H F Labs

«КУС»

Руководство по развертыванию

Оглавление

1 Требования к аппаратной платформе

1.1 Общие требования

В данном разделе представлены *минимальные* системные требования

Минимальная конфигурация состоит из сервера «КУС», сервера СУБД и рабочей станции для сотрудников HFLabs. Для работы пользователей нужно выделить им клиентские машины.

На всех серверах не должно быть установлено приложений, которые замедляют работу с дисковой подсистемой или перехватывают сетевой трафик (антивирус, фаервол и т.п.). Чтобы защитить серверы, используйте DMZ-зоны.

1.2 Требования к сетевой инфраструктуре

Отсутствуют аппаратные или программные межсетевые экраны, которые закрывают неиспользуемые/простаивающие TCP-соединения между:

- сервером приложений «КУС» и сервером СУБД;
- сервером приложений «КУС» и сервером Active Directory.

Требования к пропускной способности каналов между компонентами:

Компонент 1	Компонент 2	Ширина канала
Рабочая станция HFLabs	Сервер приложений «КУС»	100 Мбит/с
Рабочая станция HFLabs	Сервер СУБД	100 Мбит/с
Сервер приложений «КУС»	Сервер СУБД	1 Гбит/с
Рабочее место пользователя	Сервер приложений «КУС»	100 Мбит/с

1.3 Требования к рабочей станции для HFLabs

1.3.1 Программно-аппаратные характеристики

Параметр	Требование
Процессор	Intel Core i3 или новее
Оперативная память	8 Гб
Свободное место на жёстком диске	100 Гб
Разрешение экрана	1920×1200
Сетевая карта	100 Мбит
Операционная система	Windows 10 и выше
Разрядность ОС	64-bit
Java	Java SE Development Kit (JDK) 17, с установленными актуальными обновлениями.

Параметр	Требование
Виртуальная среда	Можно использовать виртуальную среду или терминальный сервер
Приложения	• DBeaver (также допустимы: pgAdmin или SQL Workbench/J); • Notepad++ • Putty • WinSCP • SoapUI или Postman • Firefox Quantum или Google Chrome • утилита для снятия профилирования приложения — jvvm_16.zip

1.3.2 Доступы и права

1. Рабочие станции внесены в домен.
2. Создан пользователь с правами локального администратора.
3. Открыт доступ к серверу приложений «КУС» по портам:
    a. 22 (SSH) для администрирования сервера приложений.
    b. 8080 (HTTP-порт «КУС»).
    c. 18080 (HTTP-порт модуля качества данных).
    d. 9990 (JMX-порт для мониторинга приложения ««КУС»»).
    e. 19990 (JMX-порт для мониторинга модуля качества данных).
4. Доступна возможность копирования файлов на сервер приложений «КУС» (по SSH).
5. Открыт доступ к серверу СУБД по порту 5432.
6. Доступ к ресурсам HFLabs через сеть Интернет:
    a. https://jira.hflabs.ru/
    b. https://confluence.hflabs.ru/
    c. https://cloud.hflabs.ru/
    d. https://fs.hflabs.ru/

1.4 Требования к серверу приложений

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 32 ядер
Оперативная память	от 128 Гб
Объем жесткого диска	от 1,5 Тб
Скорость чтения с диска	SSD-диск для данных: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 10 000 TBW
Сетевая карта	1 Гбит
Операционная система	• AlmaLinux 8 или 9 (рекомендуется) • Red Hat Enterprise Linux 8 или 9 • Debian 11 • Альт Сервер 10 (входит в реестр отечественного ПО) • Astra Linux Common Edition Орел (входит в реестр отечественного ПО)
Виртуальная среда	Не допускается, только аппаратная платформа
Прочие требования	Запрещена установка антивируса

1.5 Требования к серверу СУБД

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 20 ядер
Оперативная память	96 Гб
Объем жесткого диска	от 4 Тб
Скорость чтения с диска	SSD с параметрами: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 10 000 TBW
Сетевая карта	1 Гбит
СУБД	Postgres 14+
Виртуальная среда	Не допускается, только аппаратная платформа
Прочие требования	Запрещена установка антивируса

1.6 Требования к рабочему месту пользователя

Минимальные требования к клиентскому рабочему месту:

Параметр	Требование
Процессор	Intel Core i3 или новее
Оперативная память	8 Гб
Свободное место на жёстком диске	50 Гб
Сетевая карта	100 Мбит
Операционная система	Windows 10 и выше
Разрядность ОС	64-bit
Разрешение экрана	1920×1080
Браузер	Рекомендуем: Mozilla Firefox Quantum версии 100+ или Google Chrome версии 100+ Поддерживаем: Edge

2 Настройка сервера СУБД PostgreSQL

2.1 Доступы и права

1. Открыть порты:
    - 5432 (или другой порт, используемый PostgreSQL).
2. В БД PostgreSQL создать схему и пользователя для «КУС». При необходимости необходимо создать пользователя ETL для записи в буферные таблицы.

2.2 Создание пользователя КУС

1. Измените приложенный ниже скрипт — вместо {password} укажите реальный пароль.
2. Запустите скрипт на выполнение из-под административной учетной записи.

```
-- ----------------------------------------------------
--      CREATE USER & SCHEMA (with same name)
-- ----------------------------------------------------
CREATE USER cdi WITH LOGIN INHERIT CREATEROLE
PASSWORD '{password}';

CREATE SCHEMA cdi AUTHORIZATION cdi;

-- ----------------------------------------------------
--                 USER PRIVILEGES
-- ----------------------------------------------------
GRANT ALL ON ALL TABLES     IN SCHEMA cdi TO cdi WITH GRANT OPTION;
GRANT ALL ON ALL SEQUENCES  IN SCHEMA cdi TO cdi WITH GRANT OPTION;
GRANT ALL ON ALL FUNCTIONS  IN SCHEMA cdi TO cdi WITH GRANT OPTION;

-- ----------------------------------------------------
--      USE OBJECT ONLY FROM CREATED SCHEMA
-- ----------------------------------------------------
SET search_path TO cdi;
```

2.3 Создание пользователя для записи в буферные таблицы

1. Измените приложенный ниже скрипт — вместо {password} укажите реальный пароль.
2. Запустите скрипт для создания пользователя ETL и выдачи прав на схему и объекты.

```
CREATE USER etl WITH LOGIN INHERIT CREATEROLE PASSWORD '{password}';

GRANT USAGE ON SCHEMA cdi to etl;

ALTER ROLE etl SET search_path TO cdi;

-- Буферы
grant select, insert, update, delete on cdi_buffer_address to etl;
grant select, insert, update, delete on cdi_buffer_consent to etl;
grant select, insert, update, delete on cdi_buffer_contact to etl;
grant select, insert, update, delete on cdi_buffer_doc to etl;
grant select, insert, update, delete on cdi_buffer_extid to etl;
grant select, insert, update, delete on cdi_buffer_increments to etl;
grant select, insert, update, delete on cdi_buffer_ph to etl;
grant select, insert, update, delete on cdi_buffer_relation to etl;

-- Sequence-ы
grant select, usage on sequence buffer_increment_seq to etl;
grant select, usage on sequence cdi_buffer_relation_record_id_seq to etl;
```

3 Настройка Active Directory

1. В Active Directory (AD) добавьте группы, соответствующие ролям, существующим в системе:
    - Менеджер данных (PERFORMER)
    - Оператор (OPERATOR)
    - Офицер информационной безопасности (GUARD)
    - Администратор (ADMINISTRATOR)
    - Оператор журнала проверок (JOURNAL_MANAGER)
    - Верификатор связей (RELATION_MANAGER)
    - Сотрудник комплаенс (KYC_OPERATOR)

   Желательно, чтобы названия групп AD семантически соответствовали назначению ролей.
2. В AD создайте учетные записи для пользователей системы с соответствующими им ролями.
3. В AD создайте тестовую учетную запись (для сотрудников HFLabs, которые будут производить внедрение системы).
4. Добавьте тестовую учетную запись в группы AD, соответствующие ролям PERFORMER и ADMINISTRATOR.
5. В AD создайте техническую учетную запись для системы «КУС», которая имеет права на чтение записей AD из следующих веток:
    - ветки AD, в которой заведены учетные записи пользователей;
    - ветки AD, в которой заведены группы.

   Для этой технической учётной записи установите режим без смены паролей.

4 Установка системы на сервер приложений

4.1 Пакет установки

Набор для установки системы содержит следующие файлы:

- cdi-linux-install.zip — скрипты для установки системы «КУС».
- cdi-web-<customer>-<version>.war — система «КУС».
- cdi-web-<customer>-<version>.war.md5 — контрольная сумма для проверки системы «КУС».
- factor-<customer>-<version>-factord-cli.zip — скрипты для установки модуля качества данных.
- factor-<customer>-<version>-factord-cli.zip.sha1 — контрольная сумма для проверки скриптов установки модуля качества данных.
- factor-<customer>-<version>-factord-install.zip — скрипты для общей установки и конфигурации модуля качества данных.
- factor-<customer>-<version>-factord-install.zip.sha1 — контрольная сумма для проверки скриптов общей установки модуля качества данных.
- factor-<customer>-<version>.war — модуль качества данных.
- factor-<customer>-<version>.war.sha1 — контрольная сумма для проверки модуля качества данных.

4.2 Предварительные настройки

4.2.1 Конфигурация файловой системы

Смонтируйте диски, где будут развернуты приложение «КУС» и модуль качества данных в /opt.

Если по требованиям политик Заказчика необходимо разворачивать приложение в иной директории, то необходимо создать символьную ссылку с директории разворачивания приложений в /opt

4.2.2 Изменение настроек ОС

Настройки параметров ОС выполняются автоматически скриптами установки, кроме отключения THP.

Отключите THP вручную, иначе модуль качества данных не сможет запуститься.

4.2.3 Создание локальных переменных

Создайте локальную переменную HFLABS_ARTEFACTS — директорию, куда будут выложены предоставленные HFLabs ресурсы, необходимые для установки.

```
# export HFLABS_ARTEFACTS=/opt/hflabs_dist && mkdir -p $HFLABS_ARTEFACTS
```

4.2.4 Скачивание артефактов

1. Создайте отдельную директорию в HFLABS_ARTEFACTS под приложение cdi

```
# mkdir -p $HFLABS_ARTEFACTS/cdi
```

2. Скопируйте следующие файлы из пакета установки в директорию HFLABS_ARTEFACTS/cdi/
    - cdi-linux-install.zip
    - cdi-web-<customer>-<version>.war
    - cdi-web-<customer>-<version>.war.md5
3. Скопируйте следующие файлы из пакета установки в директорию HFLABS_ARTEFACTS/
    - factor-<customer>-<version>-factord-cli.zip
    - factor-<customer>-<version>-factord-cli.zip.sha1
    - factor-<customer>-<version>-factord-install.zip
    - factor-<customer>-<version>-factord-install.zip.sha1
    - factor-<customer>-<version>.war
    - factor-<customer>-<version>.war.sha1

4.3 Установка модуля качества данных

1. Перейдите в HFLABS_ARTEFACTS:

```
cd $HFLABS_ARTEFACTS
```

2. Выполните скрипт установки из-под root:

```
unzip $HFLABS_ARTEFACTS/factor-<customer>-<version>-factord-
install.zip && sh $HFLABS_ARTEFACTS/install-factor.sh
```

Скрипт выполнит следующие операции:

a. проверит наличие всех архивов и контрольных сумм для них;

b. создаст структуру каталогов для модуля качества данныха;

c. произведёт настройки ОС;

d. создаст группу и пользователя для службы;

e. установит и зарегистрирует службу в systemd;

f. проверит отключение THP — если настройка не изменена, то в консоли будет предупреждение:

```
WARNING: Transparent hugepage is enabled. You MUST disable
THP manually before starting the service
```

3. Проверьте, что служба модуля качества данныха успешно установлена:

```
systemctl status factor
```

4.4 Установка приложения «КУС»

1. Перейдите в HFLABS_ARTEFACTS/cdi:

```
cd $HFLABS_ARTEFACTS/cdi
```

2. Выполните скрипт установки из-под root:

```
unzip cdi-linux-install.zip && sh install-cdi.sh
```

Скрипт выполнит следующие операции:

a. создаст структуру каталогов для системы cdi;

b. произведёт настройки ОС;

c. создаст группу hflabs и пользователя cdi для службы;

d. установит и зарегистрирует службу в systemd;

e. проверит отключение THP — если настройка не изменена, то в консоли будет предупреждение:

```
WARNING: Transparent hugepage is enabled. You MUST disable
THP manually before starting the service
```

3. Убедитесь, что в консоли нет ошибок и отправьте вывод из консоли в службу поддержки для дополнительной проверки.

4. Проверьте, что служба cdi успешно установлена:

```
systemctl status cdi
```

4.5 Настройка приложения «КУС»

Все настройки «КУС» указываются в одном файле `/opt/cdi/configuration/cdi.conf`. Настройки должны быть указаны одной строкой в формате:

`НазваниеПеременной=ПрисвоенноеЗначение`.

Заполните параметры подключения к БД (`CDI_DS_URL` должен быть указан одной строкой без переносов):

```
# Connection-url
CDI_DS_URL={url одной строкой}
# Имя пользователя
CDI_DS_USERNAME={username}
# Пароль
CDI_DS_PASSWORD={password}
```

5 Запуск системы

5.1 Модуль качества данных

Запуск модуля качества данных

Запуск должен производиться из-под пользователя с правами на выполнение команды service.

```
service factor start
```

Остановка модуля качества данных

Остановка должна производиться из-под пользователя с правами на выполнение команды service.

```
service factor stop
```

5.2 Приложение «КУС»

Запуск приложения «КУС»

Запуск должен производиться из-под пользователя с правами на выполнение команды service.

```
service cdi start
```

Остановка приложения «КУС»

Остановка должна производиться из-под пользователя с правами на выполнение команды service.

```
service cdi stop
```

5.3 Добавление служб в автозапуск

```
chkconfig cdi on && chkconfig factor on
```

5.4 После первого запуска

После первого запуска Единого клиента необходимо зайти в админку на вкладку «Триггеры» и запустить триггер afterDatabaseBackupTrigger.

6 Проверка доступности системы

Для проверки доступности «КУС» используется URL:
`http://{hostname}:{port}/cdi/api/manage/health`

- осуществляет проверку доступности БД (`dbHealthIndicator`): берет соединение из `dataSource` и вызывает на нем метод `isValid`;
- осуществляет проверку доступности модуля качества данных (`factorHealthIndicator`): отправляет запрос в API модуля качества данных: `/api/manage/health` и проверяет полученный статус (таймаут на получение ответа — 1с).

Проверки вызываются синхронно во время обработки запроса `/health`.

В ответе отображаются статусы по каждому компоненту. Если будет общий статус DOWN, по ответу можно увидеть, какой именно компонент перестал отвечать.

7 Контакты технических специалистов

Контакты технических специалистов, которые могут проконсультировать по процессу развёртывания и настройки экземпляра ПО и его функционирования:

- Максим Родионов — maksimrod@hflabs.ru;
- Никита Назаров — nikitan@hflabs.ru;
- Александр Беслик — alexanderb@hflabs.ru.