

# Кросс-отраслевая платформа "Semantic"

## Руководство по установке

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления.

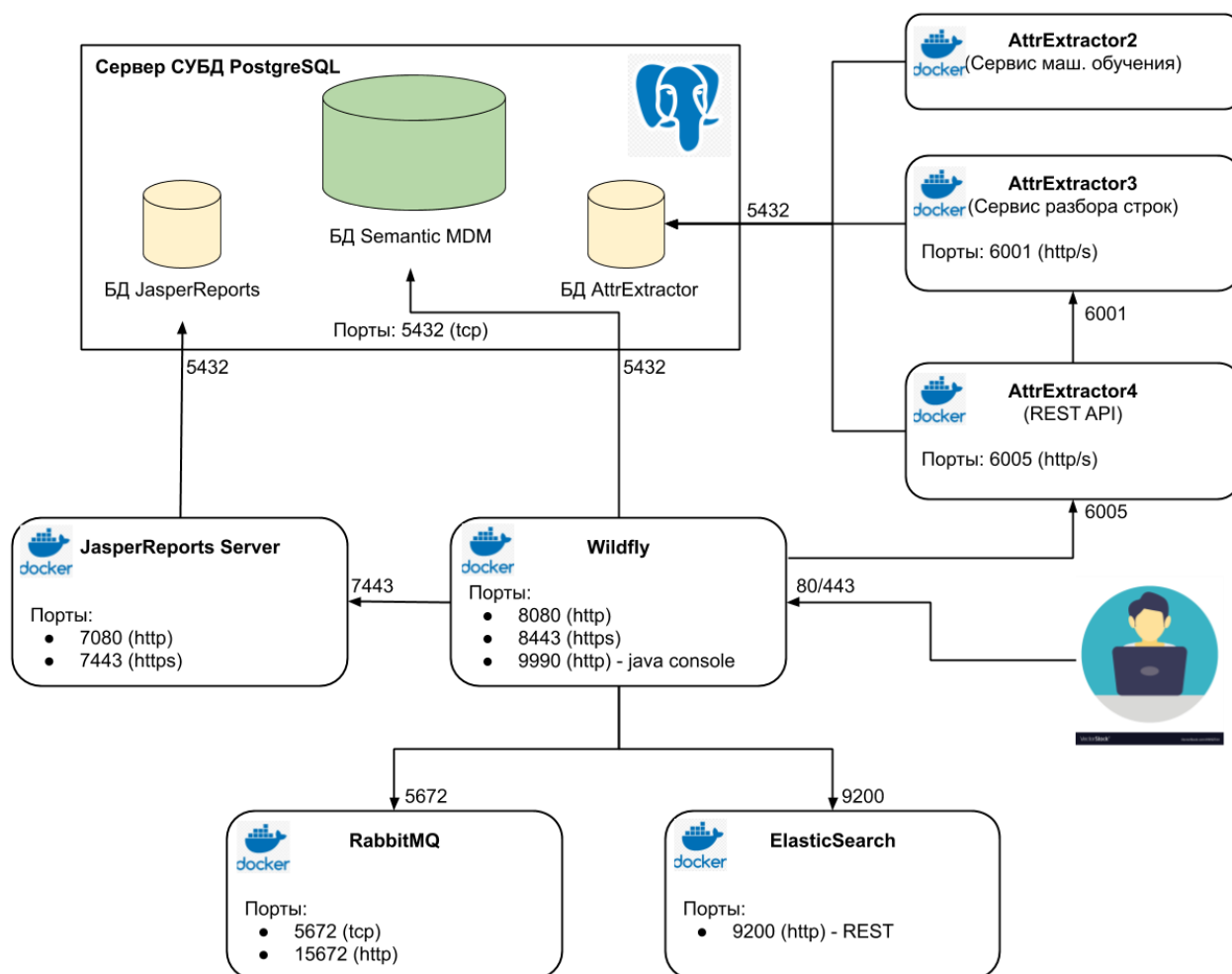
Никакая часть данного документа не может быть воспроизведена или передана в любой форме и любыми способами в каких-либо целях без письменного разрешения АО «ЭСДИАЙ СОЛЮШЕН».

© SDI Solution, 2023. Все права защищены.

## Содержание

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Схема взаимодействия Docker-контейнеров .....                                  | 3  |
| Установка сервера БД PostgreSQL и развёртывание базы данных Semantic MDM ..... | 4  |
| Установка сервера БД PostgreSQL версии 13 .....                                | 4  |
| Развёртывание базы данных Semantic MDM .....                                   | 4  |
| Подготовка к запуску Docker-контейнеров .....                                  | 6  |
| Настройка и запуск Docker-контейнеров .....                                    | 7  |
| RabbitMQ .....                                                                 | 7  |
| Настройка .....                                                                | 7  |
| Запуск .....                                                                   | 7  |
| Opensearch .....                                                               | 8  |
| Настройка .....                                                                | 8  |
| Смена пароля для пользователя «admin» .....                                    | 8  |
| Запуск .....                                                                   | 8  |
| WildFly .....                                                                  | 9  |
| Настройка .....                                                                | 9  |
| Настройка хранения файлов в БД или в MinIO .....                               | 10 |
| Настройка количества потоков .....                                             | 10 |
| Запуск .....                                                                   | 11 |
| Настройка интеграции .....                                                     | 11 |
| Настройка авторизации через Active Directory .....                             | 12 |
| Структура каталогов wildfly .....                                              | 14 |
| JasperServer .....                                                             | 16 |
| Настройка .....                                                                | 16 |
| Запуск .....                                                                   | 16 |
| Настройка после запуска .....                                                  | 16 |
| Структура каталогов jasperserver .....                                         | 19 |
| AttrExtractor .....                                                            | 20 |
| Настройка .....                                                                | 20 |
| Дополнительная настройка СУБД PostgreSQL .....                                 | 20 |
| Запуск .....                                                                   | 21 |
| MinIO .....                                                                    | 23 |
| Настройка .....                                                                | 23 |
| Запуск .....                                                                   | 23 |
| Приложение 1 .....                                                             | 24 |
| Создание самоподписанного SSL-сертификата (файлы cert.key cert.crt) .....      | 24 |
| Создание хранилища (файл cer.keystore) .....                                   | 24 |
| Создание хранилища Java (файл cacerts) .....                                   | 25 |
| Приложение 2 .....                                                             | 27 |
| Создание файла enable-ldap.cli .....                                           | 27 |
| Создание файла disable-ldap.cli .....                                          | 28 |

## Схема взаимодействия Docker-контейнеров



## Установка сервера БД PostgreSQL и развёртывание базы данных Semantic MDM

### Установка сервера БД PostgreSQL версии 13

1. Установить PostgreSQL версии 13 по инструкциям с официального сайта:  
<https://www.postgresql.org/download>  
<https://www.postgresql.org/docs/13/creating-cluster.html>
2. Установить административный пароль для пользователя (*postgres*) службы PostgreSQL, выполнив в терминале последовательно команды (в данном примере устанавливается пароль *masterkey*):  

```
sudo su - postgres  
psql -c "alter user postgres with password 'masterkey'"  
exit
```
3. Создать нового пользователя (*m2*) с паролем (в данном примере устанавливается пароль *masterkey*) и пустой базы данных (*m2*) для Semantic MDM, выполнив в терминале последовательно команды:  

```
sudo su - postgres  
psql -c "CREATE ROLE m2 WITH SUPERUSER LOGIN PASSWORD 'masterkey'"  
createdb m2 --owner m2  
exit
```
4. Выполнить «тонкую» настройку PostgreSQL, открыв на редактирование файл */var/lib/pgsql/13/data/postgresql.conf* и сделать изменения, предложенные на сайте:  
<https://www.pgconfig.org>
5. Выполнить «тонкую» настройку PostgreSQL, открыв на редактирование файл */var/lib/pgsql/13/data/pg\_hba.conf* и сделать следующие изменения:
  - 5.1. Строку №82 изменить с *host all all 127.0.0.1/32 ident* на *host all all 127.0.0.1/32 trust*
  - 5.2. В конец файла добавить строку *host all all 0.0.0.0/0 md5*
  - 5.3. Сохранить изменения в файл
6. Перезапустить службу PostgreSQL, выполнив в терминале команду:  

```
sudo systemctl restart postgresql-13
```
7. Настроить Firewall для удалённого доступа к PostgreSQL, выполнив в терминале последовательно команды:  

```
sudo firewall-cmd --add-service=postgresql --permanent  
sudo firewall-cmd --reload
```

### Развёртывание базы данных Semantic MDM

1. Загрузить файл *empty\_db.23.2.backup* с внешнего носителя на сервер во временный каталог */tmp/*
2. Запустить терминал и перейти во временный каталог */tmp/*, выполнив в терминале команду:  

```
cd /tmp/
```

3. Восстановить базу данных из резервной копии, выполнив в терминале команду:  
`pg_restore --host 127.0.0.1 --port 5432 --username "postgres" --no-password --dbname "m2" --role "m2" --verbose "/tmp/empty_db.23.2.backup "`

## Подготовка к запуску Docker-контейнеров

1. На сервере установить движок Docker по инструкции: <https://docs.docker.com/engine/install/>
2. В СУБД PostgreSQL создать 3 базы данных для Semantic MDM (имя БД не важно) и AttrExtractor (имя БД не важно) и JasperServer (имя БД: jasperserver).
3. Восстановить базу данных Semantic MDM из резервной копии. Файл «empty.backup».
4. Восстановить базу данных JasperServer из резервной копии. Файл «jasperserver.backup».
5. Создать каталог /opt/dockers и скопировать в него файл архива «dockers.tar.gz».
6. Перейти в каталог /opt/dockers, выполнив команду:  
`cd /opt/dockers`



*Все команды из этой инструкции выполняются в рамках данного каталога, если не оговорено дополнительно.*

7. Скопировать дистрибутивные файлы в каталог /opt/dockers.
8. Загрузить локальные Docker-образы, выполнив последовательно команды:  
`sh /opt/dockers/load-rabbitmq.sh`  
`sh /opt/dockers/load-opensearch.sh`  
`sh /opt/dockers/load-wildfly.sh`  
`sh /opt/dockers/load-jasperserver.sh`  
`sh /opt/dockers/load-attrextractor.sh`  
`sh /opt/dockers/load-minio.sh`

## Настройка и запуск Docker-контейнеров

### RabbitMQ

#### Настройка

1. Настройка не требуется.

#### Запуск

1. Запустить файл `/opt/dockers/run-rabbitmq.sh`, выполнив команду:  
`sh /opt/dockers/run-rabbitmq.sh`

## Opensearch

### Настройка

Скорректировать файл /opt/dockers/run-opensearch.sh:

1. В строке №7 скорректировать значения потребления памяти «-Xms2g -Xmx2g» где:  
Xms - минимальный объём, выделяемый на старте  
Xmx - максимальный объём

### Смена пароля для пользователя «admin»

1. Запустить файл /opt/dockers/run-opensearch.sh, выполнив команду:  
`sh /opt/dockers/run-opensearch.sh`
2. Получить hash пароля, выполнив команду и запомнив её вывод:  
`docker exec -it opensearch /usr/share/opensearch/plugins/opensearch-security/tools/hash.sh -p passwd`  
где `passwd` – это пароль
3. Запустить файл /opt/dockers/del-opensearch.sh, выполнив команду:  
`sh /opt/dockers/del-opensearch.sh`
4. Скорректировать файл /opt/dockers/opensearch/securityconfig/internal\_users.yml, заменив в строке №14 « \$2y\$12\$77bkIOJBVqn7K/0SHomEi.r34iDKXplzzC22RX9.AFcXn/Dm3WI5W » выводом команды из пункта №2

### Запуск

5. Запустить файл /opt/dockers/run-opensearch.sh, выполнив команду:  
`sh /opt/dockers/run-opensearch.sh`

## WildFly

### Настройка

1. Скорректировать файл /opt/dockers/wildfly/dist/cli-commands/db1.cli:
  - 1.1. В строках №№11 и 14 скорректировать протокол http или https по которому будет доступен Docker с WildFly.
  - 1.2. В строках №№11 и 14 вместо «Доменное\_Имя\_Сервера» прописать корректное доменное имя сервера, где будет запущен Docker с WildFly.
  - 1.3. В строках №№11 и 14 вместо «Порт» прописать порт, на который будет настроен Docker с WildFly. По-умолчанию порт для протокола http=8080, а для протокола https=8443
  - 1.4. В строке №17 вместо «IP\_адрес\_PostgreSQL» прописать корректный IP адрес сервера PostgreSQL.
  - 1.5. В строке №17 вместо «Имя\_БазыДанных\_PostgreSQL» прописать корректное имя базы данных PostgreSQL для Semantic MDM.
  - 1.6. В строке №17 вместо «схема» прописать корректное имя схемы в базе данных PostgreSQL для Semantic MDM.
  - 1.7. В строке №20 вместо «Имя\_Пользователя\_PostgreSQL» прописать корректное имя пользователя PostgreSQL с правами администратора.
  - 1.8. В строке №21 вместо «Пароль\_Пользователя\_PostgreSQL» прописать корректный пароль пользователя из пункта 3.
  - 1.9. В строке №23 вместо «IP\_адрес\_сервера\_где\_запущен\_Docker\_Opensearch» прописать корректный IP адрес сервера, где запущен Docker с Opensearch.
  - 1.10. В строке №26 вместо «Пароль\_пользователя\_Opensearch» прописать корректный пароль пользователя «admin» Opensearch. Пароль по-умолчанию: passw0rd
  - 1.11. В строках №№11, 14, 58, 64 вместо «Доменное\_Имя\_Сервера» прописать корректное доменное имя сервера, где будет запущен Docker с WildFly.
  - 1.12. В строках №№69-75 прописать корректные данные почтового ящика, от которого будет вестись рассылка сообщений.
2. Сгенерировать jwt.keystore и поместить его в каталог /opt/dockers/wildfly/dist/configuration/, выполнив команду в терминале:  
keytool -genkey -alias alias -keyalg RSA -keysize 2048 -keystore  
/opt/dockers/wildfly/dist/configuration/jwt.keystore -storepass secret -keypass secret
3. Для запуска с использованием протокола https необходимо сделать следующее:
  - 3.1. разместите файлы cert.keystore и cacerts в каталог (см. приложение 1)  
/opt/dockers/wildfly/dist/configuration/.
  - 3.2. В файле /opt/dockers/wildfly/dist/cli-commands/db1.cli раскомментировать (удалить символ # в начале строки) №№53-61.
  - 3.3. В файле /opt/dockers/wildfly/dist/cli-commands/db1.cli в строке №54 заменить «Пароль\_к\_keystore» на пароль к файлу cert.keystore (см. приложение 1).
  - 3.4. В файле /opt/dockers/wildfly/dist/cli-commands/db1.cli в строке №56 заменить «Пароль\_к\_Сертификату» на пароль к сертификату (см. приложение 1).

4. Скорректировать файл /opt/docker/run-wildfly-http.sh или run-wildfly-https.sh:  
В строке №15 скорректировать значения потребления памяти «-Xms3G -Xmx3G -XX:MetaspaceSize=96M -XX:MaxMetaspaceSize=2G» где:  
Xms - минимальный объём, выделяемый на старте  
Xmx - максимальный объём  
XX:MetaspaceSize - объём памяти, выделяемой под классы на старте  
XX:MaxMetaspaceSize – максимальный объём памяти, выделяемой под классы

### Настройка хранения файлов в БД или в MinIO

1. Для хранения файлов в БД дополнительных настроек не требуется
2. Для хранения файлов в MinIO необходимо скорректировать файл /opt/docker/wildfly/dist/cli-commands/db1.cli:
  - 2.1. Закомментировать строку №31, добавив в начало строки символ #
  - 2.2. Раскомментировать строки №33-36, удалив в начале строки символ #
  - 2.3. В строке №34 вместо «Адрес\_сервера\_minio\_1» и «Адрес\_сервера\_minio\_1» указать адреса 1 и 2 ноды MinIO соответственно. Если используется только одна нода, то удалить «,http://Адрес\_сервера\_minio\_2:9000».
  - 2.4. В строке №35 вместо «Имя\_Пользователя\_minio» прописать имя пользователя MinIO. Имя пользователя по-умолчанию: minioroot
  - 2.5. В строке №36 вместо «Пароль\_Пользователя\_minio» прописать пароль пользователя MinIO. Пароль по-умолчанию: passw0rd

### Настройка количества потоков

Берём минимальное количество ядер из сервера приложений и сервера БД. Это будет **XXX**  
Скорректировать файл /opt/docker/wildfly/dist/cli-commands/db1.cli:

1. В строке №45 указать максимальное количество потоков параллельной обработки мелкого задания, являющегося частью одного большого:  
`/system-property=ru.sdi.m2.short.thread.max:add(value=XX)`  
Где **XX** = **XXX**
2. В строке №80 указать количество одновременно выполняемых долгих задач, например, экспорт-импорт xml или excel:  
`/subsystem=ee/managed-executor-service=background-long:add(jndi-name="java:boss/ee/concurrency/executor/background-long", context-service="default", thread-factory="low-priority", hung-task-threshold="0", long-running-tasks="true", core-threads="XX", max-threads="XX", keepalive-time="60000", reject-policy="RETRY_ABORT")`  
Где **XX** = **XXX/4**
3. В строке №82 указать количество одновременно выполняемых коротких задач, например, публикация пакета изменений:

```
/subsystem=ee/managed-executor-service=background-short:add(jndi-name="java:jboss/ee/concurrency/executor/background-short", context-service="default", thread-factory="low-priority", hung-task-threshold="0", long-running-tasks="true", core-threads="XX", max-threads="XX", keepalive-time="60000", reject-policy="RETRY_ABORT")
```

Где **XX** = **XXX**/2

4. В строке №83 указать количество потоков пост-обработки изменений сделанных прямыми запросами

```
managed-executor-service=modification-processors:add(jndi-name="java:jboss/ee/concurrency/executor/modification-processors", context-service="default", thread-factory="medium-priority", hung-task-threshold="0", long-running-tasks="false", core-threads="XX", max-threads="XX", keepalive-time="60000", reject-policy="RETRY_ABORT")
```

Где **XX** = **XXX**\*8

5. В строке №84 указать степень параллелизма прямых запросов:

```
/subsystem=ejb3/thread-pool=default:write-attribute(name=max-threads, value= XX)
```

Где **XX** = **XXX**\*8

## Запуск

1. Для запуска с использованием протокола http, запустить файл /opt/dockers/run-wildfly-http.sh, выполнив команду:

```
sh /opt/dockers/run-wildfly-http.sh
```

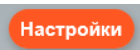
2. Для запуска с использованием протокола https, запустить файл /opt/dockers/run-wildfly-https.sh, выполнив команду:

```
sh /opt/dockers/run-wildfly-https.sh
```

## Настройка интеграции

1. Войти в раздел настроек, нажав на главной странице Semantic MDM кнопку «Навигация» 

и выбрать пункт «Настройки»



2. Нажать ссылку «Интеграция»



3. В разделе «Сервис разбора строк» в поле «Адрес сервиса» указать адрес сервиса разбора строк, вида: `https://IP_адрес_сервиса:Порт_Сервиса`

4. В разделе «RabbitMQ» указать:

4.1. В поле «Адрес (без указания порта)» указать адрес RabbitMQ, вида:

`https://IP_адрес_RabbitMQ`

4.2. В поле «Логин» указать: `m2`

4.3. В поле «Пароль» указать: `m2`

- 4.4. Нажать кнопку «Перезапустить Rabbit MQ»
5. В разделе «Сервер отчетов JasperReports» указать:
  - 5.1. В поле «Адрес сервера» указать адрес JasperReports, вида:  
`https://IP_адрес_сервера_JasperReports:Порт_Сервера`
  - 5.2. В поле «Логин» указать: `mdm-sla`
  - 5.3. В поле «Пароль» указать: `111`

SEMANTIC MDM™ Настройки

Основные  
Интеграция  
Отладка  
Расширения

Сервис разбора строк

Адрес сервиса

Сервис разбора строк - Генерация позиций номенклатуры

Справочники номенклатуры

Rabbit MQ

Адрес (без указания порта)

Логин

Пароль

Перезапустить Rabbit MQ

Сервер отчетов JasperReports

Адрес сервера

Логин

Пароль

### Настройка авторизации через Active Directory

1. Включить в домен хост с сервером приложений Semantic MDM.
2. Обеспечить доступ к контроллеру домена по имени с хоста с сервером приложений Semantic MDM.
3. На контроллере домена выполнить команду:  
`setspn -A HTTP/<имя домена СП> <имя участника-службы>`  
где:  
<доменное имя СП> – доменное имя хоста с сервером приложений Semantic MDM, например, `app.sdi.ru`;  
<имя участника-службы> – имя пользователя домена, по которому клиент однозначно определяет экземпляр службы.
4. На контроллере домена выполнить команду:  
`ktpass -princ HTTP/<имя домена СП>@<имя домена> -mapuser <имя участника-службы> -pass <пароль участника-службы> -ptype KRB5_NT_PRINCIPAL -out <путь к файлу *.keytab>`  
где:  
<имя домена> – имя домена, например, `sdi.ru`;

<доменное имя СП> – доменное имя хоста с сервером приложений Semantic MDM, например, app.sdi.ru;

<имя участника-службы> – имя пользователя домена, по которому клиент однозначно определяет экземпляр службы;

<пароль участника-службы> – пароль;

<путь к файлу \*.keytab> – полный путь к файлу с расширением \*.keytab, который будет сформирован.

4.1. Если используется несколько доменов, то на других контроллерах домена, при выполнении команды *ktpass* нужно добавить флаг «-in <путь к файлу \*.keytab с другого домена>», что бы в одном файле \*.keytab были данные со всех доменов. Например:

```
ktpass -princ HTTP/<имя домена СП>@<имя домена> -taruser <имя участника-службы> -pass <пароль участника-службы> -ptype KRB5_NT_PRINCIPAL -in <путь к файлу *.keytab с другого домена> -out <путь к файлу *.keytab>
```

5. Сформированный на контроллере домена файл с расширением \*.keytab скопировать в каталог /opt/dockers/wildfly/dist/configuration

6. Включение авторизации через Active Directory.

6.1. Удалить файлы disable-ldap.cli и disable-ldap.cli.started в каталоге /opt/dockers/wildfly/dist/cli-commands/, если они там присутствуют.

6.2. Скопировать файл enable-ldap.cli (см. Приложение 2) в каталог /opt/dockers/wildfly/dist/cli-commands/.

6.3. Запустить docker-контейнер WildFly, выполнив в терминале команду:

```
docker restart wildfly
```

7. Отключение авторизации через Active Directory.

7.1. Удалить файлы enable-ldap.cli и enable-ldap.cli.started в каталоге /opt/dockers/wildfly/dist/cli-commands/, если они там присутствуют..

7.2. Скопировать файл disable-ldap.cli (см. Приложение 2) в каталог /opt/dockers/wildfly/dist/cli-commands/.

7.3. Запустить docker-контейнер WildFly, выполнив в терминале команду:

```
docker restart wildfly
```

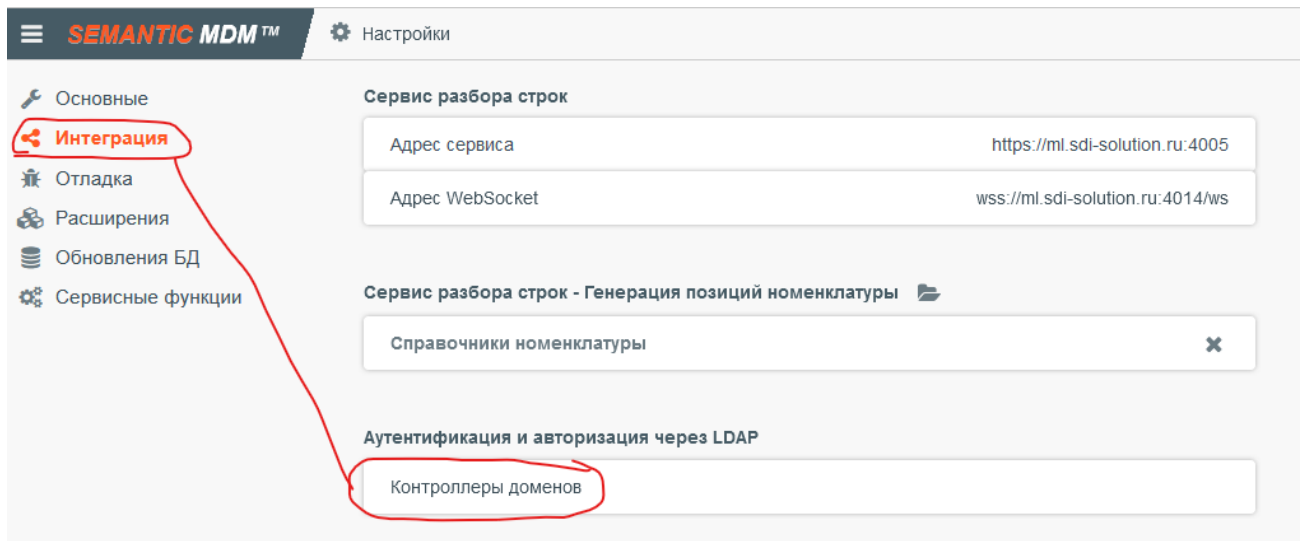
8. Войти в Semantic MDM от имени пользователя с правами администратора.

9. Войти в раздел настроек, нажав на главной странице Semantic MDM кнопку «Навигация» 

и выбрать пункт «Настройки»



10. В разделе «Интерация» нажать на «Контроллеры домена».



11. Заполнить столбцы «Адрес контроллера домена», «Путь поиска пользователей» и «Домен». Если необходимо несколько строк, то их можно создать нажатием кнопки «Создать».

| Контроллеры доменов                      |                                          |                        | Создать | Удалить | × |
|------------------------------------------|------------------------------------------|------------------------|---------|---------|---|
| Адрес контроллера домена                 | Путь поиска пользователей                | Домен                  |         |         |   |
| ldap://dc1.sdi-solution.local:389        | CN=Users,DC=sdi-solution,DC=local        | sdi-solution.local     |         |         |   |
| ldap://dc1sub.sub.sdi-solution.local:391 | CN=Users,DC=sub,DC=sdi-solution,DC=local | sub.sdi-solution.local |         |         |   |
| ldap://dc2.sdi-solution2.local:390       | CN=Users,DC=sdi-solution2,DC=local       | sdi-solution2.local    |         |         |   |

## Структура каталогов wildfly

/opt/dockers/wildfly/dist/ - Каталог с файлами для настройки Wildfly в контейнере при его создании. Примонтирован через volumes внутри контейнера по пути /tmp/dist/

/opt/dockers/wildfly/dist/postgresql-42.2.8.jar - Модуль для соединения с БД.

/opt/dockers/wildfly/dist/start.sh - Основной исполняемый файл, который запускается внутри контейнера при старте, настраивает и запускает основной процесс. Так называемый ENTRYPOINT.

/opt/dockers/wildfly/dist/cli-commands/ - Каталог с файлами, содержащими CLI-команды, выполняемыми в контейнере при его создании.

/opt/dockers/wildfly/dist/cli-commands/db1.cli - CLI-команды для настройки соединения с БД и другими настраиваемыми параметрами индивидуальными для разных контейнеров.

/opt/dockers/wildfly/dist/cli-commands/main.cli - CLI-команды для настройки других параметров.

`/opt/dockers/wildfly/dist/client-software/` - Каталог с файлами для клиентов (лицензия, документация, описание API и др.)

`/opt/dockers/wildfly/dist/configuration/` - Каталог с файлами конфигурации, которые копируются в `/opt/jboss/wildfly/standalone/configuration` при создании контейнера.

`/opt/dockers/wildfly/dist/deployment/` - Каталог со сборками, которые деплоятся при создании контейнера.

`/opt/dockers/wildfly/dist/modules/` - Каталог с файлами модулей, которые копируются в `/opt/jboss/wildfly/modules` при создании контейнера.

`/opt/dockers/wildfly/standalone/` - Каталог с файлами, создаваемыми Wildfly при работе в контейнере. Примонтирован через volumes внутри контейнера по пути `opt/jboss/wildfly/standalone2`

## JasperServer

### Настройка

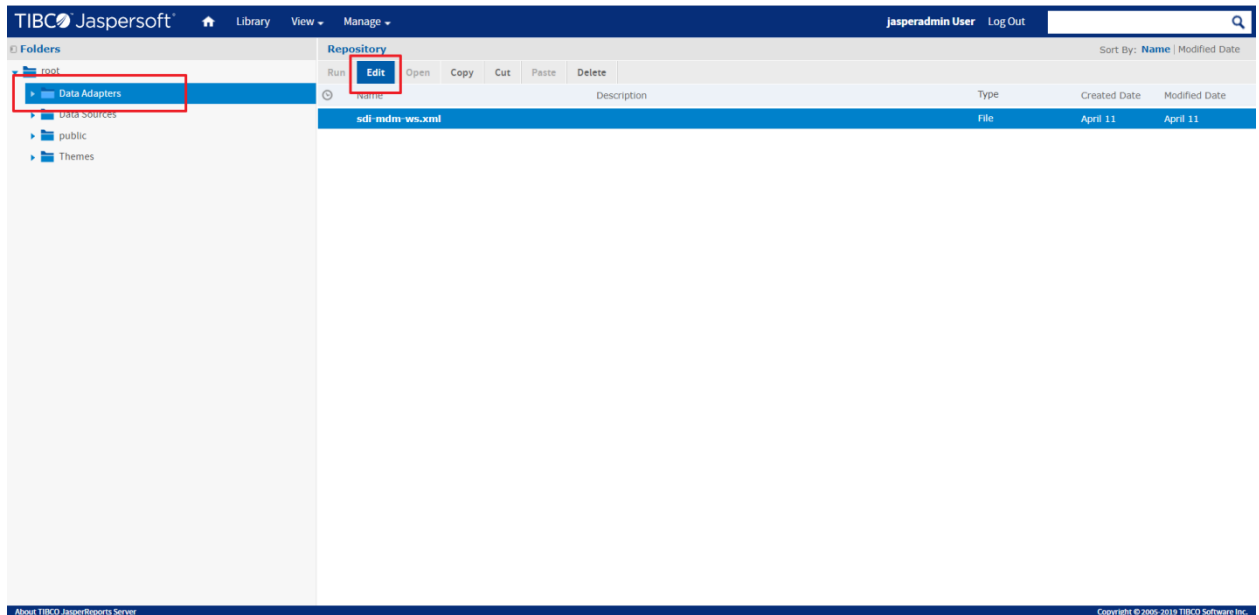
1. Скорректировать файл /opt/dockers/run-jasperserver.sh:
  - 1.1. В строке №5 вместо «IP\_адрес\_PostgreSQL» прописать корректный IP адрес сервера, где установлен PostgreSQL.
  - 1.2. В строке №7 вместо «Имя\_Пользователя\_PostgreSQL» прописать корректное имя пользователя PostgreSQL с правами администратора.
  - 1.3. В строке №8 вместо «Пароль\_Пользователя\_PostgreSQL» прописать корректный пароль пользователя из пункта 3.
  - 1.4. Сохранить изменения в файл.
2. Скорректировать файл /opt/dockers/jasperserver/dist/web.xml:
  - 2.1. В строке №285 вместо «IP\_Адрес\_Semantic\_MDM» прописать корректный IP адрес сервера, где установлен Semantic MDM.
  - 2.2. В строке №285 вместо «Доменное\_Имя\_Semantic\_MDM» прописать корректное доменное имя сервера, где установлен Semantic MDM и по которому доступен Web-клиент Semantic MDM.
3. Скорректировать файл /opt/dockers/jasperserver/dist/sdi-mdm-ws.xml:
  - 3.1. В строке №4 вместо «Доменное\_Имя\_Semantic\_MDM» прописать корректное доменное имя сервера, где установлен Semantic MDM. Также скорректировать протокол http или https, по которому доступен Web-клиент Semantic MDM.
  - 3.2. В строке №4 вместо «Порт» прописать порт, на который будет настроен Docker с WildFly. По-умолчанию порт для протокола http=8080, а для протокола https=8443
4. Для запуска с использованием протокола https, разместите файлы cert.keystore и cert.cer (см. приложение 1) в каталог /opt/dockers/jasperserver/dist/. Если данные файлы отсутствуют, то будет использоваться протокол http.
5. Для запуска с использованием протокола https, скорректировать файл /opt/dockers/jasperserver/dist/serverssl.xml:
  - 5.1. в строке №63 заменить «Пароль\_к\_keystore» на пароль к файлу cert.keystore (см. приложение 1).

### Запуск

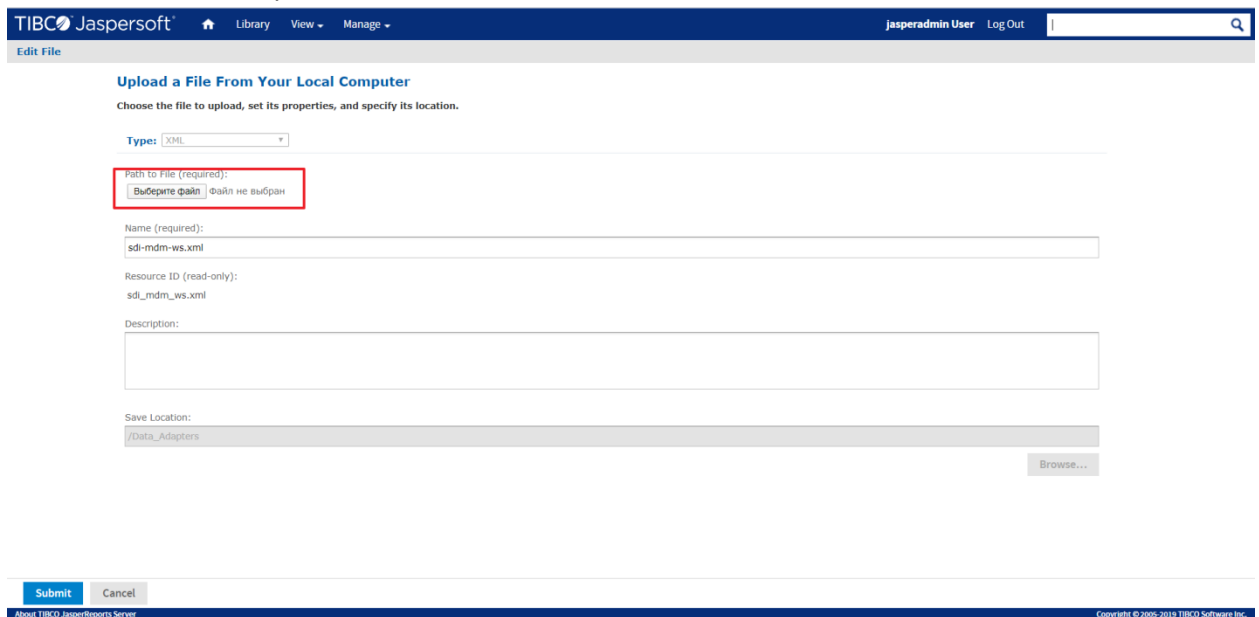
1. Запустить файл /opt/dockers/run-jasperserver.sh, выполнив команду:  
`sh /opt/dockers/run-jasperserver.sh`

### Настройка после запуска

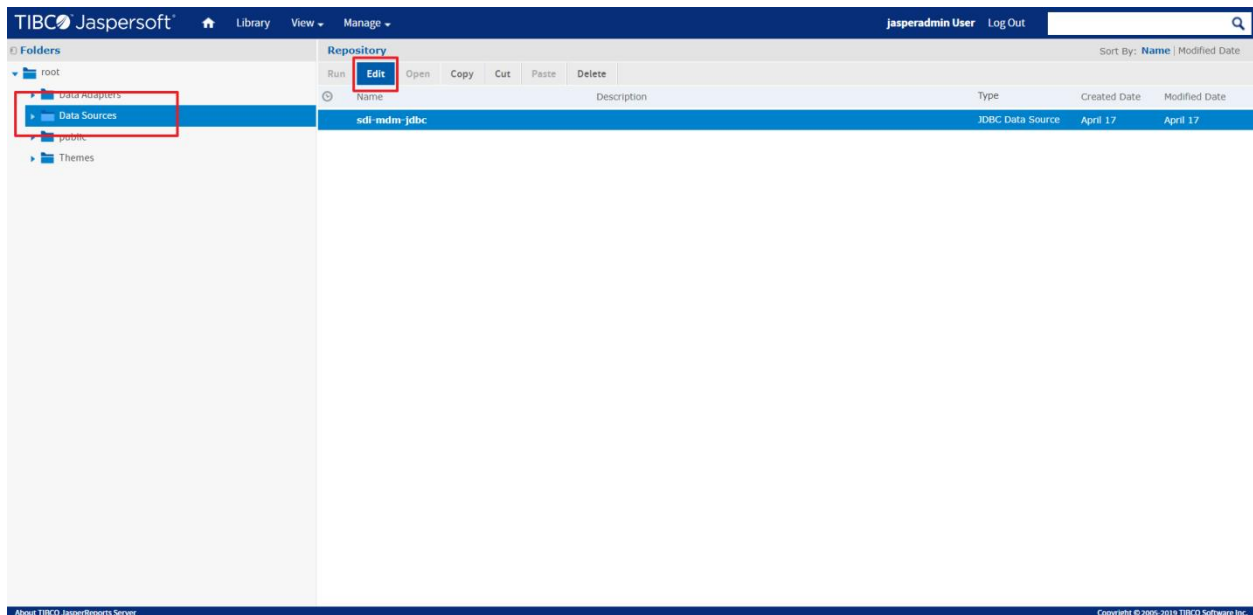
1. Открыть в браузере страницу JasperServer по адресу `http://Доменное_Имя_JasperServer:7080` или `https://Доменное_Имя_JasperServer:7443` в зависимости от протокола http или https.
2. Ввести логин `jasperadmin` и пароль `jasperadmin`
3. В дереве встать на узел «Data Adapters» и нажать кнопку «Edit»



4. Нажать кнопку «Выберите файл» и указать файл /opt/dockers/jasperserver/dist/sdi-mdm-ws.xml
5. Нажать кнопку «Submit»

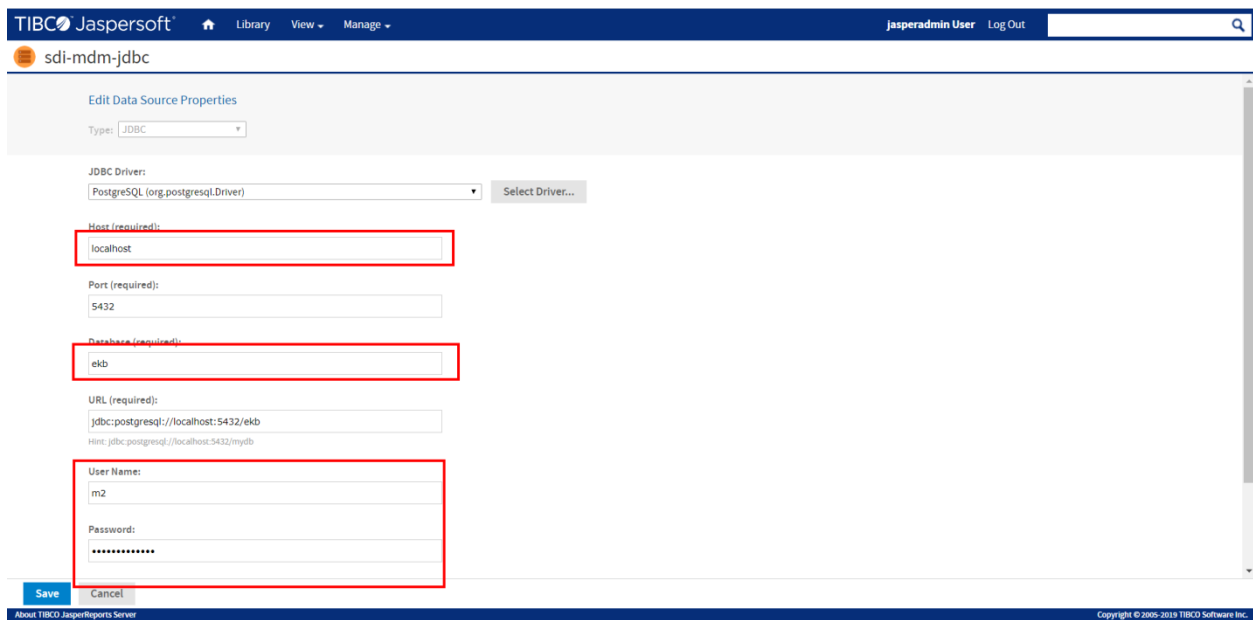


6. В дереве встать на узел «Data Sources» и нажать кнопку «Edit»



7. В поле «Host (required)» ввести IP-адрес сервера PostgreSQL с БД Semantic MDM.
8. В поле «Database (required)» ввести имя БД Semantic MDM.
9. В поле «User Name» ввести имя пользователя с правами Администратора на сервере PostgreSQL.
10. В поле «Password» ввести пароль пользователя с правами Администратора на сервере PostgreSQL.
11. Нажать кнопку «Save».

Эти настройки идентичны настройкам WildFly (см. соответствующий раздел).



### Структура каталогов jasperserver

/opt/docker/JasperServer/dist/ - Каталог с файлами для настройки JasperServer в контейнере при его создании. Примонтирован через volumes внутри контейнера по пути /tmp/dist/

## AttrExtractor

### Настройка

Скорректировать файл /opt/dockers/attrextractor/workdir/config.ini:

1. В строке №2 вместо «IP\_адрес\_PostgreSQL» прописать корректный IP адрес сервера, где установлен PostgreSQL.
2. В строке №2 вместо «Имя\_БазыДанных\_PostgreSQL» прописать корректное имя базы данных PostgreSQL для AttrExtractor.
3. В строке №2 вместо «Имя\_Пользователя\_PostgreSQL» прописать корректное имя пользователя PostgreSQL с правами администратора.
4. В строке №2 вместо «Пароль\_Пользователя\_PostgreSQL» прописать корректный пароль пользователя из пункта 3.
5. В строке №3 вместо «public» прописать корректное имя схемы пользователя если она отличается от «public».
6. В строке №5 вместо «IP\_адрес\_OpenSearch» прописать корректный IP адрес сервера, где установлен OpenSearch.
7. Скопировать файл /opt/dockers/wildfly/dist/configuration/jwt.keystore с сервера где установлен Wildfly в любой каталог, в терминале перейти в этот каталог и выполнить команды (при запросе паролей, вводить: secret):  

```
keytool -importkeystore -srckeystore jwt.keystore -destkeystore certml.p12 -srcalias alias -srcstoretype jks -deststoretype pkcs12
```

```
openssl pkcs12 -in certml.p12 -out certml.pem
```

```
openssl rsa -in certml.pem -pubout -out /opt/dockers/attrextractor/workdir/m2ml.pem
```
8. Для запуска с использованием протокола https, разместить файлы cert.key и cert.crt (см. приложение 1) в каталог /opt/dockers/attrextractor/workdir/ и раскомментировать строки 34-35 и 40-45 (удалив символ # в начале строки) и закомментировать строки 36-37 (добавив символ # в начале строки) в файле /opt/dockers/attrextractor/workdir/nginx.conf.
9. В firewall открыть доступ к портам, на которых будет запущен сервис разбора строк (по-умолчанию 6001, 6004, 6005, 6014 и 6015).

### Дополнительная настройка СУБД PostgreSQL

1. Установить расширение для генерации UUID, для этого выполнить в терминале команды, где <db\_name> - имя БД AttrExtractor:  

```
sudo su - postgres psql
```

```
\c <db_name>;
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-oss";
```

2. Если сервер базы данных находится на той же машине, что контейнеры с остальными частями системы, то добавить в настроечный файл `/var/lib/pgsql/13/data/pg_hba.conf` строку:

```
host      all             all             172.17.0.0/16      password
```

- 2.1. Если сервер базы данных находится отдельно от контейнеров с остальными частями системы, то добавить в настроечный файл `/var/lib/pgsql/13/data/pg_hba.conf` строку, где `<IP_адрес>` - IP-адрес сервера с остальными частями системы:

```
host      all             all             <IP_адрес>/16      password
```

- 2.2. Перезапустить службу PostgreSQL, выполнив в терминале команду:  
`sudo systemctl restart postgresql-13`

## Запуск

1. Запустить файл `/opt/dockers/load-attrextractor.sh`, выполнив команду:  
`sh /opt/dockers/load-attrextractor.sh`
2. Запустить файл `/opt/dockers/run-attrextractor1.sh`, выполнив команду:  
`sh /opt/dockers/run-attrextractor1-docker.sh`  
Этот файл нужно запустить 1 раз для создания БД и её инициализации.

3. Активировать окружение и импортировать extractor в БД:

- 3.1. Выполнить команды в терминале:

```
cd /opt/dockers/attrextractor
```

```
tar -xzf attr_extractor_env.tar.gz -C attr_extractor_env
```

```
source attr_extractor_env/bin/activate
```

```
m2-extractor.import -n gsap -s gsap.json -et GSAP -cs
```

```
postgresql+psycopg2://Имя_Пользователя_PostgreSQL:Пароль_Пользователя_PostgreSQL  
@IP_адрес_PostgreSQL:5432/Имя_БазыДанных_PostgreSQL -sn public
```

Где «IP\_адрес\_PostgreSQL» - IP адрес сервера, где установлен PostgreSQL  
«Имя\_БазыДанных\_PostgreSQL» - имя базы данных PostgreSQL для AttrExtractor  
«Имя\_Пользователя\_PostgreSQL» - имя пользователя PostgreSQL с правами администратора  
«Пароль\_Пользователя\_PostgreSQL» - пароль пользователя PostgreSQL  
«public» - имя схемы пользователя если она отличается от «public»

4. Запустить файл `/opt/dockers/run-attrextractor2-docker.sh`, выполнив команду:  
`sh /opt/dockers/run-attrextractor2.sh`

5. Запустить файл `/opt/dockers/run-attretractor3-docker.sh`, выполнив команду:  
`sh /opt/dockers/run-attretractor3.sh`
6. Запустить файл `/opt/dockers/run-attretractor4-docker.sh`, выполнив команду:  
`sh /opt/dockers/run-attretractor4.sh`
7. Запустить файл `/opt/dockers/run-attretractor5-docker.sh`, выполнив команду:  
`sh /opt/dockers/run-attretractor5.sh`
8. Запустить файл `/opt/dockers/run-attretractor6-docker.sh`, выполнив команду:  
`sh /opt/dockers/run-attretractor6-docker.sh`
9. Запустить файл `/opt/dockers/run-nginx.sh`, выполнив команду:  
`sh /opt/dockers/run-nginx.sh`

## MinIO

### Настройка

Скорректировать файл `/opt/dockers/attrextractor/workdir/config.ini`:

1. В строке №2 вместо «Имя\_Пользователя\_minio» прописать имя пользователя MinIO. Имя пользователя по-умолчанию: `minioroot`
2. В строке №2 вместо «Пароль\_Пользователя\_minio» прописать пароль для пользователя MinIO. Пароль по-умолчанию: `passw0rd`

### Запуск

1. Запустить файл `/opt/dockers/run-minio.sh`, выполнив команду:  
`sh /opt/dockers/run-minio.sh`

## Приложение 1

### Создание самоподписанного SSL-сертификата (файлы cert.key cert.crt)

При «заказе» сертификата можно установить срок, в течение которого он должен оставаться действующим (число 365 в запросе можно поменять на любое другое). Мы создадим сертификат, который будет действителен в течение одного года. Для этого выполнить команду:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout cert.key -out cert.crt
```

С помощью этой команды запускается создание самоподписанного SSL-сертификата, а также серверного ключа для его защиты. Оба этих файла будут храниться в текущей директории.

В процессе создания сертификата система будет задавать вопросы, на которые нужно будет ответить.

Самое важное поле “Common Name” — здесь нужно вбить доменное имя сайта, если у него еще нет домена (или его использование не предполагается), можно вбить IP-адрес.

Примерный вывод в консоли:

*You are about to be asked to enter information that will be incorporated into your certificate request.*

*What you are about to enter is what is called a Distinguished Name or a DN.*

*There are quite a few fields but you can leave some blank*

*For some fields there will be a default value,*

*If you enter '.', the field will be left blank.*

-----

**Country Name (2 letter code) [AU]:RU**

**State or Province Name (full name) [Some-State]:Moscow Region**

**Locality Name (eg, city) []:Moscow**

**Organization Name (eg, company) [Internet Widgits Pty Ltd]:OOO Romashka**

**Organizational Unit Name (eg, section) []:Sales**

**Common Name (e.g. server FQDN or YOUR name) []:example.com**

**Email Address []:webmaster@example.com**

### Создание хранилища (файл cer.keystore)

1. Перейти в каталог с файлами cert.crt и cert.key

2. Выполнить команду:

```
openssl pkcs12 -export -in cert.crt -inkey cert.key -out cert.p12 -name server
```

2.1. На запрос пароля необходимо ввести пароль и запомнить его.

2.2. На выходе получаем файл cert.p12

3. Выполнить команду:

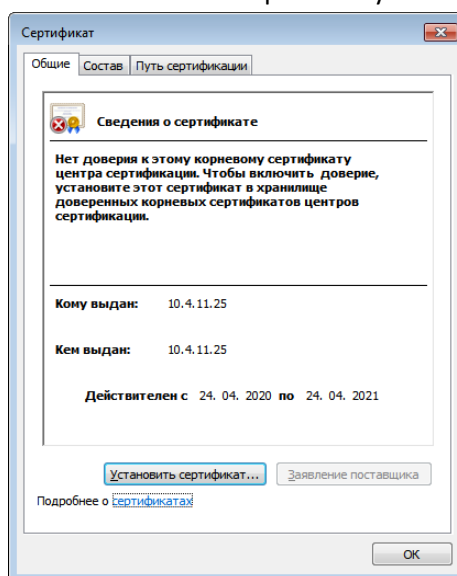
```
keytool -importkeystore -srckeystore cert.p12 -srcstoretype PKCS12 -destkeystore cert.keystore -deststoretype pkcs12
```

3.1. На запрос пароля необходимо ввести пароль и запомнить его.

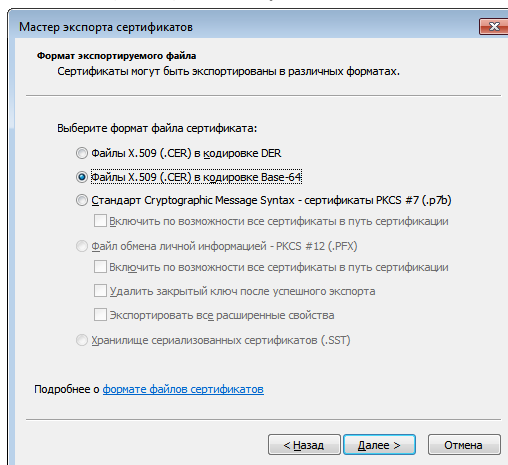
3.2. На выходе получаем файл cert.keystore

## Создание хранилища Java (файл cacerts)

1. Перейти в каталог с файлами cert.crt, cert.key и cert.keystore
2. На этом шаге для конвертации сертификата типа CRT в тип CER понадобится компьютер под управлением ОС Windows. Для конвертации сделать следующее:
  - 2.1. Скопировать файл cert.crt на компьютер под управлением ОС Windows.
  - 2.2. Дважды кликнуть на файле cert.crt. Файл откроется в утилите просмотра сертификатов.



- 2.3. Перейти на вкладку Состав и нажать кнопку Копировать в файл... Откроется мастер экспорта сертификатов.
- 2.4. Нажать кнопку Далее в мастере создания сертификатов.
- 2.5. Выбрать опцию «Файлы X.509 (.CER) в кодировке Base-64» и нажать кнопку Далее.



- 2.6. Указать каталог для сохранения сертификата и имя файла cert.cer и Нажать кнопку Далее

- 2.7. Нажать кнопку Готово
- 2.8. Скопировать файл cert.cer в каталог с файлами cert.crt, cert.key и cert.keystore в Linux
3. Выполнить команду:  

```
$JAVA_HOME/bin/keytool -import -alias mdmdev -file cert.cer -keystore cacerts
```

На запрос пароля необходимо ввести пароль и запомнить его.  
На запрос «Trust this certificate? [no]:» написать yes и нажать Enter
4. На выходе получаем файл cacert

## Приложение 2

### Создание файла enable-ldap.cli

1. Войти в раздел настроек, нажав на главной странице Semantic MDM кнопку «Навигация»  и выбрать пункт «Настройки» .
2. Включить переключатель «Авторизация через LDAP»



3. В появившемся окне «Генератор cli-файла для настройки LDAP» заполнить все поля и нажать кнопку «Сгенерировать».

Генератор cli-файла для настройки LDAP
Сгенерировать
X

|                                |                        |
|--------------------------------|------------------------|
| Домен                          | sdi-solution.local     |
| Адрес контроллера домена ?     | dc1.sdi-solution.local |
| Адрес Semantic MDM ?           | mdm.sdi-solution.local |
| Имя пользователя ?             | user1                  |
| Пароль                         | Password1              |
| Имя пользователя SPN           | user2                  |
| Пароль SPN                     | Password2              |
| RegExp удаления домена ?       | @[a-zA-Z0-9-]*         |
| RegExp удаления пользователя ? | [a-zA-Z0-9-]*@         |

**Внимание!**

Для включения/отключения авторизации LDAP на сервере приложений требуется выполнить соответствующий cli-файл (enable-ldap.cli/disable-ldap.cli) на хосте, где установлен сервер приложений Semantic MDM, после чего он будет автоматически перезапущен [подробнее](#)

4. Сохранить файл enable-ldap.cli на диск.

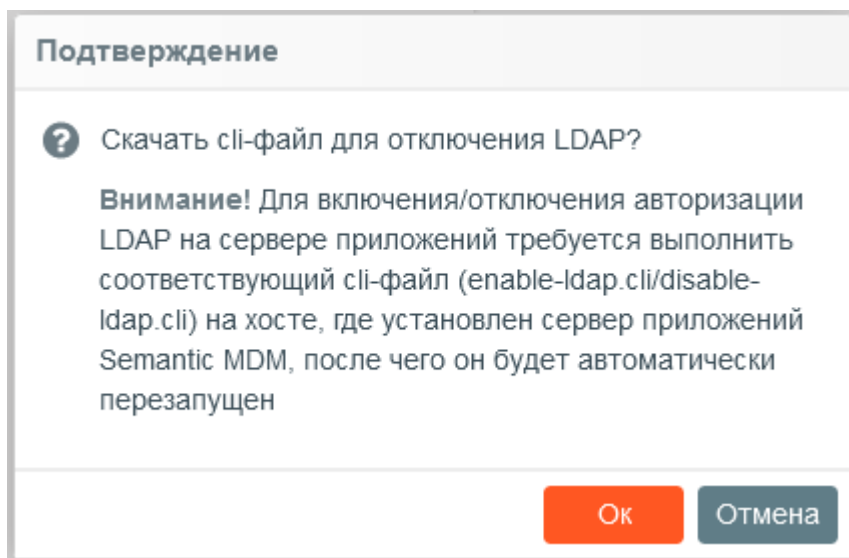
## Создание файла `disable-ldap.cli`

6. Войти в раздел настроек, нажав на главной странице Semantic MDM кнопку «Навигация»  и выбрать пункт «Настройки» .

7. Выключить переключатель «Авторизация через LDAP»



8. В появившемся окне «Подтверждение» нажать кнопку «ОК»



9. Сохранить файл `disable-ldap.cli` на диск.