT 8 SP Server 10 в качестве базовой ОС. В случае использования другой ОС, требуется внесение соответствующих корректив в Dockerfile: имя образа базовой ОС, используемый менеджер пакетов и т.п. Данные изменения производятся администратором, и выходят за рамки данного Руководства. Более подробную информацию можно получить в документации на используемую операционную систему. В примере ниже подразумевается что базовый образ ОС предварительно загружен локально. |

*# Based on official ALT 8 SP Server 10 image and certified Axiom JDK 17.0*
*#*
*# USAGE:*
*# START\_CMD can be redefined as axternal parameter. By default - "java -cp app/\* -jar app/app.jar"*
*# JDK\_JAVA\_OPTIONS can be EXTENDED by external parameter with the same name, but can't be redefined*
*# also checks presence of mounted external file certs/cacerts, if exist it will be used instead of default*

*# В следующей строке указать базовый образ выбранной операционной системы*
 FROM altsp:c10f1

 COPY files/ /tmp/

 RUN apt-get update **\**
 && apt-get install -y glibc-locales unzip openssl **\**
 && apt-get clean **\**
 && adduser -u 1000 -d /egov -m -U -l app **\**
 && usermod -L app **\**
 && mkdir -p /egov/java/app **\**
 && chown -R 1000:1000 /egov/java **\**
 && cd /tmp **\**
 && apt-get install -y ./axiomjdk-jdk-certified17.0.6+11-linux-amd64.alt8.rpm **\**
 && tar xzvf linux-amd64.tgz **\**
 && cd linux-amd64 **\**
 && apt-get update **\**
 && apt-get install -y 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 /tmp **\**
 && rm -rf axiomjdk-jdk-certified17.0.6+11-linux-amd64.alt8.rpm linux-amd64 linux-amd64.tgz **\**
 && echo -e '#!/bin/bash -l \n\
 [ -z "${START\_CMD}" ] && START\_CMD="java -jar app/app.jar" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-exports=java.base/sun.security.util=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-exports=java.base/sun.security.x509=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-exports=java.base/sun.security.pkcs=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-exports=java.base/sun.security.provider=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-exports=java.base/sun.security.tools.keytool=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-exports=java.base/sun.net=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-opens=java.base/jdk.internal.misc=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-opens=java.base/java.lang=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-opens=java.base/java.nio=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-opens=java.xml/org.w3c.dom=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} --add-opens=java.base/java.util=ALL-UNNAMED" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -Dio.netty.tryReflectionSetAccessible=true" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -Dsaffron.default.charset=UTF-16LE" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -Dsaffron.default.collation.name=UTF-16LE\$en\_US" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -Dsaffron.default.nationalcharset=UTF-16LE" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -XX:+UseContainerSupport" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -XX:InitialRAMPercentage=80.0" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -XX:MaxRAMPercentage=80.0" \n\
 DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -XX:+FlightRecorder" \n\
 [ -f certs/cacerts ] && DEFAULT\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} -Djavax.net.ssl.keyStore=certs/cacerts -Djavax.net.ssl.trustStore=certs/cacerts" \n\
 JDK\_JAVA\_OPTIONS="${DEFAULT\_JAVA\_OPTIONS} ${JDK\_JAVA\_OPTIONS}" \n\
 export JDK\_JAVA\_OPTIONS \n\
 [ -d /chgCfgTmp ] && cp -f /chgCfgTmp/\* /egov/java \n\
 exec ${START\_CMD} \n' >/docker-entrypoint.sh **\**
 && chmod 755 /docker-entrypoint.sh

 ENV PATH=*${*PATH*}*:/opt/cprocsp/bin/amd64

 WORKDIR /egov/java

 ENTRYPOINT ["/docker-entrypoint.sh"]

 RUN chown -R 1000 /etc/opt/cprocsp **\**
 && echo -e '[ -s /egov/csp.lic ] && /opt/cprocsp/sbin/amd64/cpconfig -license -set $(cat /egov/csp.lic)' >>/etc/profile.d/license\_cpro.sh

 *#############################################*
 *# APPLICATION specific #*
 *#############################################*

 *# При сборке образа, ниже должна быть раскомментирована только одна строка!*

 *# Раскомментировать при сборке образа Агента СМЭВ4*
 *#COPY einfahrt/app/app.jar app/app.jar*

 *# Раскомментировать при сборке образа Prohibitor*
 *#COPY prohibitor/app/app.jar app/app.jar*

 *# Раскомментировать при сборке образа Notarius*
 *#COPY notarius-ng/app/app.jar app/app.jar*

1. В созданном файле Dockerfile, ниже комментария APPLICATION specific, раскомментировать строку, относящуюся к тому компоненту, образ для которого требуется собрать. Например, для сборки Агента, раскомментировать строку COPY einfahrt/app/app.jar app/app.jar

|  |
| --- |
| Внимание: |
| Для каждой сборки должна быть раскомментирована только одна строка COPY в данном разделе |

1. Выполнить команду:

docker build . -t einfahrt:latest

Tag должен соответствовать имени собираемого образа приложения

1. Повторить пункты 4 и 5 для опциональных компонентов Notarius и Prohibitor, с раскомментированием соответствующей строки в Dockerfile и указанием корректного тега образа в команде docker build.
2. Сохранить созданные образы в файлы. Пример ниже - для Агента, при сохранении образов опциональных Prohibitor и Notarius указать соответствующие имена.

docker save einfahrt:latest | gzip >einfahrt.tgz

1. Скопировать полученные .tgz архивы на целевые сервера.

# Термины и определения

| Термин | Определение |
| --- | --- |
| Агент СМЭВ4, также Экземпляр ПО Агент (СМЭВ4) | Экземпляр ПО «Агент (СМЭВ4)», установленный в контуре ИС УВ и обеспечивающее сопряжение Экземпляров ПО «Витрина данных» и ИС УВ с Ядром СМЭВ4 |
| 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 СМЭВ4 в соответствии с загруженной в СМЭВ4 спецификацией OpenAPI |
| Инициатор (запроса) | Участник взаимодействия, который формирует исходный запрос к REST-сервису ИС Ответчика для передачи через СМЭВ4 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 |
| Подзапрос (данных) | SQL-запрос, который отправляется Ядром СМЭВ4 в адрес Поставщика данных |
| Поставщик (данных СМЭВ4) | Участник взаимодействия, являющийся источником данных для других участников и использующий СМЭВ4 для передачи данных |
| Потребитель (данных СМЭВ4) | Участник взаимодействия, получающий данные от Поставщиков данных для дальнейшей их обработки и использующий для передачи запросов и получения данных СМЭВ4 |
| Регламентированный SQL-запрос (РЗ) | SQL-запрос, выраженный в терминах Модели данных, загруженной в СМЭВ4, и зарегистрированный в Ядре СМЭВ4 под символической мнемоникой, используемой ИС Потребителя СМЭВ4 для выполнения регламентированного запроса. Может иметь параметры, значения которых задаются Потребителем данных СМЭВ4 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 |
| СМЭВ4 | Единый сервис доступа к данным СМЭВ, предназначенный для автоматизации процесса передачи данных и уведомлений об изменении данных между организациями или органами власти, ответственными за формирование и ведение информационных ресурсов, зарегистрированных в НСУД |
| 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 СМЭВ4 | Централизованная часть СМЭВ4, 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 СМЭВ4 и обеспечивающий обмен данными с другими Участниками взаимодействия с использованием СМЭВ4 в соответствии с загруженной в СМЭВ4 спецификацией OpenAPI |
| SQL | (англ. Structured Query Language) — декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных |

# История изменений документа

Таблица 12.1 История изменений документа

|  |  |
| --- | --- |
| Версия | Изменения документа |
| 3.4.0 | 1. Скорректирована команда, используемая при установке CryptoPro JCSP при наличии лицензионного кода CryptoPro JCSP:
2. Расширено описание решения типовых проблем для ошибки Ошибка вызова функции acquireContext:0x8009001a:
* Раздел 6.
1. Расширено описание настроек групп топиков при использовании нескольких схем Витрин данных
* Раздел 4.3.3.
 |
| 3.5.0 | 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 | 1. Обновлена версия агента.
2. Внесены изменения в описание конфигурационного файла.
 |
| 3.7.0 | 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 Агента СМЭВ4 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. 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. Добавлен раздел «3.3.12 Настройка типа аутентификации агента в ядре».
2. Обновлены примеры конфигураций.
3. Исправлены ошибки.
 |
| 3.9.1 | Изменений нет. |
| 3.10.0 | 1. Обновлен раздел описания конфигурационного файла (см. Раздел 4.3.5.1).
 |
| 3.11.1 | Изменений конфигурации нет. |
| 3.12.0 | В конфигурационном файле исключен параметр query.metadata.storeToDb.Добавлено описание метрики agent2broker\_connection. |
| 3.13.0 | В конфигурационном файле исключены параметры:* datamart-registration.datamarts.registrationFlow
* datamart-registration.datamarts.definedProfile

Из поставки исключен файл postgresql.jsonДобавлена поддержка операционных систем:* RedOS 7.3;
* AstraLinux 1.7;
* ALT SP Server 10.
 |
| 3.14.0 | 1. Удалено Приложение А «Добавление промежуточных сертификатов в ключ CryptoPro».
2. Добавлено Приложение А «Список метрик Агента СМЭВ4».
3. Добавлено Приложение Б «Настройка и установка Сервиса проверки полномочий».
4. Для работы Агента СМЭВ4 не требуется лицензия CryptoPro JCP.
 |
| 3.15.0 | 1. Изменен порядок разделов Руководства.
2. Доработка оформления документа по комментариям Заказчика.
 |
| 3.16.0 | 1. Обновлена Аннотация к настоящему Руководству
2. Добавлено приложение С «Настройка и Установка Сервиса подписания и верификации сообщений»
3. Добавлено приложение Д «Подготовка Docker образов для возможности запуска приложений под Docker (podman)»
 |
| 3.17.0 | Минорные исправления по документу |
| 3.18.0 | В приложении Г изменены пути |
| 3.19.0 | Минорные исправления по документу |
| 3.20.0 | Значение параметра query.default-query-timeout (Пользовательский таймаут для SQL-запросов) по умолчанию установлено в 20 секундИзменены способ включения и настройки логирования для платформы Гостех (см. Раздел 3.3)Добавлена возможность сохранения тел запросов во внешнюю систему (clickhouse) (см. Раздел 3.4) |
| 3.21.0 | Минорные исправления по документу |
| 3.22.0 | Добавлены разделы:* + 4.5 Переопределение значений портов REST и JDBC интерфейсов АгентаСМЭВ4;
	+ 4.3.15 Настройка таймаутов исполнения запросов по умолчанию (опционально)
 |

1. Перечисленные документы размещены на [портале ЕСКС](https://info.gosuslugi.ru/docs/section/%D0%A1%D0%9C%D0%AD%D0%92_4_%28%D0%9F%D0%9E%D0%94%D0%94%29/). [↑](#footnote-ref-1)
2. Данные порты могут быть переопределены посредством конфигурационного файла, см. [Раздел 4.5](#_4.5_Переопределение_значений), [Раздел 4.3.9](#_4.3.9_Настройка_организации) п.6 [↑](#footnote-ref-2)
3. В соответствии с разделами 2.3 и 2.5 документа «Методические рекомендации по работе с СМЭВ4», размещенном на [портале ЕСКС](https://info.gosuslugi.ru/docs/section/%D0%A1%D0%9C%D0%AD%D0%92_4_%28%D0%9F%D0%9E%D0%94%D0%94%29/) [↑](#footnote-ref-3)