

Программа для ЭВМ «Рутокен CLM»

(инструкция по использованию)

В данном документе описаны состав программного обеспечения, его установка, настройка и порядок работы пользователей и администраторов.

Содержание:

1. Общая информация.....	2
1.1 Термины, определения и сокращения.....	2
2. Компоненты системы.....	3
2.1 Схема взаимодействия компонентов.....	3
2.2 Центр управления.....	3
2.3 Веб-сервер.....	3
2.4 База данных.....	3
2.5 Агент CLM.....	4
2.6 Поддерживаемые центры сертификации.....	4
3. Быстрый старт.....	4
3.1 Шаг 1. Установка и настройка Центра управления.....	4
3.2 Шаг 2. Установка агентов.....	5
3.3 Шаг 3. Добавление хранилища.....	5
3.4 Шаг 4. Добавление сканера.....	5
3.5 Шаг 5. Добавление группы агентов.....	5
3.6 Шаг 6. Регистрация агентов.....	6
3.7 Шаг 7. Добавление центра сертификации.....	6
3.8 Шаг 8. Создание шаблона выпуска сертификатов.....	6
3.9 Шаг 9. Настройка автообновления.....	7
4. Работа в веб-интерфейсе.....	7
4.1 Авторизация.....	7
4.2 Раздел «Обзор».....	7
4.3 Раздел «Сертификаты».....	8
4.4 Раздел «Хранилища».....	9
4.5 Раздел «Шаблоны».....	9
4.6 Раздел «Автообновление».....	10
4.7 Раздел «Настройки».....	10
5. Конфигурация Центра управления.....	10
5.1 Настройки REST и gRPC.....	11
5.2 Настройки TLS и mTLS.....	11
5.3 Ключи аутентификации.....	11

5.4 Настройки базы данных.....	12
5.5 Начальная учётная запись администратора.....	12
5.6 Журналирование и аудит.....	12
6. Модель данных и масштабирование.....	12
7. Агенты CLM.....	13
7.1 Источники обнаружения сертификатов.....	13
7.2 Источники рабочей конфигурации.....	13
7.3 Файловое хранилище сертификатов.....	13
8. Настройка транспорта уведомлений.....	14
8.1 Электронная почта через SMTP.....	14
8.2 SMS через шлюз.....	14
9. Диагностика.....	14
9.1 Запуск утилит.....	14
9.2 Собираемые данные.....	15
9.3 Формат результата.....	15
10. Встроенная документация.....	15
11. Удаление.....	15

1. Общая информация

Рутокен CLM (далее — CLM) — программный комплекс из клиентской и серверной части. CLM обеспечивает централизованное управление жизненным циклом технологических и системных сертификатов, включая выпуск, учёт, хранение, мониторинг, продление, отзыв и аудит.

1.1 Термины, определения и сокращения

Термин	Определение
Агент	Локальный клиентский компонент, который устанавливается на сервер или устройство, взаимодействует с серверной частью CLM и автоматизирует работу с сертификатами.
Запрос на сертификат (CSR)	Закодированное сообщение, которое владелец ключа ЭП направляет в УЦ для получения сертификата. Содержит информацию о владельце сертификата.
Ключ проверки ЭП (открытый ключ)	Уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.
Ключ ЭП (закрытый ключ)	Уникальная последовательность символов, предназначенная для создания ЭП.
Сертификат ключа проверки ЭП	Электронный документ, выданный УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата.
Удостоверяющий центр, центр сертификации (УЦ, ЦС)	Программное обеспечение, которое создаёт и выдаёт сертификаты ключей проверки ЭП, а также отзывает, приостанавливает и возобновляет их действие.
Хранилище	Место на конечном устройстве, где хранятся файлы сертификата и ключевой пары и с которым работает установленный на устройстве агент.
Электронная подпись (ЭП)	Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом с ней связана и

Термин	Определение
	используется для определения лица, подписывающего информацию.

2. Компоненты системы

2.1 Схема взаимодействия компонентов

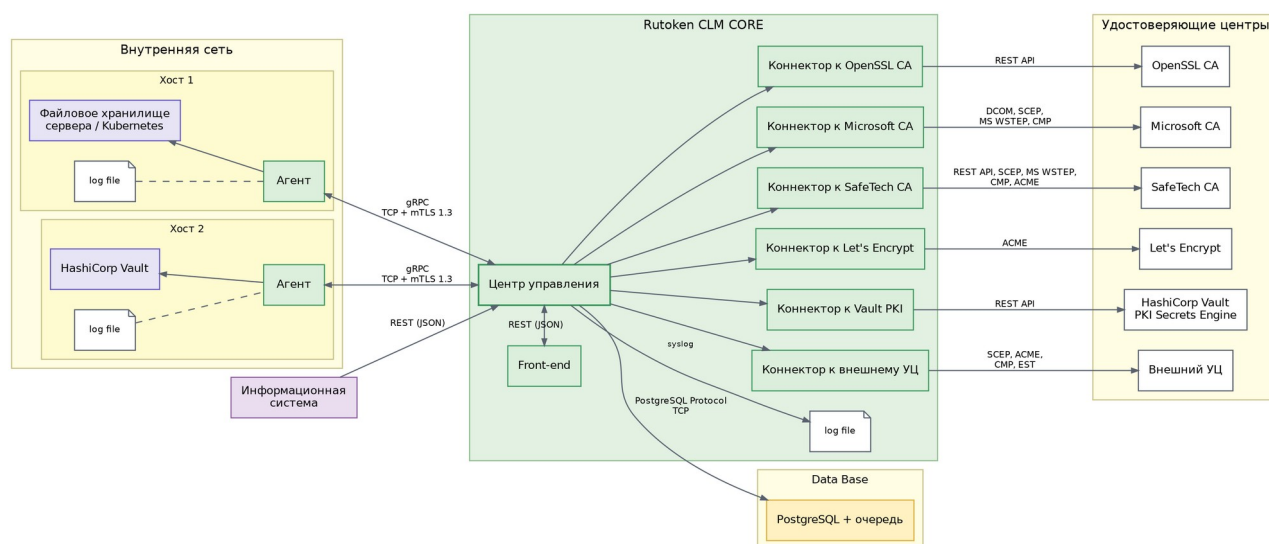


Рисунок 1. Взаимодействие агентов, Центра управления, базы данных и удостоверяющих центров

Центр управления отвечает за оркестрацию жизненного цикла сертификатов и хранит серверное состояние. Агенты выполняют работу непосредственно в той среде, где сертификаты обнаруживаются или устанавливаются. PostgreSQL, Kubernetes, HashiCorp Vault и внешние удостоверяющие центры не являются компонентами CLM: это зависимости или объекты интеграции.

2.2 Центр управления

Центр управления (CLM Service) — центральный монолитный сервер, который выполняет основную логику системы:

- хранит информацию о сертификатах и отслеживает их статусы и сроки действия;
- создаёт сценарии обновления и поиска сертификатов на конечных устройствах и управляет ими;
- взаимодействует с удостоверяющими центрами через коннекторы и со встроенным УЦ;
- управляет агентами, установленными на конечных устройствах.

Минимальные системные требования: ОС Debian 13, СУБД PostgreSQL 17.7, 4 ядра CPU, 4 ГБ RAM, 40 ГБ на диске. Предпочтительный порт — 7000.

2.3 Веб-сервер

Веб-сервер входит в состав Центра управления и построен на библиотеках РОСО C++. По протоколу HTTP или HTTPS он предоставляет веб-интерфейс CLM, REST API для веб-интерфейса и внешних информационных систем и встроенную документацию. Порт веб-сервера задаётся параметром `server.port` (по умолчанию 7000), адрес — параметром `server.url`.

2.4 База данных

База данных хранит информацию о сертификатах и их шаблонах, агентах, сервисах, устройствах, пользователях и организациях. Минимальные системные требования: ОС Debian 13, СУБД PostgreSQL 17.7, 2 ядра CPU, 4 ГБ RAM, 40 ГБ на диске.

Обратите внимание. если большая нагрузка на Центр управления не предполагается, база данных может располагаться на том же сервере.

2.5 Агент CLM

Агент — клиентская часть CLM, которая устанавливается на конкретное устройство и выполняет следующие задачи:

- поиск файлов ключей и сертификатов в каталогах, в секретах Kubernetes и в HashiCorp Vault;
- генерация ключевой пары и формирование запроса на сертификат;
- установка сертификатов в хранилище;
- обновление сертификатов в хранилищах по расписанию, установленному в Центре управления;
- обмен данными с Центром управления;
- запись выполненных действий в журнал.

Агент подключается к Центру управления по протоколу gRPC с взаимной аутентификацией (mTLS). Минимальные системные требования: ОС Debian 13, 1 vCPU, 2 ГБ RAM, 10 ГБ на диске. Предпочтительный порт — 50051.

2.6 Поддерживаемые центры сертификации

Для всех перечисленных центров сертификации доступны выпуск, обновление и отзыв сертификатов.

Центр сертификации	Протоколы подключения
OpenSSL CA	REST API
Microsoft CA	DCOM, SCEP, MS WSTEP, CMP
SafeTech CA	REST API, SCEP, MS WSTEP, CMP, ACME
Let's Encrypt	ACME
HashiCorp Vault PKI Secrets Engine	REST API
Любой внешний УЦ, поддерживающий стандартные протоколы	SCEP, ACME, CMP, EST

3. Быстрый старт

В разделе описаны установка и настройка системы с нуля: создание первого хранилища, настройка группы агентов со сканированием и создание плана автообновления. Для настройки отдельных компонентов используйте инструкции в соответствующих разделах.

3.1 Шаг 1. Установка и настройка Центра управления

Центр управления распространяется в виде DEB-пакета. Чтобы установить его:

1. Откройте терминал и перейдите в каталог с DEB-пакетом.
2. Установите Центр управления:

```
sudo dpkg -i rt-clm-service-<version>.deb
```

3. Настройте параметры сервера и базы данных:

```
sudo /opt/rutoken/rt-clm-service/bin/rt-clm-service-configure
```

В результате будет установлен и настроен Центр управления и создана база данных. Веб-интерфейс CLM будет доступен по адресу, указанному при конфигурации сервера.

3.2 Шаг 2. Установка агентов

Агент CLM распространяется в виде DEB-пакета и устанавливается на каждое устройство, на котором нужно отслеживать сертификаты и ключевые пары:

1. Откройте терминал и перейдите в каталог с DEB-пакетом.
2. Установите агент CLM:

```
sudo dpkg -i rt-clm-agent-<version>.deb
```

В результате будет установлен пакет `rt-clm-agent` и создан пользователь с таким же именем. Повторите шаги на всех устройствах. Затем создайте хранилища, задайте параметры сканирования и зарегистрируйте агенты в CLM.

3.3 Шаг 3. Добавление хранилища

Хранилище в CLM — это указание на место на конечном устройстве, где хранятся сертификаты и ключевые пары.

1. Откройте веб-интерфейс CLM и авторизуйтесь как администратор.
2. Перейдите в раздел **Хранилища** и нажмите **Добавить новое хранилище**.
3. Заполните поля:
 - o Название хранилища;
 - o Время замены файлов при обновлении;
 - o Тип хранилища.
4. Заполните поля, которые зависят от выбранного типа хранилища.
5. При необходимости выберите среду для хранилища.
6. Нажмите **Сохранить**.

Важно. каталог, HashiCorp Vault или пространство имён Kubernetes должны быть созданы на конечном устройстве заранее.

3.4 Шаг 4. Добавление сканера

Сканер задаёт, как агенты ищут сертификаты и ключевые пары в хранилище.

1. Перейдите в раздел **Хранилища → Сканирование** и нажмите **Добавить новый сканер**.
2. Заполните обязательные поля:
 - o Имя сканера;
 - o Глубина поиска;
 - o Среда;
 - o Интервал между сканированиями;
 - o Тип хранилища.
3. Заполните обязательные поля для выбранного типа хранилища.
4. Нажмите **Сохранить**.

Обратите внимание. при сканировании агенты автоматически создают хранилища с названием каталога, в котором найдены сертификаты.

3.5 Шаг 5. Добавление группы агентов

Группа агентов объединяет агентов с общими характеристиками, например с одними и теми же хранилищами.

1. Перейдите в раздел **Хранилища → Агенты** и нажмите **Добавить агентов**.
2. Заполните обязательные поля:
 - o Название группы;
 - o Количество агентов;

- o Время жизни данных инициализации агента.
- 3. Выберите хранилище, с которым будет связана группа, и сканер, которым будут пользоваться агенты.
- 4. Нажмите **Сохранить**.

Группа вместе с агентами появится в разделе **Агенты**. Для каждого агента будет создан файл первичной настройки, необходимый для регистрации.

3.6 Шаг 6. Регистрация агентов

1. Перейдите в раздел **Хранилища → Агенты**.
2. В строке агента нажмите кнопку загрузки, чтобы скачать файл первичной настройки (bootstrap).
3. Перенесите файл на устройство, на котором установлен агент.
4. Установите файл и выдайте пользователю агента права на него:

```
sudo install -m 0600 <название_файла>.json  
/etc/rt-clm-agent/agent_bootstrap.json  
sudo chown rt-clm-agent /etc/rt-clm-agent/agent_bootstrap.json
```

5. Перезапустите агент:

```
sudo systemctl restart rt-clm-agent
```

Статус агента в веб-интерфейсе изменится на **Зарегистрирован**. Агент получит от Центра управления информацию о хранилищах и сканерах и приступит к работе. После первого сканирования найденные сертификаты появятся в веб-интерфейсе CLM.

3.7 Шаг 7. Добавление центра сертификации

1. Перейдите в раздел **Настройки → Центры сертификации** и нажмите **Добавить центр сертификации**.
2. Заполните обязательные поля:
 - o Название центра сертификации;
 - o Тип центра сертификации;
 - o Доступность CRL и OCSP;
 - o Протокол подключения.
3. Заполните поля для выбранного типа центра сертификации и протокола, прикрепите сертификат центра сертификации.
4. При необходимости добавьте описание и нажмите **Сохранить**.

Новый центр сертификации появится в разделе **Центры сертификации** и будет доступен для выпуска сертификатов.

3.8 Шаг 8. Создание шаблона выпуска сертификатов

1. Перейдите в раздел **Шаблоны** и нажмите **Добавить новый шаблон**.
2. Заполните обязательные поля:
 - o Название шаблона;
 - o Центр сертификации;
 - o Использование ключа;
 - o Алгоритм ключей;
 - o Алгоритм подписи.
3. При необходимости заполните необязательные поля и нажмите **Создать шаблон**.

3.9 Шаг 9. Настройка автообновления

1. Перейдите в раздел **Автообновление** и нажмите **Создать план автообновления**.
2. Пройдите шаги мастера:
 - нажмите **Настроить** и выберите фильтры, чтобы найти нужные сертификаты;
 - выберите сертификаты, которые нужно обновлять автоматически;
 - выберите частоту обновления.
3. Нажмите **Создать план автообновления**.

План появится в разделе **Автообновление**. Для разных групп сертификатов можно создать несколько планов, например если одни сертификаты нужно обновлять чаще других.

4. Работа в веб-интерфейсе

4.1 Авторизация

1. Откройте веб-интерфейс CLM в браузере.
2. Введите логин и пароль.
3. Нажмите **Войти**.

Адрес и порт веб-интерфейса задаются при первичной настройке Центра управления. После входа откроется главная страница.

4.2 Раздел «Обзор»

Обзор — главная страница веб-интерфейса CLM. На ней находятся:

1. сводка по сертификатам, статус которых недавно изменился или скоро изменится: новые, истекающие, в процессе выпуска, ожидающие автообновления;
2. список удостоверяющих центров и их состояние; по нажатию на карточку УЦ открывается его описание и конфигурация;
3. диаграмма статусов всех сертификатов; по нажатию на статус открывается раздел **Сертификаты** с соответствующим фильтром.

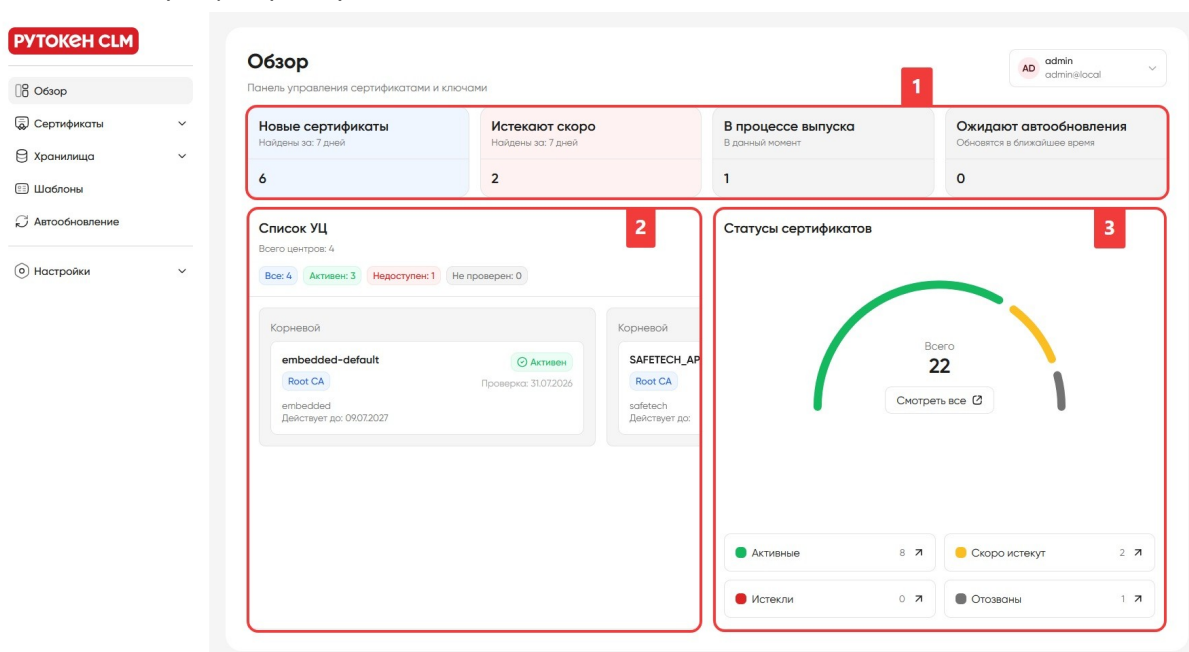


Рисунок 2. Главная страница веб-интерфейса CLM

4.3 Раздел «Сертификаты»

4.3.1 Выпуск нового сертификата

Обратите внимание. перед выпуском нужно создать шаблон (см. подраздел 4.5).

1. Откройте веб-интерфейс CLM и авторизуйтесь как администратор.
2. Перейдите в раздел **Сертификаты** и нажмите **Выпуск нового**.
3. Выберите способ выпуска:
 - о **По CSR (base64)** — если запрос уже сформирован: вставьте текст запроса и выберите шаблон;
 - о **Без запроса** — выберите шаблон, укажите, где будет сгенерирована ключевая пара (или выберите существующую) и где будет храниться сертификат.
4. Нажмите **Выпустить сертификат**.

4.3.2 Импорт имеющихся сертификатов

Сертификаты импортируются из CSV-файла со следующей структурой:

```
pem, templateName, disposition, rawRequest, revokedAt
```

Поле	Обязательность	Значение
pem	Обязательное	Сертификат в кодировке base64 вместе со строками BEGIN CERTIFICATE и END CERTIFICATE.
templateName	Необязательное	Имя шаблона сертификата.
disposition	Необязательное	Статус из Microsoft CA или текстовый статус: 20, DB_DISP_ISSUED, issued — статус берётся из сертификата; 21, DB_DISP_REVOKED, revoked — revoked; pending, active, denied, error, failed — unknown; expired — expired; valid — valid; suspended — suspended.
rawRequest	Необязательное	Исходный запрос на сертификат в кодировке base64.
revokedAt	Необязательное	Дата и время отзыва, если сертификат отозван.

1. Откройте веб-интерфейс CLM и авторизуйтесь как администратор.
2. Перейдите в раздел **Сертификаты** и нажмите **Импорт имеющегося**.
3. Прикрепите CSV-файл и нажмите **Импортировать**.

4.3.3 Просмотр информации о сертификате

В разделе **Сертификаты** найдите сертификат и нажмите на его название. В карточке сертификата указаны общая информация, SAN, хранилища сертификата и история его статусов.

4.3.4 Действия с сертификатами

В разделе **Сертификаты** доступны перевыпуск, приостановка, возобновление действия приостановленного сертификата, загрузка и отзыв сертификата.

- Для одного сертификата: найдите его с помощью фильтров или поиска, откройте карточку и нажмите кнопку нужного действия.
- Для нескольких сертификатов: отберите их фильтрами, отметьте флажками в левой колонке и нажмите кнопку действия справа от поисковой строки.

4.3.5 Запросы на сертификаты

Список запросов открывается в разделе **Сертификаты** → **Запросы**. Запрос может находиться в статусе **Выпущен**, **В процессе**, **Ошибка**, **Неизвестен** (CLM не удалось получить статус выпуска) или **Отменён**. Подробности о запросе открываются по нажатию на строку.

4.4 Раздел «Хранилища»

4.4.1 Управление хранилищами

Хранилища добавляются так, как описано в шаге 3 быстрого старта. Чтобы изменить хранилище, откройте его карточку в разделе **Хранилища**, нажмите **Редактировать**, внесите изменения и нажмите **Сохранить**.

4.4.2 Статусы агентов

- **Не зарегистрирован** — агент создан в CLM, но на устройство не передан файл первичной настройки или агенту не удалось с его помощью подключиться.
- **Зарегистрирован** — устройство с агентом успешно зарегистрировано. Зарегистрированный агент находится в состоянии **Онлайн**, если передавал сигнал о работоспособности в течение порогового времени, или **Офлайн**, если не передавал его дольше. Пороговое время задаётся параметром `notification.agent.offline_sec` и по умолчанию составляет 180 секунд (см. подраздел 5.1).

4.4.3 Управление агентами

Группы агентов добавляются и регистрируются так, как описано в шагах 5 и 6 быстрого старта. Чтобы переименовать агент, в разделе **Хранилища** → **Агенты** нажмите **Редактировать** в строке агента, введите новое имя и нажмите **Подтвердить**.

4.4.4 Управление сканерами

Сканеры добавляются так, как описано в шаге 4 быстрого старта. Чтобы изменить сканер, откройте его карточку в разделе **Хранилища** → **Сканирование**, нажмите **Редактировать**, внесите изменения и нажмите **Сохранить**.

4.5 Раздел «Шаблоны»

4.5.1 Добавление шаблона

Шаблон добавляется так, как описано в шаге 8 быстрого старта. Созданные шаблоны хранятся только в CLM и не передаются в центры сертификации.

Wildcard-сертификаты в HashiCorp Vault. если в шаблоне включена опция **Разрешение на выпуск wildcard**, символ `*` не подставляется автоматически. Укажите его явно в Common Name, например `*.example.com`.

4.5.2 Импорт шаблонов из центра сертификации

Импорт возможен из Microsoft CA (подключение по MS WSTEP с аутентификацией NTLM или Kerberos), SafeTech CA и HashiCorp Vault PKI Secrets Engine (подключение по REST API). Из внешних УЦ, подключённых по стандартным протоколам (Generic Root CA), импорт невозможен: эти протоколы предназначены только для выпуска сертификатов.

1. Откройте веб-интерфейс CLM и авторизуйтесь как администратор.
2. Перейдите в раздел **Шаблоны** и нажмите **Импортировать шаблоны**.
3. Выберите центр сертификации и укажите название шаблона. Если название не указано, будут импортированы все шаблоны центра сертификации.
4. Нажмите **Импортировать**.

4.5.3 Изменение и удаление шаблонов

Чтобы изменить шаблон, откройте его карточку, нажмите **Редактировать**, внесите изменения и нажмите **Сохранить**. Чтобы удалить один шаблон, нажмите **Удалить** в его карточке; чтобы удалить несколько — отметьте их флажками и нажмите **Удалить** справа от поисковой строки, затем подтвердите удаление.

4.6 Раздел «Автообновление»

Планы автообновления создаются так, как описано в шаге 9 быстрого старта. Чтобы переименовать план, отметьте его флажком, нажмите **Редактировать** справа от поисковой строки, измените название и нажмите **Сохранить**.

4.7 Раздел «Настройки»

4.7.1 Центры сертификации

Центры сертификации добавляются так, как описано в шаге 7 быстрого старта. Чтобы изменить конфигурацию, откройте карточку центра, нажмите **Редактировать**, внесите изменения и нажмите **Сохранить**. Чтобы удалить центр сертификации, нажмите **Удалить** в его карточке и подтвердите удаление.

Важно. удалить центр сертификации можно, только если через него в CLM не выпускались сертификаты.

4.7.2 Уведомления

Важно. перед настройкой уведомлений по электронной почте и SMS настройте SMTP-сервер и SMS-шлюз через REST API (см. раздел 8).

1. Откройте веб-интерфейс CLM и авторизуйтесь как администратор.
2. Перейдите в раздел **Настройки** → **Уведомления** и нажмите **Добавить новое правило**.
3. Заполните обязательные поля:
 - Название правила;
 - Тип отправки;
 - Событие.
4. Если правило должно применяться только к отдельным шаблонам, выберите их.
5. Добавьте получателей: создайте нового или выберите из общего списка. Общий список формируется из ранее заведённых получателей и может загружаться из каталога LDAP (интеграция настраивается через API).
6. При необходимости добавьте текст уведомления и нажмите **Сохранить**.

Чтобы изменить правило, отметьте его флажком, нажмите **Редактировать**, внесите изменения и нажмите **Сохранить**. Изменения применяются со следующего срабатывания правила.

5. Конфигурация Центра управления

Рабочая конфигурация располагается в файле `/etc/rt-clm-service/rt-clm-service.properties`. Утилита `rt-clm-service-configure` задаёт начальные параметры подключения к базе данных; настройки TLS, аутентификации, журналирования и интеграций задаёт администратор. Ниже приведены основные параметры, а не полный их перечень.

Важно. файл конфигурации содержит пароль базы данных и может содержать другие учётные данные. Защищайте его как секрет.

5.1 Настройки REST и gRPC

Параметр	По умолчанию	Назначение
<code>server.port</code>	7000	Порт HTTP(S) для REST API, веб-интерфейса и встроенной документации.
<code>server.url</code>	localhost	Имя узла или URL, публикуемый для пользователей, интеграций и агентов.
<code>grpc.port</code>	50051	Порт gRPC для зарегистрированных агентов.
<code>grpc.tls.serverName</code>	clm.local	Имя сервера TLS, которое ожидают агенты.
<code>agent.command_poll_interval_sec</code>	1	Резервный интервал опроса очереди команд для агента без назначенного профиля, с. Значение из профиля агента (AgentProfile) имеет приоритет.
<code>notification.agent.offline_sec</code>	180	Время без регистрации или сигнала о работоспособности, после которого агент считается недоступным, с. Регистрация агента при этом не сбрасывается.

REST- и gRPC-эндпоинты должны быть доступны с узлов, на которых развёрнуты агенты. Публикуемые имена следует согласовать с DNS, маршрутизацией и идентификаторами в TLS-сертификатах. Значение `notification.agent.offline_sec` следует держать с запасом выше интервала отправки сигнала о работоспособности, заданного в профиле агента.

5.2 Настройки TLS и mTLS

Параметр	По умолчанию	Назначение
<code>openSSL.server.certificateFile</code>	rt-clm-service.pem	Сертификат HTTPS для REST.
<code>openSSL.server.privateKeyFile</code>	rt-clm_tls.key	Закрытый ключ HTTPS для REST.
<code>openSSL.server.caConfig</code>	rt-clm-service_rootcert.pem	Доверенные сертификаты для TLS в REST.
<code>grpc.tls.certFile</code>	rt-clm-service.pem	Сертификат сервера gRPC.
<code>grpc.tls.keyFile</code>	rt-clm_tls.key	Закрытый ключ сервера gRPC.
<code>grpc.tls.caFile</code>	rt-clm-service_rootcert.pem	Удостоверяющий центр для проверки агентов по mTLS.

Файлы по умолчанию располагаются в каталоге `/etc/rt-clm-service/`. Перед вводом в эксплуатацию замените тестовые TLS-материалы: идентификаторы в сертификатах должны соответствовать значениям `server.url`, `grpc.tls.serverName` и адресам, которые используют клиенты.

5.3 Ключи аутентификации

Токены доступа подписываются ключом RSA: закрытый ключ задаётся параметром `auth.jwt_private_key_file` (по умолчанию `rt-clm-jwt-private.pem`), открытый — параметром `auth.jwt_public_key_file` (`rt-clm-jwt-public.pem`). Относительные пути по умолчанию раскрываются в рабочем каталоге службы `/var/lib/rt-clm-service`. Все экземпляры Центра управления в одной инсталляции должны использовать одинаковый ключевой материал.

5.4 Настройки базы данных

Параметр	Значение из пакета	Назначение
DBMS	psql	Тип СУБД (PostgreSQL).
SQL.server.address	localhost	Узел PostgreSQL.
SQL.server.port	5432	Порт PostgreSQL.
SQL.server.dataBase	clm_test	Имя базы данных.
SQL.server.uid	postgres	Учётная запись СУБД. В эксплуатации используйте отдельную служебную учётную запись.
SQL.server.pwd	тестовое значение	Пароль базы данных.
SQL.server.pool_size	16	Размер пула подключений для одного процесса Центра управления.

5.5 Начальная учётная запись администратора

Параметр	Значение из пакета	Назначение
auth.default.seed_enabled	true	Создание начальной области (realm) и учётной записи администратора.
auth.default.seed.realm	default	Имя создаваемой области.
auth.default.seed.username	admin	Имя учётной записи администратора.
auth.default.seed.password	change-me	Пароль-заглушка.
auth.default.seed.role	admin	Назначаемая роль.
auth.default.seed_reset_password_on_start	true	Сброс пароля учётной записи при каждом запуске.
auth.default.seed_force_role	true	Принудительное назначение роли при запуске.

Перед вводом в эксплуатацию. замените тестовые учётные данные. После получения первичного доступа отключите сброс пароля при запуске, чтобы перезапуск службы не восстанавливал известный пароль.

5.6 Журналирование и аудит

Метки времени в журналах Центра управления и агента указываются в UTC без суффикса часового пояса.

Группа параметров	Значение из пакета	Назначение
logger.server.*	Запись в файл	Приёмник журналов службы, уровень детализации, ротация и настройки syslog.
audit.syslog.*	Отключено	Передача событий аудита и безопасности через syslog.
audit.nats.*	Отключено	Рассылка событий аудита и безопасности через NATS без гарантии доставки.
auto_renewal.*	Включено	Планировщик автоматического перевыпуска.

Запрещено журналировать. закрытые ключи, токены, пароли базы данных, содержимое файлов первичной настройки агентов, токены Vault и учётные данные Kubernetes.

6. Модель данных и масштабирование

PostgreSQL хранит всё состояние Центра управления: агентов, реестр сертификатов, цели сканирования, шаблоны, заявки жизненного цикла, привязки хранилищ, очереди и данные аудита.

Центр управления не хранит собственного состояния: асинхронная работа между экземплярами координируется через очереди в базе данных. Поэтому для масштабирования можно запустить несколько экземпляров Центра управления над одной базой данных. Все экземпляры одной инсталляции

должны использовать одну схему и базу данных, одну ключевую пару для подписи токенов, одинаковые TLS-идентификаторы, публикуемые адреса и совместимую конфигурацию.

Внимание. экземпляры, подключённые к разным базам данных, образуют независимые инсталляции CLM. Повторная инициализация базы данных уничтожает хранящееся в ней состояние и не является процедурой масштабирования или обновления.

7. Агенты CLM

Агент регистрируется с помощью файла первичной настройки (bootstrap), который формирует Центр управления. Файл содержит начальные адреса подключения, токен и данные для регистрации, но не содержит настроек обнаружения и хранилищ. После регистрации агент получает рабочую конфигурацию от Центра управления и сохраняет последнюю принятую версию локально.

7.1 Источники обнаружения сертификатов

Источник	Назначение	Необходимый доступ
Файловая система	Поиск сертификатов в заданных каталогах на узле с агентом.	Права на чтение и обход заданных путей.
Kubernetes внутри кластера	Поиск сертификатов в секретах Kubernetes из пода с агентом.	Права ServiceAccount на получение списка секретов в пространстве имён.
Kubernetes вне кластера	Поиск сертификатов через kubeconfig на Linux-узле с агентом.	Файл kubeconfig, сетевой доступ к API и ограниченные права на секреты.
HashiCorp Vault	Поиск сертификатов в заданных разделах Vault KV или PKI.	Адрес Vault, токен с ограниченными правами, пространство имён (если используется), проверяемый TLS.

Для работы с Vault KV указываются адрес Vault, токен с ограниченными правами, пространство имён Vault Enterprise (необязательно), версия механизма секретов KV, точка монтирования и путь. Обнаружение и хранение — разные функции, для каждой следует выдавать минимально необходимые права. Поиск в Vault PKI включается явно: пока точки монтирования PKI не настроены, запросы к PKI не выполняются.

7.2 Источники рабочей конфигурации

Источник	Что определяет
Файл первичной настройки	Начальные адреса для регистрации, токен и исходные данные агента.
Профиль агента (AgentProfile)	Сигнал о работоспособности, опрос, переподключение, журналирование и телеметрию.
Конфигурация агента	Назначенные привязки обнаружения, хранилищ и расписания, которые формирует Центр управления.
Цели сканирования	Настройки обнаружения для файловой системы, Kubernetes или Vault.
Хранилища сертификатов	Размещение и доступ для операций жизненного цикла сертификатов.

Внимание. не правьте сохранённую конфигурацию на стороне агента вручную: очередное обновление от Центра управления её перезапишет.

7.3 Файловое хранилище сертификатов

Файловые сканеры находят сертификаты в заданных каталогах на узле с агентом, а файловые хранилища используются для размещения сертификатов при операциях жизненного цикла. На каждом узле должны быть заранее подготовлены нужные каталоги и минимально достаточные права доступа для непривилегированного пользователя агента.

8. Настройка транспорта уведомлений

Правила уведомлений ссылаются на переиспользуемые транспорты доставки и не хранят параметры подключения к SMTP или SMS внутри себя.

8.1 Электронная почта через SMTP

1. Создайте конфигурацию SMTP через метод `/smtpserver`.
2. Проверьте аутентификацию через `/smtpserver/test/login`.
3. Отправьте тестовое сообщение через `/smtpserver/test/send-email`.
4. Укажите имя сохранённой конфигурации в параметре `smtpServer` канала электронной почты.

Имя конфигурации, адрес и порт обязательны. Аутентификацию можно не настраивать, только если SMTP-сервер явно разрешает отправку без неё с узла Центра управления. Не отключайте проверку сертификата сервера, чтобы обойти неверно настроенное доверие.

8.2 SMS через шлюз

Тип шлюза	Модель доставки
http	API провайдера по HTTP или HTTPS с подстановочными параметрами <code><phone></code> и <code><message></code> .
smpp	Подключение по протоколу SMPP к SMS-центру.
smtp	Доставка по схеме «электронная почта → SMS» через существующую конфигурацию SMTP.

Создайте и проверьте шлюз до того, как ссылаться на него из правила (параметр `channels[].smsGateway`). SMS отправляются асинхронно; состояние отправок можно посмотреть через метод `/notification/delivery`.

9. Диагностика

Для диагностики предусмотрены две утилиты командной строки: `rt-clm-service-diagnostics` собирает данные на сервере Центра управления, `rt-clm-agent-diagnostics` — на узле с агентом. При инциденте общего характера сначала запустите утилиту на сервере; если данных недостаточно — на узле, где наблюдается проблема. Если один из этапов сбора завершается ошибкой, утилита продолжает работу и помечает недоступные данные в отчёте.

Обратите внимание. утилиты поставляются отдельными необязательными пакетами. Их установка не требует остановки или перезапуска CLM.

9.1 Запуск утилит

Утилиты запускаются от `root` или от непривилегированного пользователя; в первом случае собираются более полные данные. Без аргументов утилита создаёт архив в текущем каталоге, флаг `--output` задаёт путь:

```
rt-clm-service-diagnostics --output /var/tmp/service-report.tar.gz
rt-clm-agent-diagnostics --output /var/tmp/agent-report.tar.gz
```

Флаг / код	Значение
<code>--help</code>	Справка по использованию.
<code>--version</code>	Версия формата диагностики.
<code>--capabilities</code>	Доступные сборщики данных и их ограничения.
Код 0	Отчёт собран полностью, все проверки успешны.
Код 1	Отчёт собран, но часть проверок завершилась ошибкой или данные были недоступны.
Код 2	Некорректные аргументы командной строки.
Код 3	Критическая ошибка или сбой при создании архива.

9.2 Собираемые данные

Утилиты не считывают закрытые ключи, секреты и другую чувствительную информацию.

На сервере: конфигурация службы без паролей и ключей; сведения о процессе, systemd и лимитах ресурсов; сетевые настройки и TLS-проверки; журналы службы и события ОС; состояние PostgreSQL (доступность, версия, настройки, схема, подключения, блокировки, репликация, статистика); список и активность агентов; журналы агентов, сохранённые в базе данных; статусы сертификатов, аудит и уведомления.

На узле с агентом: файл первичной настройки и состояние агента; сведения о хосте (файловая система, права, место на диске, DNS, сеть); настройки сканирования и хранения; состояние сертификатов и запросов в сканируемых каталогах; журналы агента; для Kubernetes — проверки контекста, RBAC, подов, узлов и томов; для Vault — проверки DNS, TLS, состояния Vault, прав токена и типов механизмов KV и PKI.

9.3 Формат результата

Элемент архива	Содержание
manifest.tsv	Список артефактов, статус их сбора и хеш SHA-256.
checks.tsv	Статус каждой проверки: успех, ошибка, пропуск, недоступно.
data/	Собранные данные.

Анализ удобно начинать с файла checks.tsv: в нём видно, какие проверки не прошли и почему.

10. Встроенная документация

Центр управления публикует документацию по адресу `https://<clm-host>:<clm-port>/docs/`:

Путь	Содержание
/docs/deployment/	Установка, регистрация агентов и приёмка развёртывания.
/docs/platform/	Рабочая конфигурация и эксплуатация.
/docs/filesystem/	Настройка сканера файловой системы Linux и файлового хранилища сертификатов.
/docs/vault/	Интеграция с HashiCorp Vault KV.
/docs/external-ca/	Протоколы внешних удостоверяющих центров.
/docs/redocly.html	Справочник REST API.
/docs/swagger.html	Интерактивный браузер OpenAPI.
/docs/release_notes.txt	Список изменений.

11. Удаление

Компоненты CLM удаляются стандартными средствами пакетного менеджера. Чтобы удалить агент, выполните на устройстве с агентом одну из команд:

```
sudo apt remove rt-clm-agent
sudo dpkg -r rt-clm-agent
```

Чтобы удалить Центр управления, выполните на сервере одну из команд:

```
sudo apt remove rt-clm-service
sudo dpkg -r rt-clm-service
```