БФТ.Хранилище электронных документов.Регион

«БФТ.ХЭД.Регион»

Версия 1.9

Руководство по установке и настройке ПО

на 37 листах

Москва 2023

Содержание

1 Введение

Система «БФТ.ХЭД.Регион» предназначена для организации хранения документов, вложений документов, их электронных подписей внешних информационных систем.

2 Первоначальная подготовка операционной системы

Установить ssh-клиент «PuTTY» на машине, с которой планируется производить подключение к удаленному серверу. Скачать клиент по следующей ссылке: https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.79-installer.msi

Открыть клиент PuTTY, в навигационной области панели «Category» выбрать раздел «Session». В поле «Host Name (or Ip address)» ввести Ip-адрес сервера, или его доменное имя, нажать «Open».

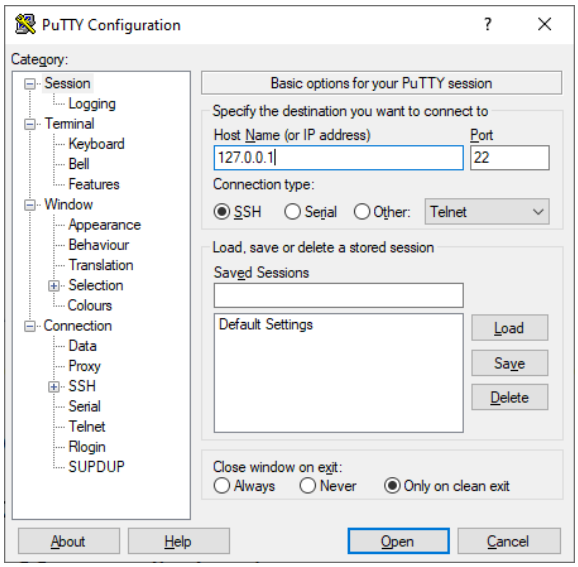

Рисунок 1 Настройка подключения через ssh-клиент PuTTY

В окне консоли ввести логин\пароль от учетной записи вашего пользователя. В командной строке (по очереди) выполнить следующий набор команд:

1.Обновить текущий репозиторий, выполнив команду:

sudo yum update

По итогу установки подтвердить действие, нажать «Y».

2.Установить «wget» , выполнив команду:

sudo yum install wget

По итогу установки подтвердить действие, нажать «Y».

3.Установить «midnight commander» , выполнив команду:

sudo yum install mc

По итогу установки подтвердить действие, нажать «Y».

4.Установить «unzip», выполнив команду:

sudo yum install unzip

По итогу установки подтвердить действие, нажать «Y».

3 Установка и подготовка сопутствующего ПО

3.1 Установка Java

Установить «**Oracle java 11»** (обратить внимание на версионность), для этого необходимо:

1.Перейти в директорию «home», выполнив команду:

cd ~

2.Установить «**Oracle java 11»**, выполнив команду:

sudo yum install -y java-11-openjdk-devel

2.1. Если на машине установлено 2 и более версии «**Oracle java**», выполнить команду:

sudo alternatives --config java

Выбрать нужную версию «**Oracle java 11**», ввести ее порядковый номер, нажать Enter

3.2 Установка PostgreSQL-12

Установить «PostgreSQL-12», для этого необходимо:

1.Указать расположение репозитория, выполнив команду:

sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm

1.1. Отключить модули «PostgreSQL», выполнить команду

sudo dnf -qy module disable postgresql

2.Установить приложение, выполнив команду (для CentOS 8 и выше):

sudo yum install -y postgresql12-server

3.Создать экземпляр базы данных, выполнив команду:

sudo /usr/pgsql-12/bin/postgresql-12-setup initdb

Если после выполнения команды появилась строка «Initializing database… OK», создание экземпляра успешно завершено.

4.Инициализировать службу СУБД, выполнив команду:

sudo systemctl enable postgresql-12

5.Запустить службу СУБД, выполнив команду:

sudo systemctl start postgresql-12

6.Проверить статус службы, выполнив команду:

systemctl status postgresql-12

Если после проверки статуса, в окне консоли зеленым цветом подсвечено сообщение «active… (running)», запуск службы прошел успешно.

7. Изменить аутентификацию по паролю, для этого:

7.1. Открыть «Midnight commander» (см. список доступных команд).

7.2. Открыть путь «/var/lib/pgsql/12/data/», внести изменения в следующие файлы:

7.2.1. Файл «pg_hba.conf»

Строку «local all all peer», изменить на «local all all trust»;
Строку «host all all 127.0.0.1/32 ident», изменить на «host all all 127.0.0.1/32 md5»;
Строку «host all all ::1/128 ident», изменить на «host all all ::1/128 md5».

7.2.2. Файл «postgresql.conf»

Определить все IP-адреса, доступными для прослушивания «listen_addresses = ‘*’».

8.Установить пароль для пользователя «postgres», выполнив команду:

sudo -u postgres psql postgres

8.1. Ввести команду для определения пароля (ввести 2 раза новый пароль, по-умолчанию пароль «postgres»):

\password postgres

9.Создать базу приложения («DBName» может быть произвольным), выполнив команду:

CREATE DATABASE DBName;

10.Выйти из «psql», выполнив команду:

\q

11.Перезапустить службу СУБД, выполнив команду:

systemctl restart postgresql-12

12.Проверить статус службы СУБД, выполнив команду:

systemctl status postgresql-12

Если после проверки статуса, в окне консоли зеленым цветом подсвечено сообщение «active… (running)», запуск службы прошел успешно.

13.Если подключение к базе данных через клиента непроходит, выполнить следующие действия:

13.1. Разрешить подключение к серверу с других машин сети (разрешить connection-порту «Tomcat», указанному в файле «server.xml» принимать запросы из вне), выполнив команду:

sudo firewall-cmd --zone=public --permanent --add-port=5432/tcp

13.2. Перезагрузить «firewall», выполнив команду:

firewall-cmd --reload

3.3 Установка и настройка Tomcat 9

Установить «Tomcat» на сервере приложения сервиса «БФТ.ХЭД.Регион», выполнить следующие действия:

1. Скачать версию «Tomcat», выполнив команду:

wget https://archive.apache.org/dist/tomcat/tomcat-9/v9.0.76/bin/apache-tomcat-9.0.76.tar.gz

2. Создать каталог, выполнив команду:

mkdir -p /opt/Tomcat/das

3. В каталог «das» распаковать данные архива «apache-tomcat-9.0.56.tar.gz», выполнив команду, выполнив команду:

tar xvf apache-tomcat-9.0.68.tar.gz -C /opt/Tomcat/das --strip-components=1

4. Создать каталоги для журналов, выполнив команды:

mkdir -p /var/log/tomcat/das/archiv
rmdir /opt/Tomcat/das/logs
ln -s /var/log/tomcat/das /opt/Tomcat/das/logs
chmod -R 770 /var/log/tomcat
chown -R tomcat:tomcat /var/log/tomcat
restorecon -Rv /var/log/tomcat

5.Создать скрипт для архивации всех журналов (архивирует все журналы на определенную дату и сохраняет архивы в каталоге «_Scripts», в течении недели), для этого:

5.1.Создать каталог для скрипта, выполнив команду:

mkdir -p /root/_Scripts

5.2.Применить скрипт (все строки сразу), выполнив команду:

cat <<EOF > /root/_Scripts/arch_log_date-tomcat.sh

#!/bin/bash

mkdir -p $1/archiv

find $1/*$(date --date '-1 day' +%Y-%m-%d)*.* -exec tar -r -f $1/archiv/$(date --date '-1 day' +%Y%m%d).tar --remove-files {} \; && find $1/archiv/*.tar -exec gzip {} \; && find $1/archiv/*.

tar.gz -mtime +5 -delete

```
chown $2:$3 $1/archiv/*.tar.gz

chmod 640 $1/archiv/*.tar.gz


EOF
```

5.3. Открыть «Midnight commander», каталог «/root/_Scripts/ », проверить скрипт «arch_log_tomcat.sh» на наличие лишних символов (при обнаружении, удалить).

5.4. Сделать файл «arch_log_tomcat.sh» исполняемым (если слева от файла присутствует символ «*», значит файл исполняемый), выполнив команды:

```
cd /root/_Scripts/
chmod u+x arch_log_date-tomcat.sh
```

6.Создать файл–конфигурацию ротации основного журнала «Tomcat» (при активной работе приложения, в «Tomcat» увеличение журнала происходит быстро), выполнив команду:

```
cat <<EOF > /etc/logrotate.d/tomcat
/var/log/tomcat/das/catalina.out
{
    rotate 10
    size 200M
    compress
    notifempty
    missingok
    copytruncate
    su tomcat tomcat
}
EOF
```

7.Открыть «Midnight commander», каталог «/etc/», взять в редактирование файл «crontab», в нижней части файла, добавить две строки, проверить файл на наличие лишних символов (при обнаружении, удалить):

```
0  */12 *  *  * root    logrotate --force /etc/logrotate.d/tomcat > /dev/null 2>&1
0   1   *  *  * root    /root/_Scripts/arch_log_tomcat.sh /var/log/tomcat/das > /dev/null 2>&1
```

8.Изменить порты в конфигурационном файле «Tomcat», если default-порт «8080» занят (если на сервере «Tomcat» в единственном экземпляре, действие пропускаем), для этого:

8.1. Открыть «Midnight commander», каталог «/opt/Tomcat/das/conf/», отредактировать файл конфигурации «server.xml» (изменить значения старых портов +1, на новые значения, как показано в примере ниже):

```
# <Server port="8005"
<Server port="8006"
```

```
# <Connector port="8080" protocol="HTTP/1.1"
#   connectionTimeout="20000"
#   redirectPort="8443" />
<Connector port="8081" protocol="HTTP/1.1"
   connectionTimeout="20000"
   redirectPort="8444" />
# <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
<Connector port="8010" protocol="AJP/1.3" redirectPort="8444" />
```

9.Создать файл «**systemd**-юнит», для запуска «Tomcat» в качестве сервиса, выполнив команду:

```
cat <<EOF >/etc/systemd/system/tomcat-das.service

# Systemd unit file for Tomcat - Application1
[Unit]
Description=Apache Tomcat Web Application Container
After=syslog.target network.target

[Service]
Type=forking

###=-- Каталог установки JDK
### OpenJDK – JRE
# Environment='JAVA_HOME=/usr/lib/jvm/jre'
### OracleJDK – JRE
Environment='JAVA_HOME=/usr/java/latest/jre'

Environment='CATALINA_PID=/opt/Tomcat/das/temp/tomcat.pid'
Environment='CATALINA_HOME=/opt/Tomcat/das'
Environment='CATALINA_BASE=/opt/Tomcat/das'
Environment='CATALINA_OPTS=-Xms512M -Xmx4096M -server -XX:+UseParallelGC'
Environment='JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom'

ExecStart=/opt/Tomcat/das/bin/startup.sh
ExecStop=/bin/kill -15 $MAINPID

User=root
Group=root
UMask=0007
RestartSec=10
Restart=always

[Install]
WantedBy=multi-user.target

EOF
```

9.1. Узнать путь к java (понадобится в п. 9.2.), выполнив команду:

sudo alternatives --config java

9.2. Открыть «Midnight commander», каталог «/etc/systemd/system», файл «tomcat-das.service», проверить на наличие лишних символов (при обнаружении, удалить). Указать путь к «**Oracle java 11**» (см. пункт 9.1.), в параметре «Environment='JAVA_HOME=…», например:

Environment='JAVA_HOME=/usr/lib/jvm/java-11-openjdk-11.0.11.0.9-1.el7_9.x86_64

9.3. Указать «systemd», чтобы он прочитал новые юниты, выполнив команду:

systemctl daemon-reload

10.Добавить «Tomcat» в автозагрузку и запустить, выполнив команду:

sudo systemctl enable tomcat-das.service --now

11.Проверить статус «Tomcat» (если статус «active… running», действие завершено успешно), выполнив команду:

sudo systemctl status tomcat-das.service

12. Открыть «Midnight commander», каталог «/opt/Tomcat/das/~logs/», файл «catalina.out», проверить лог-файл на наличие ошибок.

13.Остановить «Tomcat», выполнив команду:

sudo systemctl stop tomcat-das.service

14.Для всех компонентов проекта «ICE», необходимо предпринять следующие действия:

14.1. Открыть «Midnight commander», каталог «/opt/Tomcat/das/conf/», файл «catalina.properties», в конце файла добавить следующий параметр:

ice.projectRoot=/opt/Tomcat/das

14.2. Создать каталог «.ice», выполнив команду:

mkdir -p /opt/Tomcat/das/.ice

14.3. Выдать права пользователю «tomcat», выполнив команды:

chmod 750 /opt/Tomcat/das/.ice

15.Разрешить подключение к серверу с других машин сети (разрешить connection-порту «Tomcat», указанному в файле «server.xml» принимать запросы из вне), выполнив команду:

sudo firewall-cmd --zone=public --permanent --add-port=8080/tcp

16.Перезагрузить «firewall», выполнив команду:

firewall-cmd --reload

27.Проверить работоспособность сайта «Tomcat» (IP-address:Port) в любом браузере, если сайт открылся, установка завершена.

3.4 Установка VNC-сервера

Установить «VNC-сервер», выполнить следующие действия:

1.Установить графическую оболочку «GNOME», выполнив команду:

sudo dnf groupinstall "Server with GUI"

2.Перезапустить сервер (в левом верхнем углу «PuTTY» нажать ПКМ, из контекстного меню выбрать «Обновить сессию»), выполнив команду:

reboot

3. Установить «VNC-сервер», выполнив команду:

sudo dnf install tigervnc-server

4.Установить пароль (запустить команду от имени пользователя, который будет обращаться к «VNC-серверу», использовать «sudo» ненужно. После того, как пароль будет введен, обратить внимание на порт – это порт «TightVNC VIEWER».), выполнив команду:

vncpasswd

5.Открыть каталог «etc\tigerVNC\», файл «vncserver.users», добавить строку «:port=user» (где «user» - логин вашего пользователя, например «m.larionov», «port» - порт, по которому будет доступна клиентская оболочка, например «1», в этом случае, порт будет 5901).

6.Запустить сервер «vncserver», выполнив команду:

vncserver

7.Настроить службу на автозапуск после каждой перезагрузки системы, выполнив команду:

systemctl daemon-reload

sudo systemctl enable vncserver@:1.service

8. Перезагрузить сервер (в левом верхнем углу «PuTTY» нажать ПКМ, из контекстного меню выбрать «Обновить сессию»), выполнив команду:

reboot

9.Проверить доступность порта (если в п.5 выбран порт «1», в команду прописать порт 5901), выполнив команду

fuser 5901/tcp

9.Войти под пользователем «root», выполнив команду:

sudo mc

10.Запустить и проверить статус службы «VNC-сервер», выполнив команды:

systemctl start vncserver@:1.service

systemctl status vncserver@:1.service

11.Настроить «Firewall», выполнив команду:

sudo firewall-cmd --permanent --zone=public --add-service vnc-server

sudo firewall-cmd --reload

12. Запустить для проверки графическую оболочку «VNC», для этого:

12.1.Открыть «TightVNC Viewer», в окне «New TightVNC Connection», в поле «Remote Host», ввести «ip-address:port» вашего сервера (порт был задан в п.4), нажать «Connect»;

12.2.В окне «Vnc Autentification», в поле «Password» ввести пароль «vncserver», нажать «ОК»;

12.3.В графической оболочке сервера нажать «Activities», выбрать «command».

12.4.Войти под «root» (ввести пароль от вашей учетной записи), выполнив команду

sudo mc

4 Установка и настройка балансировщика

4.1 Установка и настройка балансировщика HAProxy

1. Установить балансировщик, выполнив команду:

yum install haproxy -y

2. Запустить службу «HAProxy» и добавить ее в автозагрузку, выполнив команду:

systemctl enable haproxy

3. Осавить службу:

systemctl stop haproxy

4. Открыть файл на редактирование конфигурационный-файл «haproxy.cfg» (располагается по адресу «etc/haproxy»), добавить содержимое (при необходимости действие выполняется на двух балансировщиках).

```
global
    log         127.0.0.1 local2
    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon
    # turn on stats unix socket
    stats socket /var/lib/haproxy/stats
#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
```

```
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 3000
#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
frontend  main *:8080
    acl url_static       path_beg       -i /static /images /javascript /stylesheets
    acl url_static       path_end       -i .jpg .gif .png .css .js
    stats uri /haproxy?stats
    acl url_app path_beg /app
    use_backend app if url_app
    use_backend static          if url_static
    default_backend             app
#---------------------------------------------------------------------
# static backend for serving up images, stylesheets and such
#---------------------------------------------------------------------
backend static
    balance     roundrobin
    server      static 127.0.0.1:4331 check
#---------------------------------------------------------------------
# round robin balancing between the various backends
#---------------------------------------------------------------------
backend app
    balance     leastconn
    server  app1 172.25.32.38:8080/app check
    server  app2 172.25.32.39:8080/app check
```

5. Запустить балансировщик, выполнив команду:

```
systemctl start haproxy
```

5 Установка приложения «БФТ.ХЭД.Регион»

Установить приложение «БФТ.ХЭД.Регион», выполнить следующие действия.

5.1 Создание базы данных для «БФТ.ХЭД.Регион»

Создать базу данных «БФТ.ХЭД.Регион», выполнить следующие действия:

1.Войти в СУБД, выполнив команду:

sudo -u postgres psql postgres

2.Создать БД, выполнив команду:

CREATE DATABASE das;

3.Выйти из СУБД, выполнив команду:

\q

5.2 Копирование сборки «БФТ.ХЭД.Регион»

Скопировать и распаковать сборку «БФТ.ХЭД.Регион», выполнить следующие действия:

1.Запросить у разработчика «БФТ.ХЭД.Регион» файл-сборку «app.war», или скачать с «TeamCity» самостоятельно (ветка «DocArchive\DocArchive Structured\1.7.0\1-Build»).

2.Перенести архив «app.war» на сервер, где расположен «Tomcat», в каталог «/home» (использовать программу «WinSCP»), для этого:

2.1.Авторизоваться в программе «WinSCP»;

2.2.Выделить файл «app.war» (на вашей машине), нажать «F5».

3.Войти под root, выполнив команду:

sudo mc

4.Открыть «Midnight commander», проверить наличие файла «app.war» в каталоге «/home/user» (где «user» - ваша учетная запись)

5.Открыть «Midnight commander», скопировать архив сборки «app.war», в каталог «/opt/Tomcat/das/webapps» (директория подготовленной сборки «Tomcat», для «БФТ.ХЭД.Регион»).

6.Запустить службу «Tomcat», выполнив команду (дождаться, пока распакуется файл сборки «app.war»):

sudo systemctl start tomcat-das.service

7.Открыть «Midnight commander», проверить распаковку сборка в каталоге «/opt/Tomcat/das/webapps/app».

8.Открыть «Midnight commander», скопировать файлы «application.properties» и «logback.xml», из каталога «/opt/Tomcat/das/webapps/app/WEB-INF/classes», в каталог «/opt/Tomcat/das».

5.3 Установка «JODConverter»

Установить «JODConverter» (необходим для обеспечения возможности просмотра вложений загруженных в «БФТ.ХЭД.Регион» через браузер), выполнить следующие действия:

1.Получить самую свежую версию программы, для этого необходимо сначала добавить официальный репозиторий Docker в систему командой:

dnf config-manager --add-repo=https://download.docker.com/linux/centos/docker-ce.repo

2. Установка Docker для CentOS 8 выполняется командой:

dnf install docker-ce

Важно: Если будет ошибка: try to add '--allowerasing' to command line to replace conflicting packages or '--skip-broken' to skip uninstallable packages or '--nobest' to use not only best candidate packages, то запускаем с параметром --allowerasing

dnf install docker-ce --allowerasing

3.Запусть службу Docker и добавить её в автозагрузку:

systemctl enable docker --now
systemctl status docker

4. Поскольку CentOS 8 перешла на новую подсистему брандмауэра - nftables, а Docker поддерживает только iptables, то сеть внутри контейнеров работать не будет.
Чтобы это исправить надо включить трафик masquerade с помощью firewalld:

firewall-cmd --zone=public --add-masquerade --permanent

Затем перезагрузите фаервол, чтобы правила активные обновились:

firewall-cmd –reload

5.Установить инструмент автоматического развертывания и конфигурирования контейнеров docker-compose:

wget https://github.com/docker/compose/releases/download/1.25.0/docker-compose-$(uname -s)-$(uname -m)

6.Перемещаем файл:

mv ./docker-compose-Linux-x86_64 /usr/local/bin/docker-compose

Соглашаемся, если предлагает перезаписать: yes

Делаем файл исполняемым:
chmod +x /usr/local/bin/docker-compose

7.Проверяем установленные версии:
docker --version
docker-compose --version

Важно: Если после команды docker-compose --version будет ошибка bash: docker-compose: command not found..., то надо выполнить команду:

sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose

8.Создаём каталог, где будут храниться данные и конфигурационные файлы:

sudo mkdir -p /opt/_Docker/jodconverter

9.Создаём файл /opt/_Docker/jodconverter/docker-compose.yaml:

cd /opt/_Docker/jodconverter
touch docker-compose.yaml

10.С следующим содержанием:

```
version: '3.7'
services:
  converter_to_pdf:
#   image: eugenmayer/jodconverter:rest
# адрес расположения файла образа
    image: srv-nexus-3.bftcom.com:5000/common/jodconverter:rest
    restart: always
    labels:
      - name_service=converter_to_pdf
    networks:
      - ice_conv_net
    ports:
      - 8081:8080
networks:
  ice_conv_net:
    driver: bridge
```

, где 8081 номер порта для JODConverter.
Вне сети БФТ файл образа выкладывается в регистр Docker.

После сохранения файла «docker-compose» требуется проверить его на наличие некорректных символов.

11.Открываем порты:

sudo firewall-cmd --permanent --add-service=kibana --add-service=jodconverter
sudo firewall-cmd -reload

12. Если устанавливаете JODConverter из регистра Docker, то запустить из папки с файлом следующей командой:

docker load -i [сборка jodconverter]

Запускаем JODConverter из папки с файлом «docker-compose.yaml» следующей командой:

docker-compose up -d

13.Команда для проверки работающих контейнеров:

docker ps

14. Добавить опцию в файл **catalina.properties** (находится по адресу /opt/Tomcat/das/conf/)

ice.converter.url=http://localhost:8081/lool/convert-to

, где 8081 порт заданный в файле docker-compose, а Docker разворачивается на этой же машине.

5.4 Установка «LibreOffice»

Установить «LibreOffice» (необходим для обеспечения возможности просмотра вложений загруженных в «БФТ.ХЭД.Регион» через браузер), выполнить следующие действия:

1. Установить «LibreOffice», для этого:

1.1. Открыть «Midnight commander», каталог «/home/user» (где «user» - ваша учетная запись).

1.2. Скачать «LibreOffice», выполнив команду:

wget https://download.documentfoundation.org/libreoffice/stable/7.5.7/rpm/x86_64/LibreOffice_7.5.7_Linux_x86-64_rpm.tar.gz

1.3. Распаковать «LibreOffice», выполнив команду:

tar -xvf LibreOffice_7.5.7_Linux_x86-64_rpm.tar.gz

1.4. Открыть «Midnight commander», каталог «/home/user/LibreOffice_7.5.7_Linux_x86-64.rpm/RPMS» (где «user» - ваша учетная запись).

1.5. Установить «LibreOffice» (каталог установки «/opt/», будет определен по умолчанию), выполнив команду:

yum localinstall *.rpm

2.Установить русификатор для «LibreOffice», для этого:

2.1. Открыть «Midnight commander», каталог «/home/user» (где «user» - ваша учетная запись).

2.2.Скачать русификатор для «LibreOffice», выполнив команду:

wget http://download.documentfoundation.org/libreoffice/stable/7.3.2/rpm/x86_64/LibreOffice_7.5.7_Linux_x86-64_rpm_langpack_ru.tar.gz

2.3..Распаковать русификатор для «LibreOffice», выполнив команду:

tar -xvf LibreOffice_7.5.7_Linux_x86-64_rpm_langpack_ru.tar.gz

2.4.Открыть «Midnight commander», каталог «/home/user/LibreOffice_7.5.7_Linux_x86-64.rpm/RPMS» (где «user» - ваша учетная запись).

2.5.Установить русификатор для «LibreOffice», выполнив команду:

yum localinstall *.rpm

5.5 Настройка файла «application.properties»

Настроить файл «application.properties», выполнить следующие действия:

1.Создать каталог «data_docarchiv», выполнив команду:

mkdir -p /home/drive_das/data_docarchiv

2.Создать базу данных (на сервере БД), выполнив команду:

CREATE DATABASE das;

2.1. Проверить создание БД, выполнив команду:

\l

3.Открыть «Midnight commander», каталог «/opt/Tomcat/das/», файл «application.properties», отредактировать следующие параметры:

3.1. В параметре «ice.rls.enabled», установить значение «false»;

3.2.В параметрах подключения к БД, добавить следующие значения:

spring.datasource.url=jdbc:postgresql://localhost:5432/das

spring.datasource.username=postgres

spring.datasource.password=postgres

3.3. После параметра «jodconverter.local.enabled=true», добавить строку с параметром «jodconverter.local.officeHome=/opt/libreoffice7.3»;

3.4.В параметре «docarch.jms.outbound.queue.name», добавить значение «docArchiveJsonOutgoingQueueDAS»;

3.5.В параметре «docarch.jms.inbound.queue.name», добавить значение «docArchiveJsonIncomingQueueDAS»;

3.6.После параметра «docarch.fsDirectory=files/attaches», добавить строку с параметром «docarch.fileStorage.directory=/home/drive_das/data_docarchiv»;

3.7.В параметре «docarch.storageType», добавить значение «fileStorage»

3.8.Добавить параметры в конец файла:

service.user.login=root

service.user.password=root

5.6 Редактирование файла «logback.xml»

Настроить редактирование файла «logback.xml», выполнить следующие действия:

1.Создать каталог, выполнить команду:

mkdir -p /home/drive_das/logs/log/log_archived

2. .Открыть «Midnight commander», каталог «/opt/Tomcat/das», файл «logback.xml», отредактировать следующие параметры:

2.1.В параметре «<File </File>», добавить значение «/home/drive_das/logs/log/das.log»;

2.2.В параметре «<FileNamePattern></FileNamePattern>», добавить значение

«/home/drive_das/logs/log_archived/das.%d{yyyy-MM-dd}.%i.log.zip»;

2.3.В параметре «<maxFileSize></maxFileSize>», добавить значение «100MB»;

2.4.В параметре «<root level="">», добавить значение «DEBUG»;

2.5. Внутри параметра «<root level="DEBUG">» (см. п.2.4.), в строке «<appender-ref ref=""/>», добавить значение «DEBUG»;

2.6.Добавить параметры вконец файла:

<logger name="org.springframework.transaction">

<level value="DEBUG" />

</logger>

<logger name="com.bftcom.azk3.server.replication.ReplicationService">

<level value="DEBUG" />

</logger>

5.7 Настройка файла «catalina.properties»

Настроить файл «catalina.properties», выполнить следующие действия:

1.Открыть «Midnight commander», каталог «/opt/Tomcat/das/conf/» , файл «catalina.properties», добавить строки с параметрами в конец файла:

spring.config.location=file:/opt/Tomcat/das/application.properties

logging.config=file:/opt/Tomcat/das/logback.xml

logback.configurationFile=/opt/Tomcat/das/logback.xml

5.8 Открытие порта «Tomcat»

Открыть порт «Tomcat», добавить его в исключения «firewall», выполить следующие действия:

1.Добавить коннектор-порт «Tomcat» (порт указан в каталоге «/opt/Tomcat/piv/conf/», файле «server.xml») в исключения «firewall», выполнив команду:

firewall-cmd --permanent --service=http --add-port=8081/tcp

2.Добавить конфигурацию http-сервиса к разрешенным, выполнив команду:

firewall-cmd --permanent --add-service=http

3.Перезапустить firewall (для применения правил), выполнив команду:

sudo firewall-cmd --reload

5.9 Открытие порта базы данных

Открыть порт базы данных, выполнить следующие действия:

1.Открыть порт, выполнить команду:

firewall-cmd --permanent --service=http --add-port=5432/tcp

2. Добавить конфигурацию http-сервиса к разрешенным, выполнив команду:

firewall-cmd --permanent --add-service=http

3.Перезапустить firewall (для применения правил), выполнив команду:

sudo firewall-cmd --reload

5.10 Первый запуск «БФТ.ХЭД.Регион»

Запустить «БФТ.ХЭД.Регион», выполнить следующие действия:

1.Открыть «Midnight commander», каталог «/opt/Tomcat/das/logs/», выделить все файлы, (нажать «*»), удалить (нажать «F8»).

2.Запустить экземпляр «Tomcat», выполнив команду:

tomcat: sudo systemctl start tomcat-das.service

3.Открыть «Midnight commander», каталог «/opt/Tomcat/das/logs/», файл «catalina.out», проверить лог на наличие ошибок.

4.Открыть «Midnight commander», каталог «/home/drive_das/logs/log/» файл «das.log», проверить лог на наличие ошибок.

5.Проверить доступность сервиса на своей машине, ввести в адресную строку браузера следующий адрес (где «server» - «ip-address» сервера приложения, «port» - «connection port» см. раздел «4.7.», п.1.)

«http://server:port/app»

5.11 Установка прикладного веб-сервиса «DocArchiveAPI»

Установить веб-сервис «DocArchiveAPI», выполнить следующие действия:

1) Установить «Tomcat» (см. п.3.3 Установка и настройка Tomcat 9).

2) Проверить, статус «Tomcat», выполнив команду (если оператор «active» = «(running)», «Tomcat» запущен):

systemctl status dockarchive-api-[port].service

где [port] – порт «Tomcat»

3) Запросить у разработчика «БФТ.ХЭД.Регион» файл-сборку «api.war».

4) Выложить файл-сборку «api.war» в директорию установки «Tomcat», каталог «webapps», дождаться извлечения артефакта в каталог «api».

5) Настроить конфигурационный файл «catalina.properties», выполнить следующие действия:

Открыть директорию установки «Tomcat», каталог «conf», взять на редактирование файл «catalina.properties»;

В параметре «spring.profiles.active», указать значение «s3,da»;

В параметре «da.base-url», в качестве значения, указать ссылку на стенд системы «Хра-нилище электронных документов» (например «http://[server]:[port]/app», где [server] - IP-адрес сервера, [port] - порт «Tomcat»);

В параметре «da.enable-da-user-auth», указать значение «false»;

В параметре «da.login», в качестве значения, указать логин технического пользователя, для доступа в систему «Хранилище электронных документов»;

В параметре «da.password», в качестве значения, указать пароль технического пользователя, для доступа в систему «Хранилище электронных документов»;

В параметре «das.base-url», в качестве значения, указать ссылку на стенд системы «Хранилище электронных документов» (например «http://[server]:[port]/app» , где [server] - IP-адрес сервера, [port] - порт «Tomcat»);

В параметре «das.login», в качестве значения, указать логин технического пользователя, для доступа в систему «Хранилище электронных документов»;

В параметре «das.password», в качестве значения, указать пароль технического пользо-вателя, для доступа в систему «Хранилище электронных документов»;

В параметре «s3.url», в качестве значения, указать ссылку на хранилище;

В параметре «s3.key», в качестве значения, указать ключ доступа к хранилищу;

В параметре «s3.secret», в качестве значения, указать секретный ключ доступа к храни-лищу;

В параметре «s3.bucket», в качестве значения, указать название основного контейнера «s3»;

В параметре «s3.temp-bucket», в качестве значения, указать название временного контейнера «s3»;

В параметре «s3.relaxed-ssl», указать значение «false» (игнорирование ошибок связанных с «SSL»);

В параметре «s3.use-region», указать значение «false» в случае, если не используем регион (значение по-умолчанию);

В параметре «s3.auto-create-bucket», в качестве значения указать «false» (параметр про-веряет наличие контейнера, в случае его отсутствия, выводится ошибка);

В параметре «s3.temp.cleaner.enabled», в качестве значения указать «false», с целью ис-ключения возможности очистки файлов, загруженных в хранилище «s3»;

В параметре «management.endpoints.web.exposure.include», указать значение «*»;

В параметре «management.endpoint.health.show-details», указать значение «always»;

В параметре «management.metrics.distribution.percentiles-histogram.http.server.requests», указать значение «true»;

Сохранить изменения в файле «Catalina.properties».

6) Настроить конфигурационный файл «application-s3.yml», выполнить следующие действия:

Открыть директорию установки «Tomcat», каталог «/webapps/api/WEB-INF/classes», взять на редактирование файл «application-s3.yml»;

В параметре «url», в качестве значения, указать ссылку на хранилище;

В параметре «key», в качестве значения, указать ключ доступа к хранилищу;

В параметре «secret», в качестве значения, указать секретный ключ доступа к хранилищу;

В параметре «bucket», в качестве значения, указать название основного контейнера «s3»;

В параметре «temp-bucket», в качестве значения, указать название временного контейнера «s3»;

В параметре «relaxed-ssl», указать значение «false» (игнорирование ошибок связанных с «SSL»);

В параметре «use-region», указать значение «false» в случае, если не используем регион (значение по-умолчанию);

В параметре «auto-create-bucket», в качестве значения указать «false» (параметр проверяет наличие контейнера, в случае его отсутствия, выводится ошибка);

Сохранить изменения в файле «application-s3.yml».

7) Настроить конфигурационный файл «application.yml», выполнить следующие действия:

Открыть директорию установки «Tomcat», каталог «/webapps/api/WEB-INF/classes», взять на редактирование файл «application.yml»;

В группе параметров «spring», параметре «profiles», указать значение «s3,das»;

В группе параметров «server», параметре «port», указать порт, который использует «Tomcat» веб-сервиса «DocArchiveAPI»;

8) Перезапустить веб-сервис «DocArchiveAPI», выполнив команду:

systemctl restart dockarchive-api-[port].service

где [port] – порт «Tomcat»

9) Проверить статус «Tomcat», выполнив команду (если оператор «active» = «(running)», «Tomcat» запущен):

systemctl status dockarchive-api-[port].service

где [port] – порт «Tomcat»

10) Проверить работоспособность веб-сервиса «DocArchiveAPI», открыть в браузере ссылку «http://[server]:[port]/api» (где «server» - IP-адрес сервера, «port» - порт «Tomcat»).

Веб-сервис «DocArchiveAPI» считается корректно работающим, если при его открытии, в браузере появится сообщение «Whitelabel Error Page».

5.12 Предварительная настройка «JAVA JDK»

Настроить «JAVA JDK», выполнить следующие действия:

1.Обновить «cache», выполнив команду:

sudo yum makecache

2.Установить «**Oracle java 8»**, выполнив команду:

sudo yum install java-1.8.0-openjdk

2.1.Если на машине установлено 2 и более версии «**Oracle java**», выполнить команду:

sudo alternatives --config java

Выбрать нужную версию «**Oracle java 8**», ввести ее порядковый номер, нажать Enter

3.Создать каталог, выполнить команду:

mkdir -p /usr/java/jdk-8

4.Создать символическую ссылку (чтобы узнать путь к «**Oracle java 8**», см. п.2.1.), выполнить команду

sudo ln -s /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.312.b07-2.el8_5.x86_64/jre /usr/java/jdk-8/jre

5.13 Создание базы данных для «СЭП»

Создать базу данных для «СЭП», выполнить следующие действия:

1.Войти в СУБД, выполнив команду:

sudo -u postgres psql postgres

2.Создать базу данных, выполнив команду:

CREATE DATABASE eds;

3.Создать роль «bfteds_user», выполнив команду:

CREATE ROLE bfteds_user LOGIN ENCRYPTED PASSWORD 'md567ba111a82b6a5fb71273ba1b14ddf71' NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;

4.Выйти с СУБД, выполнив команду:

\q

5.14 Установка и настройка «Крипто Про JCP»

Установить и настроить «Крипто Про JCP», выполнить следующие действия:

1.Скачать дистрибутивы «Крипто Про JCP» (версию «2.0.41789» и выше) и «jce_policy-8» (отключить vpn-клиент «cisco») по следующим ссылкам:

http://www.cryptopro.ru/products/csp/jcp/downloads

https://www.oracle.com/ru/java/technologies/javase-jce8-downloads.html#license-lightbox

2.Перенести архивы «jce_policy-8.zip» и «jcp-2.0.41789.zip» на сервер «СЭП», в каталог «/home» (использовать программу «WinSCP»), для этого:

2.1. Авторизоваться в программе «WinSCP»;

2.2. Выделить файлы «jce_policy-8.zip» и «jcp-2.0.41789.zip» (на вашей машине), нажать «F5».

3. Выполнить вход на сервер с помощью графической оболочки «TightVNC» (если «TightVNC» у вас неустановлен, см. раздел «3.5. Установка VNC-сервера»), для этого:

3.1. Открыть «TightVNC Viewer», в окне «New TightVNC Connection», в поле «Remote Host», ввести «ip-address:port» вашего сервера, нажать «Connect»;

3.2.В окне «Vnc Autentification», в поле «Password» ввести пароль «vncserver», нажать «ОК»;

3.3.В графической оболочке сервера нажать «Activities», выбрать «Terminal».

3.3.1. Войти под «root» (ввести пароль от вашей учетной записи), выполнив команду

sudo mc

3.3.2. Открыть «Midnight commander», каталог «/home/user/» (где «user» – ваша учетная запись), выполнить команду:

unzip -d /var/tmp/jcp jcp-2.0.41789.zip

3.3.3. Открыть «Midnight commander», каталог «/var/tmp/jcp/jcp-2.0.41789», выполнить команду установки:

./setup_gui.sh /usr/java/jdk-8/jre

3.3.3.1. Последовательность установки:

Выбрать «Русский язык», нажать «Далее»;

Нажать 2 раза «Далее» (ничего не меняем);

Установить галку в поле «Модули Cades...",», нажать «Далее»;

Ключ не вводить (у нас «Trial» версия);

В окне «Установка» снять галку в поле «Запустить панель управления»;

Нажать «Установка».

3.3.4.Открыть «Midnight commander», каталог «/var/tmp/jcp/jcp-2.0.41789», выделить файлы «AdES-core.jar», «CAdES.jar», «cpSSL.jar» и «XAdES.jar», скопировать в каталог «/usr/java/jdk-8/jre/lib/ext»;

3.3.5. Открыть «Midnight commander», каталог «/var/tmp/jcp/jcp-2.0.41789/dependencies», выделить файлы «commons-logging-1.2.jar» и «xmlsec-1.5.0.jar», скопировать в каталог «/usr/java/jdk-8/jre/lib/ext»;

3.3.6. Открыть «Midnight commander», каталог «/var/tmp/jcp/jcp-2.0.41789/dependencies», выделить файлы «bcpkix-jdk15on-1.60.jar» и «bcprov-jdk15on-1.60.jar», скопировать в каталог «/usr/java/jdk-8/jre/lib/ext»;

5.15 Установка приложения «СЭП»

Установить приложение «СЭП», выполнить следующие действия:

1.Запросить у разработчика сборку «СЭП».

2.Перенести архив «СЭП» на сервер, в каталог «/home/user» (использовать программу «WinSCP»), для этого:

2.1. Авторизоваться в программе «WinSCP»;

2.2. Выделить файл (на вашей машине), нажать «F5».

3.Создать каталоги, выполнив команду:

mkdir -p /etc/bftcom/log-configs/eds/

mkdir -p /etc/bftcom/configs/eds/

4.Открыть «Midnight commander», проверить наличие пакета-установщика «СЭП» в каталоге «/home/user» (где «user» - ваша учетная запись).

4.1. Установить пакет «eds.assembly-1.0.XX.noarch.rpm» (вместо .XX. указать версию, например 163-1):

yum install -y eds.assembly-1.0.210-1.noarch.rpm

5.Остановить службу «СЭП», выполнив команду:

systemctl stop eds

6.Переименовать файлы, выполнив команды:

6.1.Открыть каталог «/etc/bftcom/configs/eds/»

cd /etc/bftcom/configs/eds/

6.2.Переименовать файлы, выполнив команды

mv application.yaml.example application.yaml

mv hikari.properties.example hikari.properties

6.3.Открыть каталог «/etc/bftcom/log-configs/eds/»

cd /etc/bftcom/log-configs/eds/

6.4.Переименовать файл, выполнив команды

mv logback.xml.example logback.xml

7. Узнать путь к «**Oracle java 8**» (понадобится в п.18), выполнив команду**:**

sudo alternatives --config java

8.Открыть «Midnight commander», каталог «/etc/sysconfig», файл «eds», в параметре «JAVA_HOME» указать путь к «**Oracle java 8**», например «/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.312.b07-2.el8_5.x86_64»

9.Открыть «Midnight commander», каталог «/etc/bftcom/configs/eds/», отредактировать перечень файлов:

9.1.Открыть файл «application.yaml», изменить параметр «port: 8080», на «port: 8090»:

- server:

    port: 8090

- hikari:

    properties-path: /etc/bftcom/configs/eds/hikari.properties

9.2.Открыть файл «hikari.properties», изменить «localhost», на «ip-address» сервера БД, изменить «eds», на alias БД:

- jdbcUrl=jdbc:postgresql://localhost:5432/eds

- username=postgres

- password=postgres

10.Открыть «Midnight commander», каталог «/etc/bftcom/log-configs/eds/», файл «logback.xml», изменить параметр «<property name="LOG_FILE_NAME" value="/var/log/bftcom/eds/eds" />».

11.Перезагрузить настройки «systemd», выполнив команду:

sudo systemctl daemon-reload

12.Запустить службу «СЭП», выполнив команду:

systemctl start eds

13.Проверить статус службы «СЭП», выполнив команду:

systemctl status eds

14.Проверить, запущен сервис, или нет, с помощью команды (порт «8080», был изменен ранее на «8090»):

fuser 8090/tcp

15.Открыть «Midnight commander», каталог «/var/log/bftcom/eds», проверить файл с логами «eds.log» на наличие ошибок.

16.Запустить графическую оболочку «VNC», проверить запуск интерфейса «swagger» в браузере, для этого:

16.1.Открыть «TightVNC Viewer», в окне «New TightVNC Connection», в поле «Remote Host», ввести «ip-address»:«port» вашего сервера, нажать «Connect»;

16.2.В окне «Vnc Autentification», в поле «Password» ввести пароль «vncserver», нажать «ОК»;

16.3.В графической оболочке сервера нажать «Activities», выбрать браузер (например «Firefox»).

16.4.В адресную строку браузера вставить ссылку http://localhost:8090/eds/swagger-ui.html, если сайт открылся, действие завершено успешно.

5.16 Открытие порта «СЭП»

Открыть порт «СЭП», выполнить следующие действия:

1.Добавить порт «8090» (ранее был использован «8080»), выполнив команду:

firewall-cmd --permanent --service=http --add-port=8090/tcp

2.Добавить конфигурацию сервиса «http» к разрешенным, выполнив команду:

firewall-cmd --permanent --add-service=http

3.Перезапустить «firewall» (для применения правил), выполнив команду:

firewall-cmd --reload

5.17 Создание и импорт сертификата

Создать и импортировать сертификат, выполнить следующие действия:

1.Запустить графическую оболочку «VNC» (см. раздел «3.5.Установка VNC-сервера»), для этого:

1.1.Открыть «TightVNC Viewer», в окне «New TightVNC Connection», в поле «Remote Host», ввести «ip-address»:«port» вашего сервера, нажать «Connect»;

1.2.В окне «Vnc Autentification», в поле «Password» ввести пароль «vncserver», нажать «ОК»;

1.3.В графической оболочке сервера нажать «Activities», выбрать «Terminal».

1.3.1.Войти под «root», выполнив команду:

sudo mc

1.3.2.Открыть «Midnight commander», каталог «/var/tmp/jcp/jcp-2.0.41789», запустить графический интерфейс «Крипто Про JCP», выполнив команду:

./ControlPane.sh /usr/java/jdk-8/jre

1.3.2.1.В окне «CryptoPro JCP settings» открыть вкладку «Keys and certificates stores», в списке «Container Stores» выбрать «HdImageStore», нажать «Create»;

1.3.2.2.В окне «Keys generation» изменить настройки следующим образом:

Установить галку в поля «Exchange key» и «Server authentication».

В поле «New container name» ввести имя контейнера «das».

В поле «Certificate subject name» добавить значение «CN=Alias,O=CryptoPro,C=RU» (где «Alias» - имя вашего сертификата).

В выпадающем списке «Provider type» выбрать значение «GOST R 34.10-2012 (256)…».

Нажать «Generate».

1.3.2.3.В окне «Random Generator Initialization» перемещать мышь в различных направлениях для формирования хеша ключа электронной подписи.

1.3.2.4.В окне «Certificate request», в области «Request coding», выбрать кодировку «DER», нажать «Save».

1.3.2.5.В окне «Save», в поле «File name» присвоить имя сертификату «das.reg», сохранить сертификат в каталог «/root».

1.3.2.6.В окне «CryptoPro JCP settings», открыть вкладку «Keys and certificates stores», в списке «Container Stores» раскрыть «HdImageStore», кликнуть дважды на контейнер «das»:

В окне «Password input» установить флаг в пункт «don’t set password», нажать «ОК».

1.3.2.7.В окне «CryptoPro JCP settings», открыть вкладку «Keys and certificates stores», в списке «Container Stores» раскрыть «HdImageStore»/«das»/«Exchange key and setificates», кликнуть дважды мышью по строке «CN=das».

В окне «Certificate view» выбрать вкладку «Details», нажать «Export».

В окне «Save» заполнить поля, выполнить экспорт сертификата:

- В поле «Save to» выбрать каталог «/home/user» (где «user» - имя вашей учетной записи).

- В поле «File name» указать имя сертификата «das.cer»

- Нажать «Save»/

1.3.2.8.В окне «CryptoPro JCP settings» нажать «ОК»/

1.4. В графической оболочке сервера нажать «Activities», выбрать браузер (например «Firefox).

1.4.1.В адресной строке браузера ввести ссылку на «БФТ.ХЭД.Регион» в следующем виде (для определения значения «port», см п.1.4.1.1.):

«http://localhost:port/app/#/)»

1.4.1.1.Открыть «Midnight commander», каталог «/opt/Tomcat/das/conf», файл «server.xml», найти значение параметра «Connector port»

1.4.2.Авторизоваться на сайте под учетной записью «root»/«root»

1.4.3.В верхней части рабочей области сайта выбрать раздел «Администрирование», вкладку «Сертификаты».

1.4.4.В рабочей области вкладки «Сертификат» нажать «Импорт сертификата».

1.4.5.В проводнике открыть каталог «/home/user» (где «user» - имя вашей учетной записи), выбрать файл «das.cer», нажать «Open».

5.18 Редактирование файла «application.properties»

Отредактировать файл «application.properties», выполнить следующие действия:

1.Открыть «Midnight commander», каталог «/opt/tomcat/das», файл «application.properties».

1.1.Указать адрес «СЭП» в параметре «ice.sign.eds.url=http://localhost:8090/eds».

2.Перезапустить «Tomcat», выполнив команду:

sudo systemctl restart tomcat-das.service

3.Открыть «Midnight commander», каталог «opt/tomcat/das/logs», выделить все файлы, (нажать «*»), удалить (нажать «F8»).

4.Открыть «Midnight commander», каталог «/data/drive_das/logs/log/», выделить все файлы, (нажать «*»), удалить (нажать «F8»).

5.Открыть «Midnight commander», каталог «/opt/Tomcat/das/logs», файл «catalina.out», проверить лог на наличие ошибок.

6.Проверить доступность web-приложения «БФТ.ХЭД.Регион», для этого:

6.1.В адресной строке браузера ввести ссылку на web-приложение «БФТ.ХЭД.Регион» в следующем виде (для определения значения «port», см п.6.2):

«http://server:port/app/#/)»

6.2.Открыть «Midnight commander», каталог «/opt/Tomcat/das/conf», файл «server.xml», найти значение параметра «Connector port».

5.19 Добавление контейнера с сертификатом через «swagger»

Добавить контейнер с сертификатом через «swagger», выполнить следующие действия:

1.Открыть «Midnight commander», каталог «/var/opt/cprocsp/keys/root» скопировать файл «das.000» в каталог «/var/opt/cprocsp/keys/eds_user».

2.Выдать права на контейнер пользователю и группе «eds_user», выполнив команду:

sudo chown -R eds_user:eds_user /var/opt/cprocsp/keys/eds_user

3.Скопировать сертификат с сервера «СЭП» на свою рабочую машину (использовать программу «WinSCP»), для этого:

3.1. Авторизоваться в программе «WinSCP»;

3.2.Выделить файл «das.cer», скопировать на свою рабочую машину (нажать F5) .

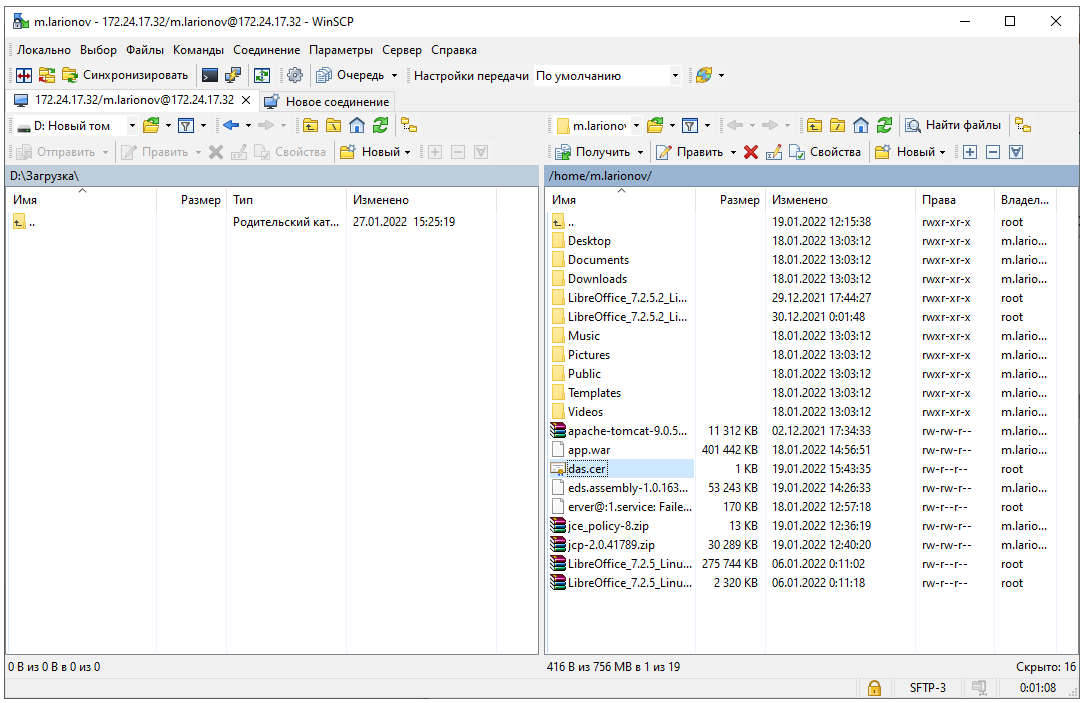

Рисунок 2 Копирование файла «das.cer»

4..Открыть «Midnight commander», каталог «/etc/bftcom/configs/eds/», файл «application.yaml», найти значение параметра «port» (понадобится в п.5.).

5.Открыть «swagger» на своей рабочей машине (для определения значения «port», см п.4, вместо «server» добавить ip-address сервера «СЭП»).

http://server:port/eds/swagger-ui.html

5.1.В «swagger» открыть «administration-controller», выбрать «Регистрация приватного ключа», нажать «Try it out», заполнить следующие поля:

В поле «Authorization» добавить значение «Basic YWRtaW46cGF2bGlu».

В поле «keyAlias» добавить имя ключа (открыть «Midnight commander», каталог «/var/opt/cprocsp/keys/eds_user/das.000/», файл «name.key»).

В поле «keyPassword» ничего не добавлять.

Нажать «Execute».

5.2. В «swagger» открыть «cert controller», выбрать «Добавить сертификат в хранилище», нажать «Try it out», нажать «Выбрать файл», импортировать файл «das.cer» (для определения пути к сертификату см. п.3.), нажать «Execute».

5.2.3.Выполнить скрипты на сервере БД, для этого

5.2.3.1.Подключиться к БД, выполнив команды:

sudo -u postgres psql postgres

\c eds;

5.2.3.2.Определить «id» контейнера, выполнив скрипт («id»=1):

select * from container;

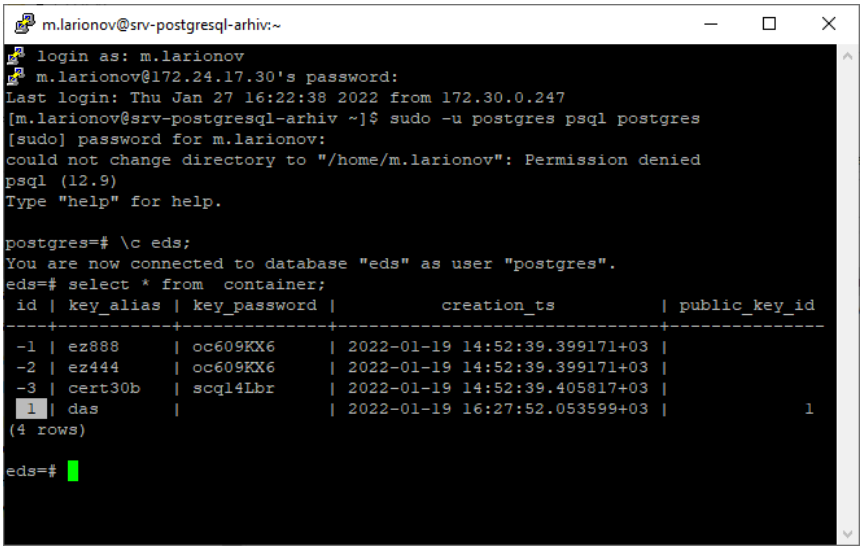

Рисунок 3 Определение «id» контейнера

5.2.3.3.Определить «id» сертификата, выполнив скрипт («id»=1):

select * from public_key;

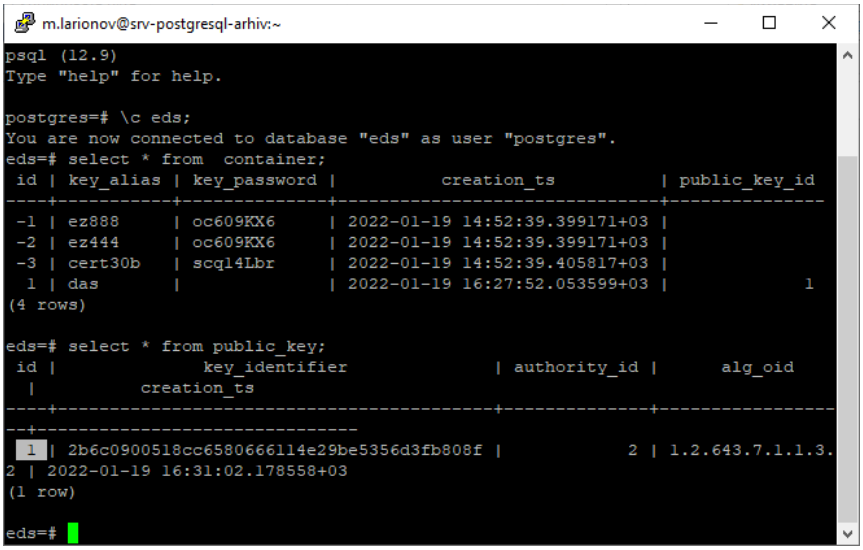

Рисунок 4 Определение «id» сертификата

5.3. В «swagger» открыть «administrator-controller», выбрать «Привязывает публичный ключ к контейнеру», нажать «Try it out», заполнить следующие поля:

В поле «containerId» добавить «id» контейнера (см. п. 5.2.3.2.).

В поле «keyId» добавить «id» сертификата (см. п. 5.2.3.3.).

Нажать «Execute».

5.4. В «swagger» открыть «authority-test-controller», выбрать «Добавляет новый аккредитованный УЦ», нажать «Try it out», заполнить следующие поля:

В поле «name» добавить «TEST».

В поле «ogrn» добавить «11111».

Нажать «Execute».

5.4.1.Выполнить скрипт на сервере БД, для этого:

5.4.1.1.Подключиться к БД, выполнив команды:

sudo -u postgres psql postgres

\c eds;

5.4.1.2.Определить «id» удостоверяющего центра, выполнив скрипт («id»=2):

select * from authority;

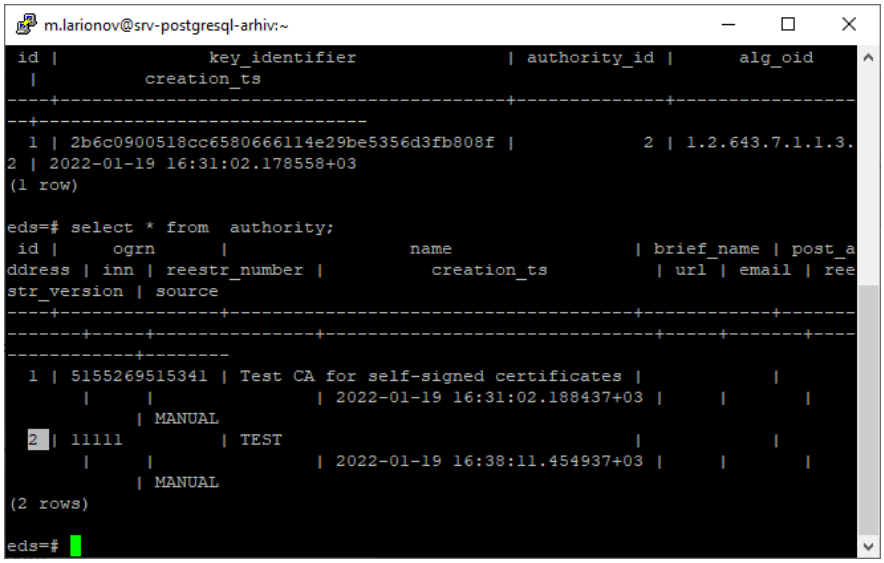

Рисунок 5 Определение «id» УЦ

5.5. В «swagger» открыть «authority-test-controller», выбрать «Добавляет новое событие в историю аккредитации УЦ», нажать «Try it out», заполнить следующие поля:

В поле «authId» добавить значение «2» (см п. 5.4.1.2.).

В поле «state» выбрать значение «ACTIVE».

В поле «validFromEpoch» добавить значение «1000000000000».

Нажать «Execute».

5.5.1.Выполнить скрипт на сервере БД, для этого:

5.5.1.1.Подключиться к БД, выполнив команды:

sudo -u postgres psql postgres

\c eds;

5.5.1.2.Определить «id» события, выполнив скрипт («id»=2):

select * from authority_accr_history;

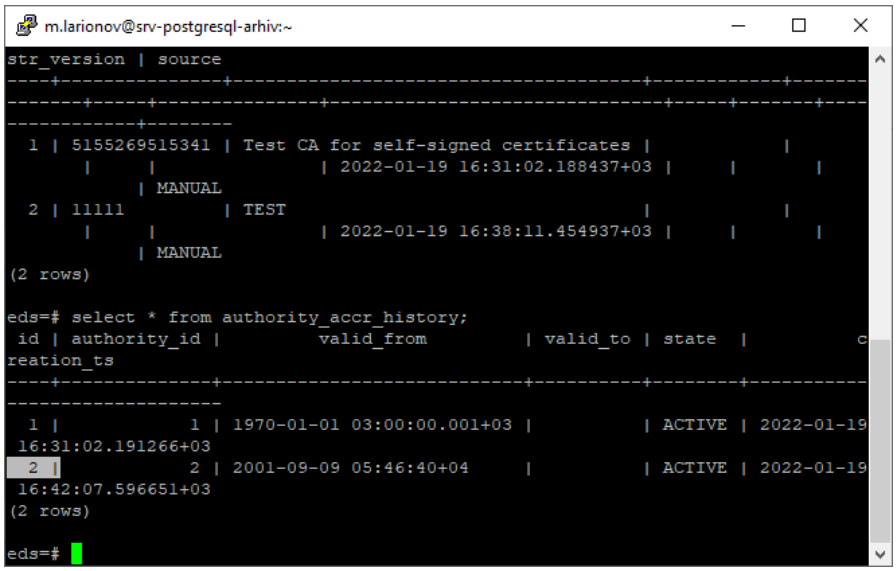

Рисунок 6 Определение «id» события

5.6. В «swagger» открыть «authority-test-controller», выбрать «Привязывает УЦ к публичному ключу», нажать «Try it out», заполнить следующие поля:

В поле «authId» добавить значение «2» (см. п.5.4.1.2.).

В поле «keyId» добавить значение «1» (см. п.5.2.3.3.).

Нажать «Execute».

5.6.1.Выполнить скрипт на сервере БД, для этого:

5.6.1.1.Подключиться к БД, выполнив команды:

sudo -u postgres psql postgres

\c eds;

5.6.1.2.В таблице «config_param», в поле «value» добавить значение «false», выполнив скрипт:

update config_param set value=false;

5.7.В «swagger» открыть «signature-generator-auth-by-cert-controller», выбрать «Создание pkcs7 подписи документа», нажать «Try it out», заполнить следующие поля:

В поле «cert» нажать «Выберите файл», выбрать сертификат «das.cer» (см. п. 3.2.).

В поле «data» нажать «Выберите файл», выбрать любой файл с рабочей машины для проверки подписи.

Нажать «Execute».

Нажать «Download file», скачать файл с подписью на рабочую машину.

5.8. В «swagger» открыть «verification-controller», выбрать «Проверка XAdES подписи», нажать «Try it out», заполнить следующие поля:

В поле «certificate» выбрать сертификат «das.cer» (см. п. 3.2.).

В поле «data» выбрать файл, который был использован для проверки подписи (см. п.5.7.).

В поле «sign» выбрать файл с подписью, который ранее скачен (см. п.5.7.).

В поле «type» выбрать значение «cms».

Нажать «Execute».

Для остальных систем настройка делается аналогично.