Установка и эксплуатация программного обеспечения «**IDM Crosstech Advanced Edition**»

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

Сокращение	Расшифровка
AD	Active Directory
CPU	Central Processing Unit
IDM CAE	Identity Management Crosstech Advanced Edition
IG	Identity Governance
LDAP	Lightweight Directory Access Protocol
RM	Request Management
БД	База данных
ИС	Информационная система
ОЗУ	Оперативная память
ОС	Операционная система
УЗ	Учётная запись

Термин	Определение
Пользователь	Структура данных в IDM CAE, описывающая человека
Ресурс	Сторонние ИС, в которых IDM CAE управляет учётными записями. Кроме того, ресурсами считаются все ИС, подключенные к IDM CAE в разделе Resources
Роль	Набор прав доступа
Учётная запись	Хранимая в ИС совокупность данных о пользователе

1. ОБЩИЕ СВЕДЕНИЯ

1.1. О документе

Руководство по развёртыванию содержит информацию для выполнения развёртывания IDM CAE в инфраструктуре компании. В руководстве представлена инструкция по установке и первоначальной настройке решения IDM CAE.

1.2. Об IDM CAE

IDM CAE предоставляет возможность централизованного управления учетными записями и правами пользователей различных информационных систем (далее – ИС) компании с помощью ключевых модулей: Base, Monitoring, Identity Governance (далее – IG) и Request Management (далее – RM). IDM CAE получает данные о работниках и организационно-штатной структуре из доверенных источников, таких как системы кадрового учёта, а также информацию о пользователях и их полномочиях из других ИС компании.

В IDM CAE настраиваются процессы управления доступом к ИС. Эти процессы могут быть как полностью автоматизированными (например, автоматическая блокировка доступа при увольнении), так и требовать вмешательства определённых работников (например, для согласования запросов).

Пользователи взаимодействуют с IDM CAE через веб-интерфейсы модулей. Доступ к различным функциям и объектам IDM CAE (разделам веб-интерфейса, отчётам и т.п.) может быть различным

2. АРХИТЕКТУРА

IDM CAE состоит из следующих основных компонентов (модулей):

- Base;
- Monitoring;
- IG;
- RM.

2.1. Описание компонентов

2.1.1. Модуль Base

Модуль Base состоит из двух компонентов:

- Provisioning Management;
- Workflow Management.

Компонент Provisioning Management в составе IDM CAE предоставляет основную функциональность для управления идентификацией и авторизацией пользователей, автоматический сбор информации об активности пользователей, контроль безопасности доступа к ресурсам, анализ и отчётность.

Компонент Workflow Management позволяет автоматизировать бизнес-процессы, а также определять и контролировать последовательность выполнения задач, управлять процессами с высокой степенью гибкости и при этом обеспечивать соответствие правилам и политикам безопасности.

2.1.2. Модуль Monitoring

Модуль Monitoring обеспечивает централизованный мониторинг процессов IDM CAE и контроль исполняемых процессов

в части модификации атрибутов УЗ IDM CAE, позволяет консолидировать информацию о кадровой принадлежности и правах доступа пользователей IDM CAE, а также обеспечивает сбор данных из IDM CAE непосредственно через хранилище данных.

Модуль Monitoring состоит из следующих компонентов:

- подсистемы сбора и обработки данных на базе ETL-инструмента Logstash и парсеров;
- подсистемы визуализации и мониторинга.

2.1.3. Модуль IG

Модуль IG позволяет выявлять конфликты полномочий. Цель работы модуля заключается в обеспечении информационной безопасности и соответствии регуляторным требованиям в рамках действующих бизнес-процессов компании.

Данный модуль может выявлять конфликты полномочий разных типов:

- между полномочиями по матрице конфликтных ролей;
- между полномочиями и подразделением работника.

2.1.4. Модуль RM

Модуль RM позволяет обрабатывать синхронные и асинхронные запросы с конкретными методами и направлять запросы на выполнение в IDM CAE (компоненты Provisioning Management и Workflow Management) с последующим получением результата. В своей работе модуль RM использует Apache Kafka в качестве брокера сообщений. Взаимодействие с внешней ИС может осуществляться через REST API.

2.2. Схема взаимодействия компонентов

Вариант взаимодействия компонентов IDM CAE представлен в Приложении 1.

Таблица сетевых соединений представлена в таблице 1.

Таблица 1 – Таблица сетевых взаимодействий

№	Источник	Назначение	Протокол / порт	Описание
1.	Пользователь/ администратор	IDM CAE (Nginx)	443 / https	Доступ в веб-интерфейс IDM CAE
2.	Nginx	IDMCAE Provisioning Management	8080 / http	Доступ в веб-интерфейс компонента Provisioning Management
3.	Nginx	IDMCAE Workflow Management	8081 / http	Доступ в веб-интерфейс компонента Workflow Management / модуля IG
4.	Nginx	IDMCAE-MONITORING	8082 / http	Доступ в веб-интерфейс модуля Monitoring
5.	IDMCAE Provisioning Management	IDMCAE Workflow Management	8081 / http	Запуск бизнес-процессов
6.	IDMCAE Workflow Management	IDMCAE Provisioning Management	8080 / http	Отправка результатов выполненного бизнес-процесса
7.	IDMCAE Provisioning Management IDMCAE Workflow Management IDMCAE-IG IDMCAE-RM	PostgreSQL	5432 / jdbc	Сохранение и работа с данными IDM CAE
8.	IDMCAE-MONITORING	PostgreSQL (Monitoring)	5432 / psycopg2	
9.	IDMCAE-RM	Apache Kafka	49443 / tcp	Связь с брокером сообщений по защищённому соединению
10.	Apache Kafka	IDMCAE-RM	49443 / tcp	
11.	IDMCAE Workflow Management (RM-делегаты)	Apache Kafka	49443 / tcp	
12.	Apache Kafka	IDMCAE Workflow Management (RM-делегаты)	49443 / tcp	

№	Источник	Назначение	Протокол / порт	Описание
13.	Logstash	PostgreSQL (Monitoring)	5432 / jdbc	Обработка данных
14.	PostgreSQL (IG)	Logstash	5432 / jdbc	
15.	PostgreSQL (Workflow Management)	Logstash	5432 / jdbc	

3. МАСШТАБИРОВАНИЕ И ВАРИАНТЫ РАЗВЁРТЫВАНИЯ РЕШЕНИЯ

3.1. Рекомендации по выбору конфигурации развёртывания

Продукт можно развернуть в одной из конфигураций:

- All-in-One;
- кластерная.

Данное руководство описывает процедуру развёртывания для конфигурации All-in-One. Последовательность шагов для развёртывания в кластерной конфигурации формируется на этапе проектирования в рамках внедрения.

Дистрибутив содержит следующие модули:

- Base;
- Monitoring;
- IG;
- RM.

3.2. Масштабирование

Масштабирование в All-in-One и кластерной конфигурациях является возможным. Последовательность шагов для масштабирования формируется на этапе проектирования в рамках внедрения.

4. РАЗВЁРТЫВАНИЕ IDM CAE

4.1. Конфигурация развёртывания All-in-One

4.1.1. Аппаратные требования для конфигурации All-in-One

Ниже перечислены минимальные аппаратные требования для поставляемого дистрибутива в рамках релиза:

- CPU: 8 ядер;
- ОЗУ: 16 ГБ;
- объём дискового пространства: 100 ГБ.

4.1.2. Программные требования для конфигурации All-in-One

Для развёртывания IDM CAE требуется операционная система РЕД ОС 8 (2024). При этом при развёртывании IDM CAE на РЕД ОС 8 должен быть установлен Python версии 3.11 (поставляется вместе с дистрибутивом).

Ниже перечислены поддерживаемые браузеры (последних версий):

- Google Chrome;
- Microsoft Edge;
- Яндекс Браузер;
- Opera;
- Mozilla Firefox.

4.1.3. Подготовка к развёртыванию конфигурации All-in-One

1. Загрузите предоставляемый дистрибутив в виде архива D-1.4.1.tar.gz в любую удобную директорию и убедитесь в наличии

УЗ root, так как установка выполняется именно от данной УЗ с повышенными привилегиями.

2. Убедитесь, что в директории `/tmp` выделено более 5 ГБ доступного пространства, так как временные файлы при установке помещаются в указанную директорию. Если размер не соответствует, выполните команду

```
sudo mount -o remount,size=5G /tmp
```

3. Перед установкой поместите файл активации лицензии с наименованием license.lic во временную директорию `/tmp`:

```
cp license.lic /tmp
```

4. В случае, если дистрибутив устанавливается как обновление с более старой версии:
    - удалите в пользовательском интерфейсе модуля Monitoring все дашборды, графики, датасеты и подключения к БД, связанные с модулем IG;
    - в модуле IG завершите все запущенные экземпляры процесса IG/Управление PM и MKP.

4.1.4. Развёртывание конфигурации All-in-One

При установке дистрибутива происходит автогенерация сертификатов, во время которой создаётся общий truststore `idmcae-truststore.jks` по пути `/opt/idmcae/certs/`.

Для установки дистрибутива выполните следующие шаги:

1. Создайте папку

```
sudo mkdir /opt/distro
```

2. Переместите архив в созданную папку и перейдите в эту папку

```
cd /opt/distro
```

3. Выполните разархивирование в директорию /opt/distro с помощью команды

```
sudo tar -xvf D-1.4.1.tar.gz
```

4. Запустите скрипт установки и настройки сервисов с помощью команды

```
sudo ./install.sh cfg.yml
```

Во время выполнения установки будет запрошен пароль для superuser, данный пароль будет использоваться для всех технологических УЗ от компонентов в СУБД, в том числе и для технологических УЗ postgres, а также для административной локальной УЗ модуля Monitoring (**при вводе пароля не используйте символы, допускается использование только букв и цифр!**).

4.1.5. Обновление версии IDM CAE

При обновлении версии IDM CAE необходимо указывать пароль от суперпользователя, который был использован при установке. Если пароль / пользователь от БД были изменены администратором для любого из модулей, необходимо привести логины к дефолтному виду (подробнее см. в Приложении 2), при этом пароли должны совпадать!

Для обновления IDM CAE выполните следующие шаги:

1. Выполните бэкап схемы и БД.
2. Очистите папку `opt/distro` от дистрибутива предыдущей версии

```
sudo rm -rf /opt/distro/*
```

3. Переместите архив в созданную папку и перейдите в эту папку

```
cd /opt/distro
```

4. Выполните разархивирование в директорию `/opt/distro` с помощью команды

```
sudo tar -xvf D-1.4.1.tar.gz
```

5. Запустите скрипт установки и настройки сервисов с помощью команды

```
sudo ./install.sh cfg.yml
```

4.1.6. Установка компонентов в конфигурации All-in-One

Установка компонентов происходит в рамках развёртывания продукта.

4.1.7. Удаление компонентов в конфигурации All-in-One

Удаление отдельных компонентов не предусмотрено.

5. ПРОВЕРКА РАБОТОСПОСОБНОСТИ

После развёртывания IDM CAE убедитесь в работоспособности компонентов. Для этого выполните команду в зависимости от проверяемого компонента:

- компонент Workflow Management модуля Base:

```
systemctl status idmcae-wm.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

- компонент Provisioning Management модуля Base:

```
systemctl status idmcae-pm.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

- модуль Monitoring:

```
systemctl status idmcae-monitoring.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

- модуль IG:

```
journalctl -u idmcae-wm.service | grep "Application IdentityGovernance started successfully!"
```

Убедитесь в наличии записи

```
Application IdentityGovernance started successfully!
```

- модуль RM:

```
systemctl status idmcae-rm.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

```
journalctl -u idmcae-wm.service | grep "RM-DELEGATES initialized successfully!"
```

Убедитесь в наличии записи

```
RM-DELEGATES initialized successfully!
```

- Apache Kafka:

```
systemctl status idmcae-kafka.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

- репозиторий:

```
systemctl status postgresql-15.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

- веб-сервис:

```
systemctl status nginx.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

- подсистема сбора и обработки IDM CAE:

```
systemctl status logstash.service
```

В результате команды проверяемый компонент должен иметь статус **active (running)**.

Также убедитесь в работоспособности веб-интерфейсов модулей. Для этого откройте веб-интерфейс каждого модуля:

- компонент Workflow Management модуля Base /модуль IG: `https://<ip_адрес_сервера>/workflow/`
- компонент Provisioning Management модуля Base: `https://<ip_адрес_сервера>/base/`

- модуль Monitoring:

  `https://<ip_адрес_сервера>/`

6. ПЕРВИЧНАЯ НАСТРОЙКА IDM CAE

После развёртывания выполните первичную настройку IDM CAE. Для этого выполните шаги, описанные для каждого модуля / компонента.

6.1. Компонент Provisioning Management модуля Base

Выполните шаги:

1. Войдите в веб-интерфейс по адресу

   `https://<ip_адрес_сервера>/base/`

2. Укажите креды:

   `User: administrator`

   `Password: <значение пароля из лога /opt/idmcae/base/var/log/midpoint/log в строке «Administrator initial password (except double quotes):» >`

3. Перейдите в раздел **Users -> All users** (1, рисунок 1). Выберите УЗ **administrator** (2, рисунок 1);

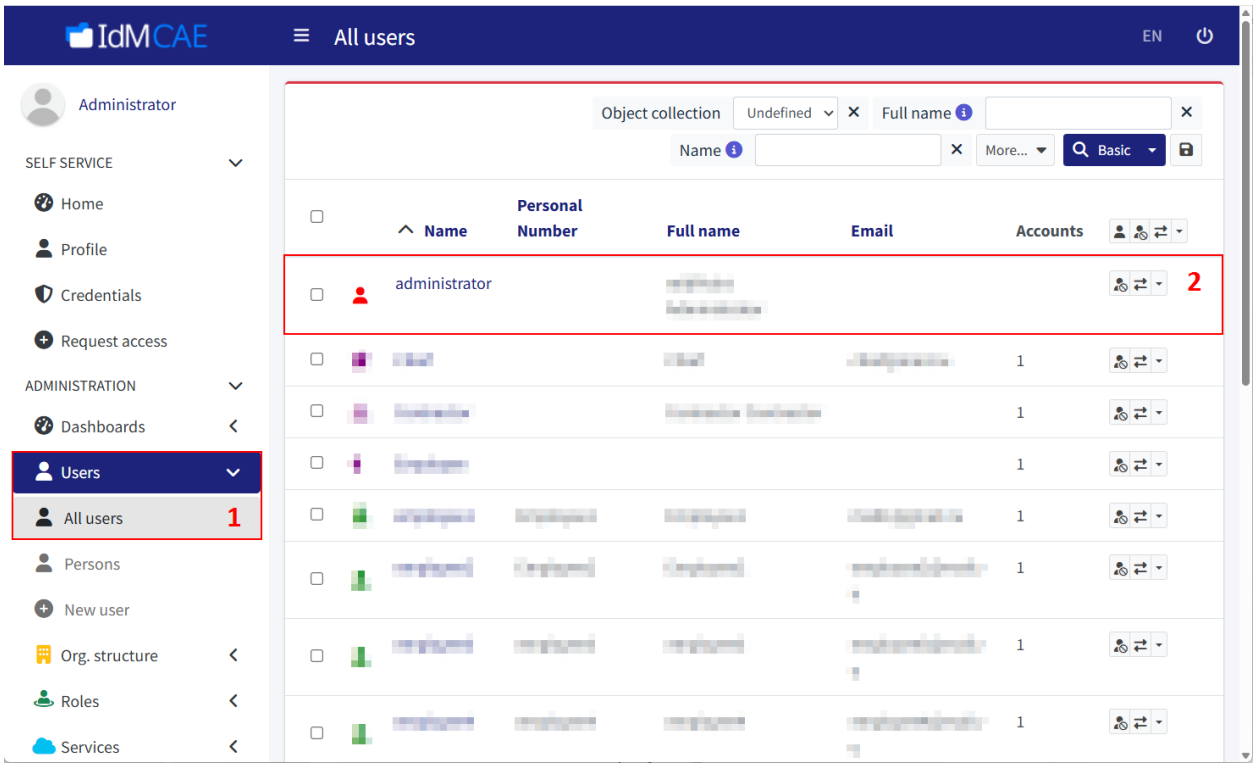


Рисунок 1 – Переход к УЗ administrator

4. Перейдите в подраздел **Password** (1, рисунок 2) и в соответствующих полях **Value** укажите новый пароль (2, рисунок 2) (для активации смены пароля предварительно нажмите на **Change**). Сохраните изменения, нажав на **Save** (3, рисунок 2).

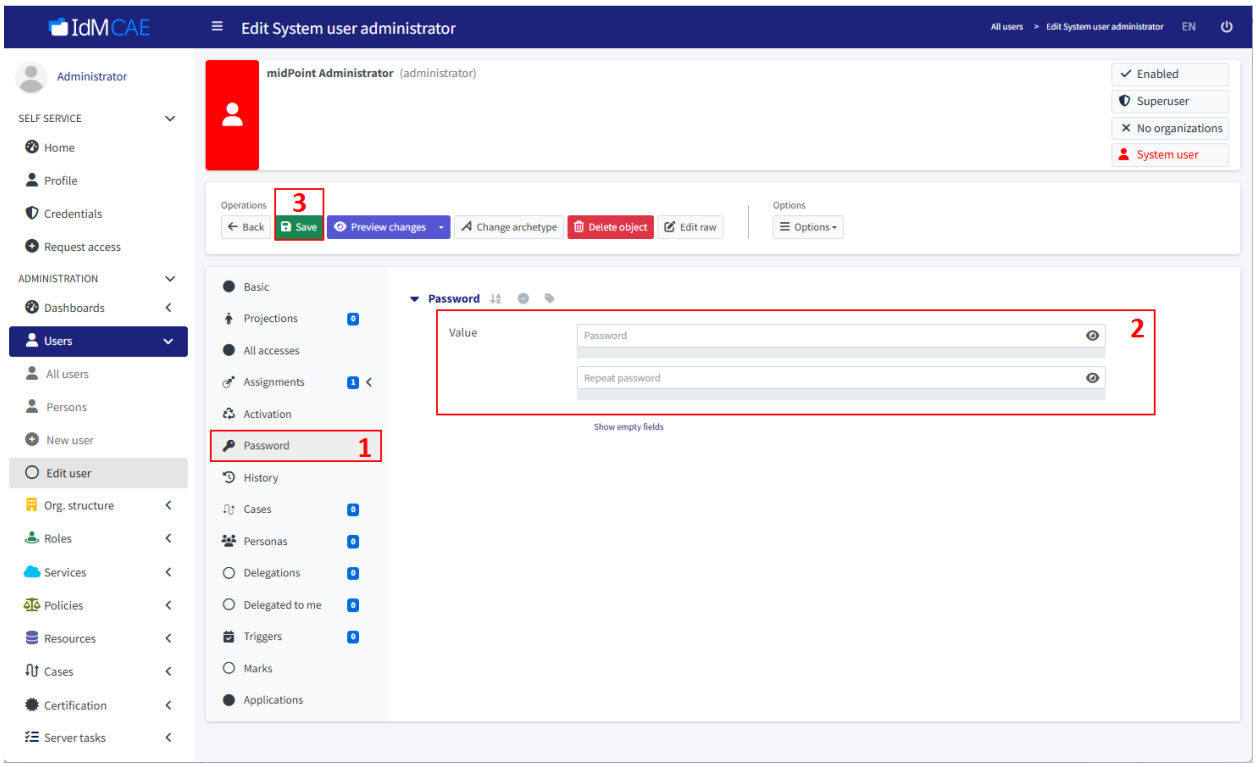


Рисунок 2 – Изменение пароля

6.2. Компонент Workflow Management модуля Base / модуль IG

Выполните шаги:

1. Откройте файл с помощью команды

```
sudo nano /usr/lib/systemd/system/idmcae-wm.service
```

2. Вставьте в параметр `MIDPOINT_TUZ_PASSWORD` значение сгенерированного пароля из лога `/opt/idmcae/base/var/log/midpoint/log/midpoint.log` в строке «`Administrator initial password (except double quotes):`»
3. Выполните команду

```
systemctl daemon-reload
```

4. Перезапустите службу с помощью команды

```
systemctl restart idmcae-wm.service
```

5. Войдите в веб-интерфейс по адресу

   `https://<ip_адрес_сервера>/workflow/`

6. В открывшемся окне с настройками УЗ администратора заполните соответствующие значения.
7. После успешного ввода данных перейдите в окно авторизации, нажав на **Sign**, и войдите с помощью созданной на предыдущем шаге УЗ.

6.3. Модуль Monitoring

Выполните шаги:

1. Войдите в веб-интерфейс по адресу

   `https://<ip_адрес_сервера>/`

2. Укажите креды, установленные по умолчанию:

   `User: admin`

   `Password: admin`

3. Нажмите на **Настройки** (1, рисунок 3) и в выпадающем меню выберите **Базы данных** (2, рисунок 3).

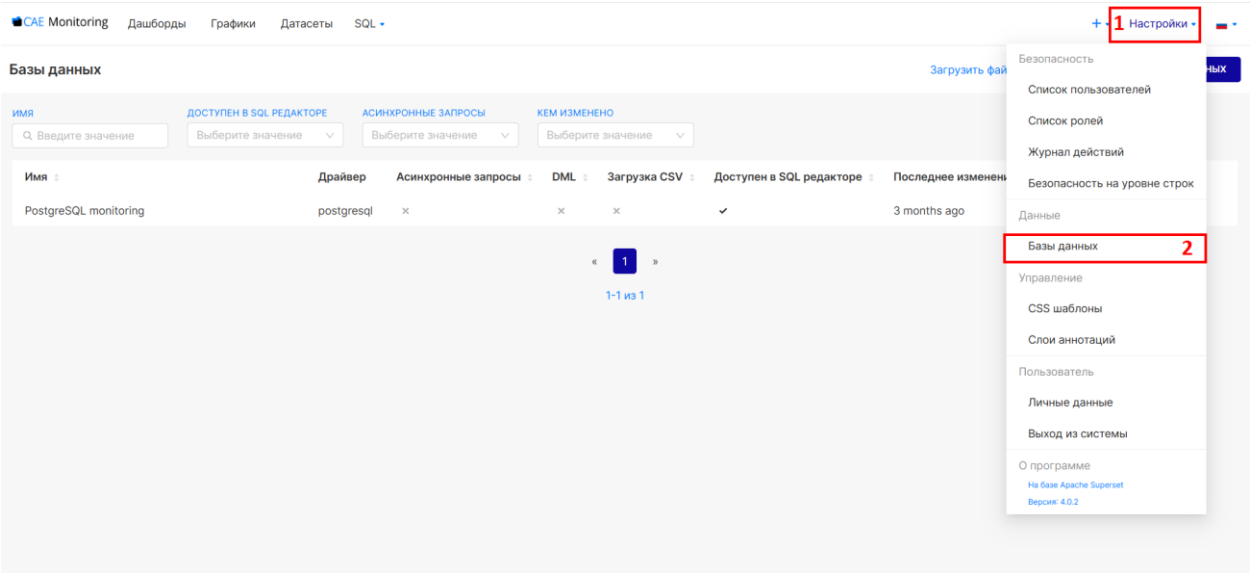


Рисунок 3 – Переход к БД

4. Нажмите на  справа от БД PostgreSQL monitoring (рисунок 4).

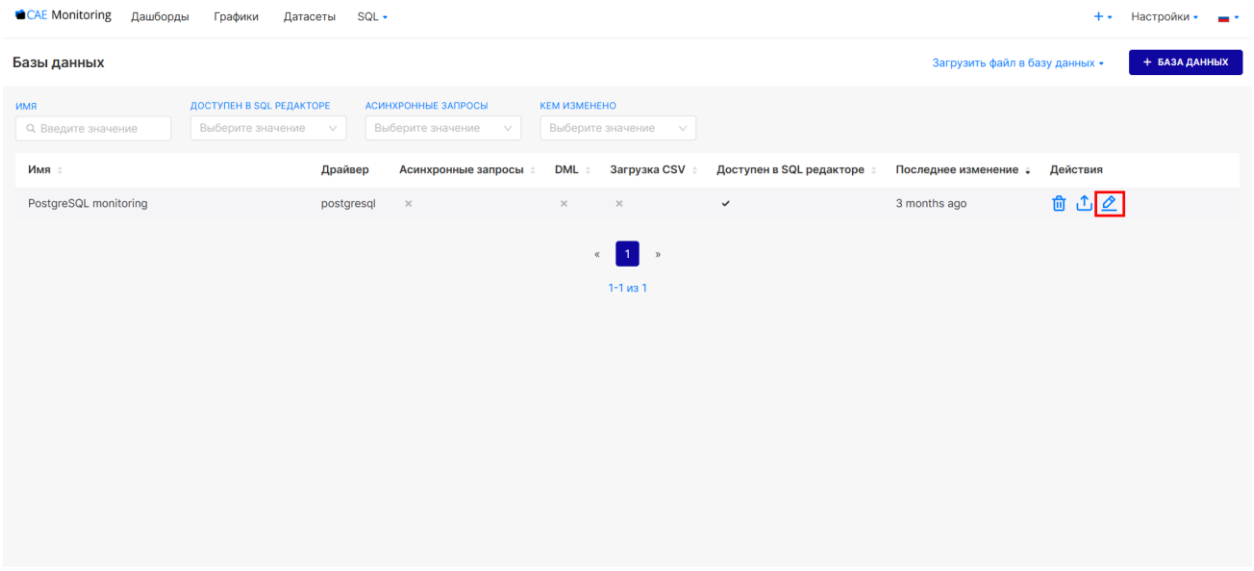


Рисунок 4 – Переход к редактированию БД

5. Вставьте введённый в разделе 4.1.4 пароль вместо `XXXXXXXXX` (1, рисунок 5). Нажмите на **ЗАВЕРШИТЬ** (2, рисунок 5).

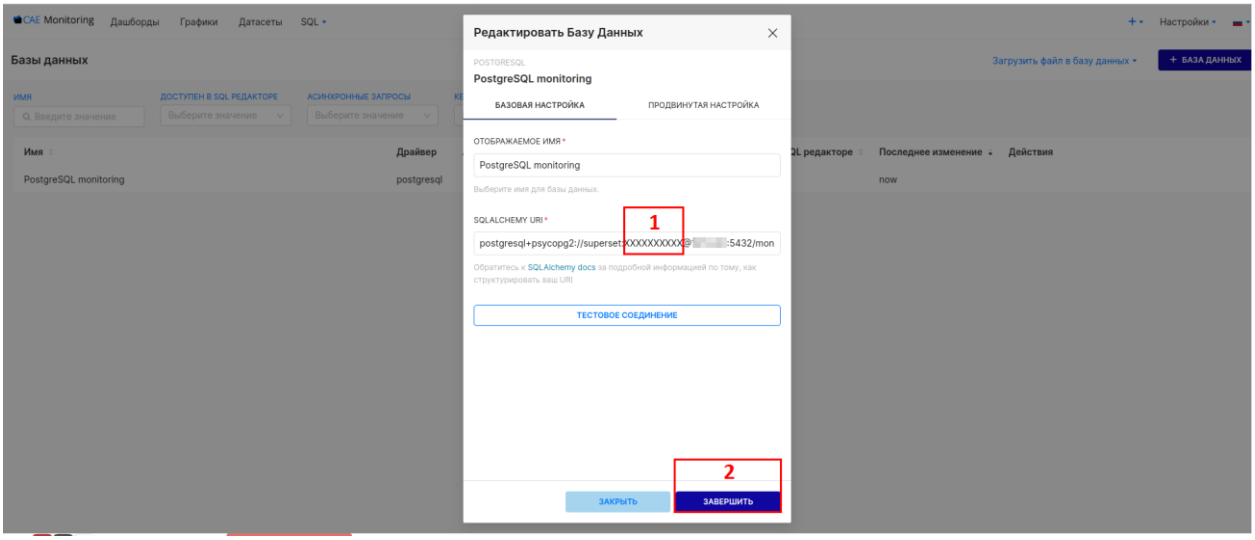


Рисунок 5 – Установка пароля

6.4. Модуль RM

При установке дистрибутива создаётся сертификат `secret-keystore.p12` по пути `/opt/idmcae/workflow/configuration/`. Сертификат используется для шифрования создаваемых паролей

при передаче переменной между делегатами компонента Workflow Management. В случае ручной генерации сертификата `secret-keystore.p12` требуется использовать шифрование типа AES / GCM / NoPadding.

6.4.1. SSL-соединение с Apache Kafka (из дистрибутива)

В разделе описываются действия по настройке SSL-соединения с компонентом Apache Kafka, который входит в состав дистрибутива.

Keystore `kafka-keystore.jks` для Apache Kafka генерируется автоматически при установке дистрибутива и расположен по пути `/var/lib/kafka/certs/` (пароль указан в скрипте автогенерации `/etc/nginx/key/generate-certs.sh`).

После развёртывания автоматически настраивается SSL-взаимодействие с Apache Kafka. Однако можно настроить SSL-взаимодействие с Apache Kafka самостоятельно, выполнив шаги согласно инструкции для Apache Kafka 4.0.0. Для дальнейшей настройки выполните следующие шаги:

1. Измените файл `/opt/idmcae/kafka/config/server.properties`, изменив / добавив атрибуты:

```
listeners=PLAINTEXT://host.name:port,SSL://host.name:port
security.inter.broker.protocol=SSL

# Listener name, hostname and port the broker or the controller will advertise to clients
```

```
advertised.listeners=PLAINTEXT://host.name:port,SSL://
host.name:port

########## SSL Settings ##########

ssl.keystore.location=*****
ssl.keystore.password=*****
ssl.key.password=*****
ssl.truststore.location=*****
ssl.truststore.password=*****
ssl.client.auth=none
ssl.enabled.protocols=TLSv1.2,TLSv1.1,TLSv1
ssl.keystore.type=JKS
ssl.truststore.type=JKS
ssl.secure.random.implementation=SHA1PRNG
```

2. В файлах служб `/usr/lib/systemd/system/idmcae-rm.service` и `/usr/lib/systemd/system/idmcae-wm.service` по умолчанию указан порт для SSL-соединения в переменной окружения `RM_KAFKA_BOOTSTRAP_SERVERS`. Если SSL-соединение не используется, измените порт, а также конфигурации всех служб, где используется SSL-соединение с Apache Kafka (`idmcae-wm.service; idmcae-rm.service`).
3. Измените параметры, если не используется SSL-соединение или ваше SSL-соединение имеет индивидуальные настройки, в файлах `/opt/idmcae/rm/config.yaml` и

/opt/idmcae/workflow/configuration/rm-delegates-config.yaml:

```
        ssl-keystore-location(ssl.keystore.location)
        ssl-keystore-password(ssl.keystore.password)
        ssl-truststore-
location(ssl.truststore.location)
        ssl-truststore-
password(ssl.truststore.password)
        ssl-key-password(ssl.key.password)
```

4. Убедитесь в наличии сертификата `secret-keystore.p12` в директории `/opt/idmcae/workflow/configuration` (при установке дистрибутива сертификат устанавливается автоматически).
5. Убедитесь в наличии сертификата `server-keystore.p12` в директории `opt/idmcae/rm/` (при установке дистрибутива сертификат устанавливается автоматически).

6.4.2. Настройка соединения и конфигурирование Apache Kafka (не из дистрибутива)

В разделе описываются действия по настройке соединения с компонентом Apache Kafka, который не входит в состав дистрибутива IDM CAE. Для настройки соединения и конфигурирования Apache Kafka выполните шаги:

1. Проверьте доступность порта подключения к Apache Kafka.
2. В файлах служб `/usr/lib/systemd/system/idmcae-rm.service` и `/usr/lib/systemd/system/idmcae-wm.service` проверьте порт подключения к Apache Kafka в переменной окружения `RM_KAFKA_BOOTSTRAP_SERVERS`.

3. Для настройки SSL-соединения проверьте в конфигурационных файлах `/opt/idmcae/rm/config.yaml` и `/opt/idmcae/workflow/configuration/rm-delegates-config.yaml` пути к SSL-сертификатам, измените их на актуальные.
4. Проверьте конфигурационной файл `server.properties` Apache Kafka на предмет состояния параметра `auto.create.topics.enable`. Если автосоздание топиков запрещено (указан `false`), проверьте в файле `/opt/idmcae/rm/config.yaml` названия топиков и убедитесь, что они созданы в кластере Apache Kafka (или создайте их самостоятельно). Если у параметра `auto.create.topics.enable` указан статус `true` или он отсутствует, топики создадутся автоматически.

6.4.3. Соединение с почтовым сервером

Перед настройкой соединения с почтовым сервером проверьте доступность порта почтового сервера с сервера, на котором развёрнута служба `idmcae-wm.service`.

Для настройки соединения с почтовым сервером укажите в файле службы `idmcae-wm.service` значения переменных окружения (подробное описание см. в Руководстве администратора для модуля RM):

- SMTP_HOST;
- SMTP_PORT;
- SMTP_LOGIN;

- SMTP_FROMADDR;
- SMTP_FROMADDR_PASSWORD;
- SMTP_AUTH_MECHANISM;
- SMTP_FROMNAME.

Если для соединения с почтовым сервером используется SSL, добавьте в системный keystore JDK по пути `/opt/idmcae/jdk/lib/security/cacerts` корневой сертификат от почтового сервера (пароль от системного keystore указан в скрипте автогенерации `/etc/nginx/key/generate-certs.sh`).

В случае отсутствия соединения с почтовым сервером при изменении пароля модулем RM нотификация об изменении пароля и само значение пароля для пользователя будет неизвестно, что приведёт к отсутствию почтовых уведомлений!

6.4.4. SSL-соединение с Provisioning Management

Для настройки SSL-соединения с Provisioning Management выполните следующие шаги:

1. (опционально) в случае получения внешнего корневого сертификата:
    - удалите существующие сертификаты

```
rm -rf /etc/nginx/ca.* /etc/nginx/cert.* /etc/nginx/key.*
```

    - переименуйте новые сертификаты и ключ (полученные от внешнего источника): CA-сертификат в `ca.pem`, клиентские сертификат и ключ

в `cert.pem` и `key.pem`, а затем поместите их в `/etc/nginx/`.

- переместите CA-сертификат в системное хранилище

```
cp /etc/nginx/key-test/ca.pem /etc/pki/ca-trust/source/anchors/
```

- обновите CA

```
update-ca-trust
```

2. Выполните команду

```
/opt/idmcae/jdk/bin/keytool -import -alias ca -keystore /opt/idmcae/certs/idmcae-truststore.jks -storepass changeit -file /etc/nginx/ca.pem -noprompt
```

3. Проверьте содержимое блока `midpoint` в файле `/opt/idmcae/workflow/configuration/rm-delegates-config.yaml`

```
rm-delegates:
…
  midpoint:
    api-url: https://${MIDPOINT_HOST}:${MIDPOINT_PORT}/base/ws/rest/
    api-username: changeit
    api-password: changeit
    trust-store-path: /opt/idmcae/certs/idmcae-truststore.jks
    trust-store-password: changeit
    disable-hostname-verification: true  # опционально
    disable-ssl: false    # опционально
    timeout: 5    # опционально, по умолчанию 30 сек
```

4. Проверьте содержимое блоков `rest-api` и `midpoint` в файле `/opt/idmcae/rm/config.yaml`

```
rm:
 …
  rest-api:
    port: <port>
    schema: https  # https указывается при использовании ssl
    ssl:
      enabled: true   # при указании false отключается проверка сертификатов, также требуется смена порта
      need-client-auth: true   # при значении true сервер требует, чтобы клиент предоставил свой сертификат для аутентификации. Сервер будет проверять клиентский сертификат по truststore
      key-store-resource: file:./server-keystore.p12
      key-store-type: PKCS12
      key-store-password: {PASSWORD1}
      key-password: {PASSWORD2}
      trust-store-resource: /opt/idmcae/certs/idmcae-truststore.jks
      trust-store-type: JKS
      trust-store-password: {PASSWORD3}
```

```
      enabled-protocols: # можно использовать протокол TLS не ниже версии 1.2
        - TLSv1.2
        - TLSv1.3
      cipher-suite: # для корректной работы требуется использовать указанные шифры
        # TLS 1.3 cipher suites (most secure)
        - TLS_AES_256_GCM_SHA384
        - TLS_AES_128_GCM_SHA256
        - TLS_CHACHA20_POLY1305_SHA256
        # TLS 1.2 cipher suites with forward secrecy (ECDHE)
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        # TLS 1.2 cipher suites (RSA key exchange - less pre-ferred but compatible)
        - TLS_RSA_WITH_AES_256_GCM_SHA384
        - TLS_RSA_WITH_AES_128_GCM_SHA256
…
  midpoint:
```

```
    api-url: https://localhost/base/ws/rest
    api-username: rm_user
    api-password: {PASSWORD4}
    trust-store-path: /opt/idmcae/certs/idmcae-truststore.jks
    trust-store-password: {PASSWORD5}
```

6.4.5. SSL-соединение по REST API с внешней ИС

Для SSL-соединения по REST API с внешней ИС выполните следующие шаги:

1. Выпустите сертификаты на стороне внешней ИС с учётом шифров, указанных в `/opt/idmcae/rm/config.yaml` в блоке `cipher-suite`

```
rm:
 …
  rest-api:
 …


    ssl:
 …
      cipher-suite: # для корректной работы требуется использовать указанные шифры
        # TLS 1.3 cipher suites (most secure)
        - TLS_AES_256_GCM_SHA384
        - TLS_AES_128_GCM_SHA256
        - TLS_CHACHA20_POLY1305_SHA256
        # TLS 1.2 cipher suites with forward secrecy (ECDHE)
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        # TLS 1.2 cipher suites (RSA key exchange - less pre-ferred but compatible)
        - TLS_RSA_WITH_AES_256_GCM_SHA384
        - TLS_RSA_WITH_AES_128_GCM_SHA256
```

2. Выполните команды

```
/opt/idmcae/jdk/bin/keytool -import -trustcacerts -alias <CA-сертификат внешней ИС> -keystore /opt/idmcae/certs/idmcae-truststore.jks -storepass changeit -file <CA-сертификат внешней ИС> -noprompt
```

```
/opt/idmcae/jdk/bin/keytool -import -alias <клиентский сертификат внешней ИС> -keystore /opt/idmcae/certs/idmcae-truststore.jks -storepass changeit -file <клиентский сертификат внешней ИС> -noprompt
```

```
/opt/idmcae/jdk/bin/keytool -import -alias <клиентский ключ сертификата внешней ИС> -keystore /opt/idmcae/rm/server-keystore.p12 -storepass changeit -file <клиентский ключ сертификата внешней ИС> -noprompt
```

7. ОБРАЩЕНИЕ В ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ

Раздел содержит требования к содержимому обращения и его оформлению.

7.1. Порядок подачи обращений в службу технической поддержки

Обращения в службу поддержки компании «ООО «Кросстех Солюшнс Групп» (Вендор) в гарантийных случаях необходимо производить через электронную почту support@ct-sg.ru.

7.2. Требование к содержанию обращения

При подаче обращения через портал технической поддержки для ускорения предоставления решения по обращению необходимо максимально подробно заполнить все поля и приложить файлы с необходимой информацией (логи, скриншоты, другие файлы).

Требования к оформлению обращений:

1. Одно обращение описывает одну проблему, возникшую в процессе работы системы.
2. Наименование обращения кратко описывает имеющуюся проблему.
3. Указан приоритет устранения проблемы:
   - критичный - существование дефекта приводит к масштабным последствиям катастрофического характера, например: потеря данных, раскрытие конфиденциальной информации;
   - средний - существование дефекта слабо влияет на типичные сценарии работы пользователей, и/или

существует обходной путь достижения цели, например: диалоговое окно не закрывается автоматически после нажатия **OK**/**Cancel**;

- низкий - существование дефекта редко обнаруживается незначительным процентом пользователей и (почти) не влияет на их работу, например: опечатка в глубоко вложенном пункте меню настроек.

4. Описание проблемы подробное и содержит следующие пункты:
   - окружение - версия ОС и ее разрядность, версия продукта, дополнительные параметры (браузеры и их версии или приложения и их версии);
   - шаги воспроизведения - алгоритм в форме пошаговой инструкции воспроизведения ошибки, где одно действие указано как один шаг;
   - ожидаемый результат - описание того, как система должна работать после выполнения шагов, указанных выше;
   - фактический результат - описание того, как система работает после воспроизведения вышеуказанной последовательности шагов;
   - вложенные файлы - дополнительная информация: скриншоты, текстовые файлы, логи, видео выполняемых действий.

5. Дополнительные параметры: предусловие, постусловие, дополнения.

8. ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Данный раздел содержит описание состава дистрибутива.

8.1. Описание дистрибутива

Дистрибутив предназначен для установки и настройки компонентов IDM CAE. Дистрибутив содержит следующие основные компоненты:

- IDMCAE Provisioning Management v. 1.4.1;
- IDMCAE Workflow Management v. 1.4.1;
- IDMCAE IG v. 1.4.1;
- IDMCAE MONITORING v. 1.4.1;
- IDMCAE RM v. 1.4.1;
- Apache Kafka v. 4.0.0;
- Java JDK v. 21;
- PostgreSQL v. 15.8;
- Logstash v. 8.10.3;
- Nginx v. 1.27.0.

8.2. Целевая схема размещения на сервере

Целевой состав компонентов представлен в таблице 2.

Таблица 2 – Целевой состав компонентов

№	Компонент	Системный пользователь	Сервис
1.	IDMCAE Provisioning Management	user: idmcae	service: idmcae-pm.service
2.	IDMCAE Workflow Management	user: idmcae	service: idmcae-wm.service

№	Компонент	Системный пользователь	Сервис
3.	IDMCAE MONITORING	user: idmcae	service: idmcae-monitoring.service
4.	IDMCAE IG	user: idmcae	service: /opt/idmcae/workflow/configuration/user lib/ service: /opt/idmcae/workflow/configuration/reso urces/ig/
5.	IDMCAE RM	user: idmcae	service: idmcae-rm.service
6.	Apache Kafka	user: idmcae	service: idmcae-kafka.service
7.	PostgreSQL	user: postgres	service: postgresql-15.service
8.	Logstash	user: logstash	service: logstash.service
9.	Nginx	user: nginx	service: nginx.service

Расположение компонентов представлено в таблицах 3 – 12.

Таблица 3 – Расположение IDMCAE Provisioning Management

№	Параметр	Значение
1.	Системный пользователь	idmcae
2.	Сервис	idmcae-pm
3.	Путь установки	/opt/idmcae/base
4.	Настройки сервиса	/opt/idmcae/base/var/config.xml
5.	Логи сервиса	/opt/idmcae/base/var/log/ (/var/log/messages)
6.	Определение сервиса	/usr/lib/systemd/system/idmcae-pm.service

Таблица 4 – Расположение IDMCAE Workflow Management

№	Параметр	Значение
1.	Системный пользователь	idmcae
2.	Сервис	idmcae-wm
3.	Путь установки	/opt/idmcae/workflow
4.	Настройки сервиса	/opt/idmcae/workflow/configuration/production_ig.yml
5.	Логи сервиса	/opt/idmcae/workflow/logs/ (/var/log/messages)
6.	Определение сервиса	/usr/lib/systemd/system/idmcae-wm.service

Таблица 5 – Расположение IDMCAE MONITORING

№	Параметр	Значение
1.	Системный пользователь	idmcae
2.	Сервис	idmcae-monitoring
3.	Путь установки	/opt/idmcae/monitoring
4.	Настройки сервиса	/opt/idmcae/monitoring/lib/python3.11/site-packages/superset/config.py
5.	Логи сервиса	/var/log/messages
6.	Определение сервиса	/usr/lib/systemd/system/idmcae-monitoring.service

Таблица 6 – Расположение IDMCAE IG

№	Параметр	Значение
1.	Системный пользователь	idmcae

№	Параметр	Значение
2.	Сервис	service: /opt/idmcae/workflow/configuration/userlib/ service: /opt/idmcae/workflow/configuration/resources/ig/
3.	Путь установки	/opt/idmcae/workflow/configuration/userlib (ядро IG) /opt/idmcae/workflow/configuration/resources/ig (модели процессов и пользовательские формы)
4.	Настройки сервиса	/opt/idmcae/workflow/configuration/production_ig.yml
5.	Логи сервиса	/opt/idmcae/workflow/logs/ (/var/log/messages)
6.	Определение сервиса	/usr/lib/systemd/system/idmcae-wm.service

Таблица 7 – Расположение IDMCAE RM

№	Параметр	Значение
1.	Системный пользователь	idmcae
2.	Сервис	service: idmcae-rm.service
3.	Путь установки	/opt/idmcae/rm
4.	Настройки сервиса	/opt/idmcae/rm/config.yaml
5.	Логи сервиса	/var/log/messages
6.	Определение сервиса	/usr/lib/systemd/system/idmcae-rm.service

Таблица 8 – Расположение Apache Kafka

№	Параметр	Значение
1.	Системный пользователь	idmcae
2.	Сервис	service: idmcae-kafka.service

№	Параметр	Значение
3.	Путь установки	/opt/idmcae/kafka
4.	Настройки сервиса	/opt/idmcae/kafka/config/
5.	Логи сервиса	/var/lib/kafka/data
6.	Определение сервиса	/usr/lib/systemd/system/idmcae-kafka.service

Таблица 9 – Расположение Java

№	Параметр	Значение
1.	Путь установки	/opt/idmcae/jdk

Таблица 10 – Расположение PostgreSQL

№	Параметр	Значение
1.	Системный пользователь	postgres
2.	Сервис	postgresql-15
3.	Путь установки	/usr/pgsql-15/
4.	Путь для хранения данных	/var/lib/pgsql/15/data/
5.	Настройки сервиса	/var/lib/pgsql/15/data/
6.	Логи сервиса	/var/log/postgresql/ (/var/log/messages)
7.	Определение сервиса	/usr/lib/systemd/system/postgresql-15.service

Таблица 11 – Расположение Logstash

№	Параметр	Значение
1.	Системный пользователь	logstash
2.	Сервис	logstash
3.	Путь установки	/etc/logstash
4.	Настройки сервиса	/etc/logstash/logstash.yml
5.	Логи сервиса	/var/log/logstash/
6.	Определение сервиса	/usr/lib/systemd/system/logstash.service

Таблица 12 – Расположение Nginx

№	Параметр	Значение
1.	Системный пользователь	nginx
2.	Сервис	nginx
3.	Путь установки	/etc/nginx
4.	Настройки сервиса	/etc/nginx/nginx.conf
5.	Логи сервиса	/var/log/nginx/
6.	Определение сервиса	/usr/lib/systemd/system/nginx.service

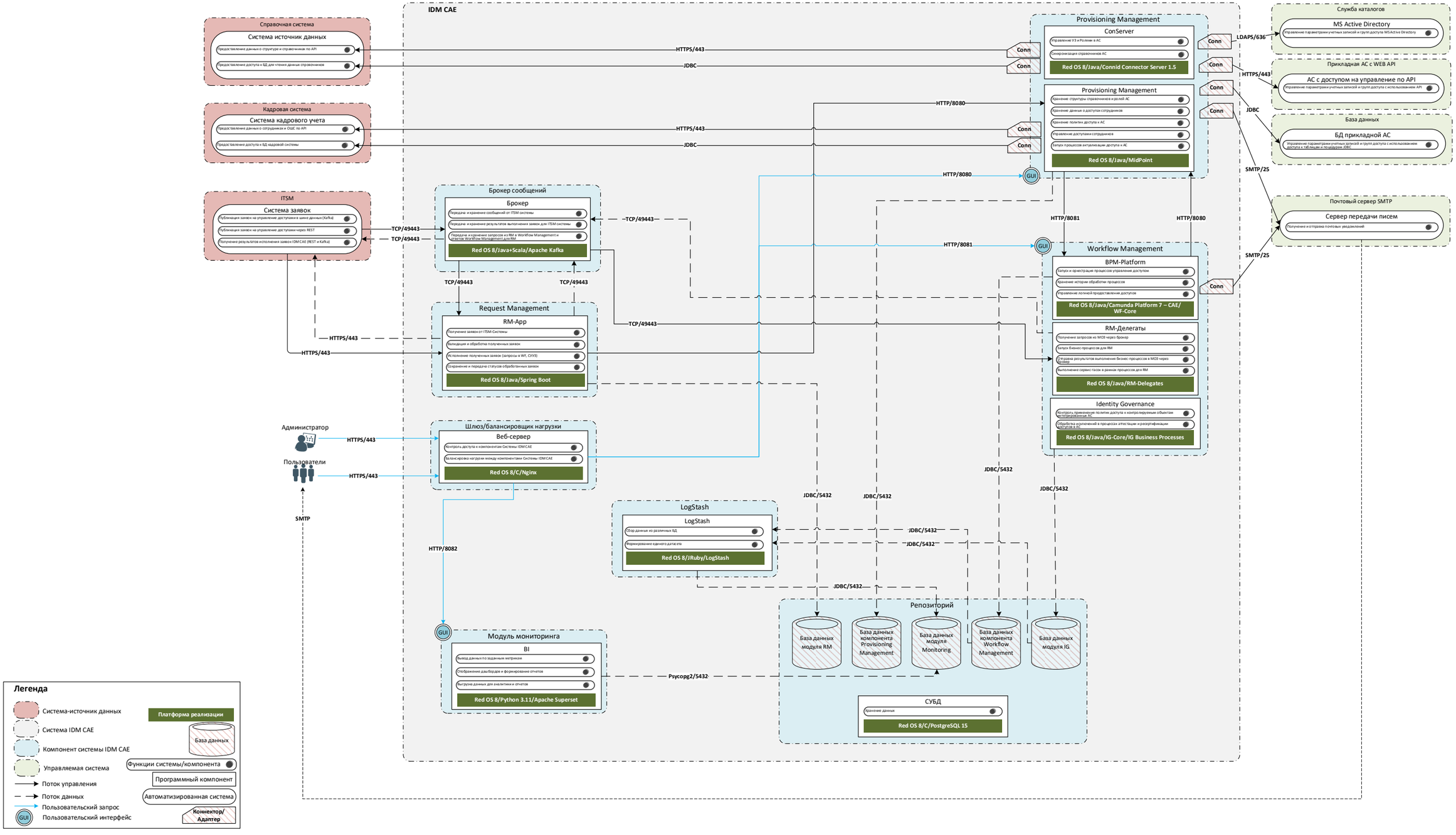
8.3. Порты компонентов

Для корректной работы компонентов необходимы порты, перечисленные в таблице 13.

Таблица 13 – Порты компонентов

№	Компонент	Порт /протокол	Описание
1.	IDMCAE Provisioning Management	8080 / tcp / http	Осуществление http-запросов
2.	IDMCAE Provisioning Management	<любой порт для интеграции> / tcp	Обеспечение интеграции
3.	IDMCAE Workflow Management	8081 / tcp / http	Осуществление http-запросов
4.	IDMCAE-MONITORING	8082 / tcp / http	Осуществление http-запросов
5.	Apache Kafka	8083 / tcp	Осуществление связи с брокером сообщений
6.	PostgreSQL	5432 / tcp	Доступ к БД
7.	Nginx	443 / tcp / https	Осуществление http-запросов
8.	Nginx	80 / tcp / http	Осуществление http-запросов

ПРИЛОЖЕНИЕ 1. ВАРИАНТ АРХИТЕКТУРНОЙ СХЕМЫ IDM CAE



ПРИЛОЖЕНИЕ 2. ДЕФОЛТНЫЕ ЛОГИНЫ МОДУЛЕЙ IDM CAE

В таблице 14 приведено дефолтное значение логинов для модулей, входящих в состав IDM CAE.

Таблица 14 – Дефолтные логины

№	Модуль / компонент	Логин
1.	Provisioning Management	midpoint
2.	Workflow Management	camunda
3.	Monitoring	superset
4.	IG	mcpd_user
5.	RM	rm_idmcae