H F Labs

Руководство по развертыванию

Оглавление

1 Подготовка к развертыванию

1.1 Методика расчета требований к аппаратному обеспечению

> Все аппаратные ресурсы должны быть доступны для EA монопольно, в том числе в случае использования виртуализации. В частности, диски для сервера приложений и сервера СУБД EA не должны использоваться другими виртуальными машинами.

Требования к процессору

Сервер приложений:

- Минимально Intel(R) Xeon(R) Silver 4114 или выше
- 1 – 10 млн исходных записей: 10 ядер на сервер.
- более 10 млн исходных записей: 20 ядер на сервер.
- более 100 млн исходных записей: 32 ядра на сервер.
- более 300 млн записей: 64 ядра на сервер.

Сервер СУБД:

- Минимально Intel(R) Xeon(R) Silver 4114 или выше
- 1 – 10 млн исходных записей: 10 ядер на сервер.
- более 10 млн исходных записей: 20 ядер на сервер
- более 300 млн исходных записей: 32 ядра на сервер

1.1.1 Требования к оперативной памяти

Сервер приложений:

- 1 – 5 млн исходных записей: 32 Гб.
- 5 — 10 млн исходных записей: 64 Гб
- более 10 млн. исходных записей: 64 Гб + 0.5*число записей (в млн) + 0.1*число связей (в млн).

СУБД:

- 1 – 10 млн. исходных записей: 32 Гб.
- более 10 млн. исходных записей: 48 Гб
- более 30 млн исходных кзаписей: 64 Гб
- более 70 млн исходных записей: 96 Гб.

1.1.2 Требования к дисковому пространству

Требования даны без учета дискового пространства под резервные копии.

Сервер приложений

- SSD-диск для прикладных данных:
    - IOPS произвольного чтения от 250 000,
    - IOPS произвольной записи от 50 000.
    - Минимум 1 000 TBW

Объем: 100Гб на приложение + 15 Гб на каждый 1 млн. исходных записей.
Пример: для 20 млн записей нужно 100+20*15 = 400 Гб

Сервер СУБД:

- Минимально Диски SAS 15K (Аппаратный RAID 10)
- Рекомендуется SSD-диски
    - IOPS произвольного чтения от 250 000,
    - IOPS произвольной записи от 50 000.
    - Минимум 10 000 TBW
- По 50 Гб на каждый 1 млн. исходных записей.

1.2 Информация для старта внедрения

1.2.1 Рабочая станция для HFLabs

1. Имя рабочей станции.
2. Учетная запись на рабочей станции:
    a. домен,
    b. логин,
    c. пароль.

1.2.2 Сервер приложений EA

1. Имя сервера и его ip-адрес. (2 сервера в случае отказоустойчивой конфигурации)
2. Учетная запись локального администратора на сервере приложений:
    a. домен,
    b. логин,
    c. пароль.
3. Учетные записи пользователей, под которыми будут работать службы «Единого адреса» и «Фактора» на сервере приложений:
    a. домен,
    b. логин,
    c. пароль.

1.2.3 СУБД

1. Hostname и IP-адрес.
2. Порт, на котором слушает Oracle.
3. SID или Service name Oracle.

4. Логин и пароль пользователя СУБД «Единого адреса».

1.2.4 Сервер Standby СУБД (в случае отказоустойчивой конфигурации)

1. Hostname и IP-адрес.
2. Порт, на котором слушает Oracle.
3. SID или Service name Oracle.
4. Логин и пароль пользователя СУБД «Единого адреса».

1.2.5 Active Directory

1. Hostname (или IP-адрес), порт для доступа к AD по протоколу LDAP.
2. Логин и пароль сервисной учетной записи.
3. dn ветки AD, в которой заведены учетные записи пользователей.
4. dn ветки AD, в которой заведены группы.

1.2.6 Сервер для почтовых оповещений

1. SMTP-сервер: адрес и порт;
2. Логин и пароль сервисной учетной записи для соединения с smtp-сервером;
3. Почтовый адрес, от имени которой будут приходить оповещения.

1.2.7 Сервер Подсказок (при наличии)

1. Имя сервера и его ip-адрес. (2 сервера в случае отказоустойчивой конфигурации)
2. Учетная запись локального администратора на сервере приложений:
    a. домен,
    b. логин,
    c. пароль.
3. Учетная запись пользователей, под которой будет работать служба «Подсказок» на сервере приложений:
    a. домен,
    b. логин,
    c. пароль.

1.2.8 Сервер балансировки (при наличии в отказоустойчивой конфигурации)

1. Имя сервера и его ip-адрес.

1.3 Требования к аппаратной платформе

В данном разделе представлены *минимальные* системные требования

Минимальная конфигурация состоит из сервера EA, сервера СУБД и рабочей станции для сотрудников HFLabs.

Конфигурация серверов зависит от планируемого объема исходных данных:

- до 1 млн данных,
- от 1 до 10 млн данных,
- от 10 до 50 млн данных,
- более 50 млн данных.

Для работы дата-стюардов нужно выделить им клиентские машины.

Для отказоустойчивой конфигурации с горячим резервом необходимы два равнозначных сервера EA и сервер Standby для СУБД, по конфигурации равнозначный основному серверу.

Для Подсказок нужен отдельный сервер Подсказок.

Для автоматического обновления справочников Подсказок и EA нужна рабочая станция с доступом к http://maven.hflabs.ru/artifactory.

В случае отказоустойчивой конфигурации с большой нагрузкой рекомендуем использовать два сервера Подсказок с выделенным Фактором.

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.

1.3.1 Сетевая инфраструктура

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

1. сервером приложений и сервером СУБД;
2. сервером приложений и сервером Active Directory.
3. двумя серверами приложений EA в отказоустойчивой конфигурации;
4. сервером Подсказок и сервером приложений EA;
5. сервером приложений EA и серверами приложения для очистки данных.

Требования к пропускной способности каналов между компонентами:

Компонент 1	Компонент 2	Ширина канала
Рабочая станция HFLabs	Сервер приложений EA	100 Мбит/с
Рабочая станция HFLabs	Сервер СУБД	100 Мбит/с
Рабочая станция HFLabs	Сервер Подсказок	100 Мбит/с
Рабочая станция HFLabs	Сервер приложений для очистки данных	100 Мбит/с
Сервер приложений EA	Сервер СУБД	1 Гбит/с
Сервер приложений EA 1	Сервер приложений EA 2	1 Гбит/с
Сервер Подсказок	Сервер приложений EA	1 Гбит/с

Компонент 1	Компонент 2	Ширина канала
Сервер приложений ЕА	Сервер приложений для очистки данных	1 Гбит/с
Рабочее место дата-стюарда	Сервер приложений ЕА	100 Мбит/с

1.3.2 Рабочая станция для HFLabs

1.3.2.1 Требования к рабочей станции для сотрудников HFLabs для внедрения и последующей поддержки

Параметр	Требование
Процессор	Intel Core i3 или новее
Оперативная память	8 Гб
Свободное место на жёстком диске	100 Гб
Разрешение экрана	1200×1024
Сетевая карта	100 Мбит
Операционная система	Windows 7 и выше
Разрядность ОС	64-bit
Java	Java SE Development Kit (JDK) 11, с установленными актуальными обновлениями.
Виртуальная среда	Можно использовать виртуальную среду или терминальный сервер
Приложения	• SQL Developer или SQL Workbench/J; • Notepad++ • Far Manager; • Базовый набор утилит из набора CygWIN— ls, cat, pwd, sed, grep, awk, bash, scp, ssh • WinSCP; • SoapUI • Firefox Quantum

1.3.2.2 Доступы и права

1. Рабочие станции внесены в домен.
2. Создан пользователь с правами локального администратора.
3. Открыт доступ к серверу приложений «Единого адреса» по портам:
    - 3389 (RDP) или 22 (SSH), в зависимости от платформы сервера приложений.
    - 8080 (HTTP-порт «Единого адреса»).
    - 18080 (HTTP-порт «Фактора»).

- 9990 (JMX-порт для мониторинга приложения «Единый адреса»).
- 19990 (JMX-порт для мониторинга приложения «Фактора»).

4. Доступна возможность копирования файлов на сервер приложений «Единого адреса» (по RDP или иным способом).
5. В случае СУБД Oracle — открыт доступ к серверу СУБД по порту 1521.
6. В случае СУБД Oracle или PostgreSQL:
   - 3389 (RDP) или 22 (SSH), в зависимости от платформы сервера СУБД.
   - 5432 — порт доступа к СУБД PostgreSQL.
7. Доступ к ресурсам HFLabs через сеть Интернет — confluence и jira.
8. Доступы к другим серверам (при их наличии):
   a. к серверу Подсказок по портам:
      - 3389 (RDP) или 22 (SSH), в зависимости от платформы сервера приложений.
      - 8080 (HTTP-порт «Подсказок»).
      - 18080 (HTTP-порт «Фактора»).
      - 9990 (JMX-порт для мониторинга приложения «Подсказок»).
      - 19990 (JMX-порт для мониторинга приложения «Фактора»).
   b. к серверам приложений для очистки данных по портам:
      - 3389 (RDP) или 22 (SSH), в зависимости от платформы сервера приложений.
      - 18080 (HTTP-порт «Фактора»).
      - 19990 (JMX-порт для мониторинга приложения «Фактора»).
   c. второму экземпляру сервера EA в случае отказоустойчивой конфигурации (горячий резерв):
      - 3389 (RDP) или 22 (SSH), в зависимости от платформы сервера приложений.
      - 8080 (HTTP-порт «Единого адреса»).
      - 18080 (HTTP-порт «Фактора»).
      - 9990 (JMX-порт для мониторинга приложения «Единый адрес»).
      - 19990 (JMX-порт для мониторинга приложения «Фактора»).

1.3.3 Сервера EA и СУБД до 1 млн записей

Все аппаратные ресурсы должны быть доступны для EA монопольно, в том числе в случае использования виртуализации. В частности, диски для сервера приложений и сервера СУБД EA не должны использоваться другими виртуальными машинами.

1.3.3.1 Сервер приложений EA

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 8 ядер
Оперативная память	24 Гб

Параметр	Требование
Объем жесткого диска	150 Гб
Скорость чтения с диска	SSD-диск для данных: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 1 000 TBW
Сетевая карта	1 Гбит
Операционная система	• **Рекомендуем**: CentOS 7+ или Red Hat Enterprise Linux 7+, x64. • Поддерживаем (+10% к стоимости поддержки): Windows 2008 Enterprise Edition и выше, x64.
Java	Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
Сервер приложений	Wildfly 16.0.0
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.3.3.2 Сервер СУБД

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 6 ядер
Оперативная память	16 Гб
Объем жесткого диска	150 Гб
Скорость чтения с диска	**Рекомендуем**: SSD с параметрами:: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 10 000 TBW Поддерживаем: SAS 15K (аппаратный RAID 10)
Сетевая карта	1 Гбит
СУБД	На выбор: • Oracle Database 12c Standard Edition. • PostgreSQL 11 версии
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.3.4 Сервера EA и СУБД от 1 до 10 млн исходных записей

Все аппаратные ресурсы должны быть доступны для EA монопольно, в том числе в случае использования виртуализации. В частности, диски для сервера приложений и сервера СУБД EA не должны использоваться другими виртуальными машинами.

1.3.4.1 Сервер приложений EA

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 10 ядер
Оперативная память	32 Гб
Объем жесткого диска	300 Гб
Скорость чтения с диска	SSD-диск для данных: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 1 000 TBW
Сетевая карта	1 Гбит
Операционная система	• **Рекомендуем**: CentOS 7+ или Red Hat Enterprise Linux 7+, x64. • Поддерживаем (+10% к стоимости поддержки): Windows 2008 Enterprise Edition и выше, x64.
Java	Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
Сервер приложений	Wildfly 16.0.0
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.3.4.2 Сервер СУБД

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 10 ядер
Оперативная память	32 Гб
Объем жесткого диска	500 Гб
Скорость чтения с диска	**Рекомендуем**: SSD с параметрами:: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 10 000 TBW Поддерживаем: SAS 15K (аппаратный RAID 10)
Сетевая карта	1 Гбит

Параметр	Требование
СУБД	На выбор: • Oracle Database 12c Standard Edition. • PostgreSQL 11 версии
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.3.5 Сервера EA и СУБД от 10 до 50 млн исходных записей

Все аппаратные ресурсы должны быть доступны для EA монопольно, в том числе в случае использования виртуализации. В частности, диски для сервера приложений и сервера СУБД EA не должны использоваться другими виртуальными машинами.

1.3.5.1 Сервер приложений EA

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 16 ядер
Оперативная память	64 Гб
Объем жесткого диска	1 Тб
Скорость чтения с диска	SSD-диск для данных: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 1 000 TBW
Сетевая карта	1 Гбит
Операционная система	• **Рекомендуем**: CentOS 7+ или Red Hat Enterprise Linux 7+, x64. • Поддерживаем (+10% к стоимости поддержки): Windows 2008 Enterprise Edition и выше, x64.
Java	Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
Сервер приложений	Wildfly 16.0.0
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.3.5.2 Сервер СУБД

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 16 ядер

Параметр	Требование
Оперативная память	64 Гб
Объем жесткого диска	2 Тб
Скорость чтения с диска	**Рекомендуем**: SSD с параметрами:: • IOPS произвольного чтения от 250 000, • IOPS произвольной записи от 50 000. • Минимум 10 000 TBW Поддерживаем: SAS 15K (аппаратный RAID 10)
Сетевая карта	1 Гбит
СУБД	Oracle: • Минимально Oracle Database 12c Enterprise Edition. • Рекомендуем: Oracle Database 12c Enterprise Edition с опцией Oracle Partitioning. • Для высокой доступности: Oracle Database 12c Enterprise Edition с опциями Oracle Active Data Guard или Oracle RAC (в зависимости от способа резервирования). Или PostgreSQL 11 версии
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.3.6 Сервера EA и СУБД более 50 млн исходных записей

Все аппаратные ресурсы должны быть доступны для EA монопольно, в том числе в случае использования виртуализации. В частности, диски для сервера приложений и сервера СУБД EA не должны использоваться другими виртуальными машинами.

1.3.6.1 Сервер приложений EA

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 1 000 TBW

Параметр	Требование
Сетевая карта	1 Гбит
Операционная система	CentOS 7+ или Red Hat Enterprise Linux 7+, x64.
Java	Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
Сервер приложений	Wildfly 16.0.0
Виртуальная среда	Не допускается, только аппаратная платформа

1.3.6.2 Сервер 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	Oracle: • Минимально Oracle Database 12c Enterprise Edition. • Рекомендуем: Oracle Database 12c Enterprise Edition с опцией Oracle Partitioning. • Для высокой доступности: Oracle Database 12c Enterprise Edition с опциями Oracle Active Data Guard или Oracle RAC (в зависимости от способа резервирования). Или PostgreSQL 11 версии
Виртуальная среда	Не допускается, только аппаратная платформа

1.3.7 Рабочее место дата-стюарда (клиентская часть)

Минимальные требования к клиентскому рабочему месту:

Параметр	Требование
Процессор	Intel Core i3 или новее
Оперативная память	4 Гб

Параметр	Требование
Свободное место на жёстком диске	10 Гб
Сетевая карта	100 Мбит
Операционная система	Windows 7 и выше
Разрядность ОС	64-bit
Разрешение экрана	1200×1024
Браузер	Рекомендуем: Mozilla Firefox Quantum версии 67+ или Google Chrome версии 75+ Поддерживаем: Internet Explorer версии 11+

1.3.8 Сервер Подсказок

Параметр	Требование
Процессор	Intel Xeon 6+ core Skylake или новее
Оперативная память	24+ Гб
Свободное место на жёстком диске	100 Гб (адреса) 200 Гб (адреса + компании)
Сетевая карта	1 Гбит\с
Скорость чтения с диска	SSD, 100k+ IOPS
Файловая система	Локальная (ext4), не сетевая (nfs)
Операционная система	• Red Hat Enterprise Linux 7+ • CentOS 7+
Разрядность ОС	64-bit

1.3.9 Сервер Подсказок с выделенным Фактором

Для получения отказоуйстойчивого решения, выдерживающего большое число запросов рекомендуем использовать 2 сервера Подсказок с выделенными Факторами.

1.3.9.1 Требования к серверу Подсказок с выделенным Фактором

Параметр	Требование
Процессор	Intel Xeon 12+ core Skylake или новее
Оперативная память	48+ Гб
Свободное место на жёстком диске	150 Гб (адреса) 250 Гб (адреса + компании)
Сетевая карта	1 Гбит\с
Скорость чтения с диска	SSD, 100k+ IOPS
Файловая система	Локальная (ext4), не сетевая (nfs)

Параметр	Требование
Операционная система	• Red Hat Enterprise Linux 7+ • CentOS 7+

1.3.10 Сервер приложений для очистки данных

Параметр	Требование
Процессор	Intel Xeon Processor серия E5-26xx v4 и выше от 8 ядер
Оперативная память	16 Гб
Объем жесткого диска	100 Гб
Скорость чтения с диска	Рекомендуем — SSD-диск для данных: • IOPS произвольного чтения от 100 000, • IOPS произвольной записи от 50 000. • Минимум 1 000 TBW. Возможно — HDD 7200
Сетевая карта	1 Гбит
Операционная система	• **Рекомендуем**: CentOS 6+ или Red Hat Enterprise Linux 6+, x64. • Поддерживаем:Windows 7 (x64) и выше или Windows 2008 Enterprise Edition и выше, x64.
Java	Java SE Development Kit (JDK) 8, с установленными актуальными обновлениями.
Сервер приложений	Wildfly 16.0.1
Виртуальная среда	Допускается

1.3.11 Сетевая инфраструктура

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

1. сервером приложений и сервером СУБД;
2. сервером приложений и сервером Active Directory.
3. двумя серверами приложений EA в отказоустойчивой конфигурации;
4. сервером Подсказок и сервером приложений EA;
5. сервером приложений EA и серверами приложения для очистки данных.

Требования к пропускной способности каналов между компонентами:

Компонент 1	Компонент 2	Ширина канала
Рабочая станция HFLabs	Сервер приложений EA	100 Мбит/с
Рабочая станция HFLabs	Сервер СУБД	100 Мбит/с
Рабочая станция HFLabs	Сервер Подсказок	100 Мбит/с
Рабочая станция HFLabs	Сервер приложений для очистки данных	100 Мбит/с
Сервер приложений EA	Сервер СУБД	1 Гбит/с
Сервер приложений EA 1	Сервер приложений EA 2	1 Гбит/с
Сервер Подсказок	Сервер приложений EA	1 Гбит/с
Сервер приложений EA	Сервер приложений для очистки данных	1 Гбит/с
Рабочее место дата-стюарда	Сервер приложений EA	100 Мбит/с

1.3.12 Рабочая станция для автоматического обновления справочников (апдейтер)

Минимальные требования к рабочей станции для установки утилиты по автоматическому скачиванию и перекладке справочников:

Параметр	Требование
Процессор	Intel Core i2 или новее
Оперативная память	4 Гб
Свободное место на жёстком диске	100 Гб
Сетевая карта	100 Мбит
Операционная система	Linux и установленный Python 2.7 или Python 3.5+.

С этой станции должен быть открыт доступ в интернет к ресурсу http://maven.hflabs.ru/artifactory.

1.4 Требования к настройке программно-аппаратной платформы

Требования к настройке программно-аппаратной платформы для развертывания Единого адреса.

1.4.1 Настройка рабочей станции для HFLabs

1.4.1.1 ОС и программное обеспечение

- Windows 7 и выше;
- Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями;
- SQL Developer или SQL Workbench/J;
- Notepad++;

- Far Manager;
- Базовый набор утилит из набора CygWIN— ls, cat, pwd, sed, grep, awk, bash, scp, ssh;
- WinSCP;
- SoapUI;
- Firefox Quantum.

1.4.1.2 Доступы и права

1. Создана учетная запись с правами локального администратора
2. Открыт доступ к серверу СУБД по портам:
    a. 22 (ssh) или 3889 (RDP);
    b. 1521 (Oracle) или 5432 (PostgreSQL).
3. Открыт доступ к серверу ЕА по портам:
    - 22 (ssh) или 3889 (RDP);
    - 8080 (HTTP-порт «Единого адреса»);
    - 18080 (HTTP-порт «Фактора»);
    - 9990 (порт для мониторинга «Единого адреса»);
    - 19990 (порт для мониторинга «Фактора»).
4. При наличии серверов приложений для очистки данных — открыт доступ к ним по портам:
    - 22 (ssh) или 3889 (RDP);
    - 18080 (HTTP-порт «Фактора»);
    - 19990 (порт для мониторинга «Фактора»).
5. При наличии сервера Подсказок — открыт доступ к ним по портам:
    - 22 (ssh) или 3889 (RDP);
    - 8080 (HTTP-порт «Подсказок»);
    - 9990 (порт для мониторинга «Подсказок»).
6. При наличии сервера Подсказок с выделенным Фактором — открыт доступ к ним по портам:
    - 22 (ssh) или 3889 (RDP);
    - 8080 (HTTP-порт «Подсказок»);
    - 9990 (порт для мониторинга «Подсказок»);
    - 18080 (HTTP-порт «Фактора»);
    - 19990 (порт для мониторинга «Фактора»).

1.4.2 Настройка сервера приложений ЕА (ОС *nix)

1.4.2.1 ОС и программное обеспечение

- CentOS 7+ или Red Hat Enterprise Linux 7+, x64.
- Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
- Wildfly 16.0.0

1.4.2.2 Установка и настройка

1. Созданы пользователи, под которым будут работать службы «Единого адреса» и «Фактора»:
    a. `eas` — для «Единого адреса»;
    b. factor — для «Фактора».

    Пользователи объединены в одну группу — `hfl`.
2. Создан пользователь `eas`_user с правами на sudo, под которым будут работать специалисты HFLabs при настройке и поддержке приложения.
3. Активирована служба ssh.
4. Установлен Java SE Development Kit (OpenJDK) 11 с последними обновлениями.

1.4.2.3 Доступы и права

1. Открыт доступ к серверу СУБД по порту, на котором слушает Oracle (1521) или PostgreSQL(5432).
2. Открыт доступ к серверам приложений для очистки данных по порту 8080.
3. Открыт доступ к серверу Active Directory по порту 3269.
4. Открыт доступ к SMTP-серверу по порту 25.
5. Открыты порты:
    - 22 (ssh);
    - 8080 (HTTP-порт «Единого адреса»);
    - 18080 (HTTP-порт «Фактора»);
    - 9990 (порт для мониторинга «Единого адреса»);
    - 19990 (порт для мониторинга «Фактора»).
6. Установка антивируса запрещена.

1.4.3 Настройка сервера приложений EA для ОС Windows

1.4.3.1 ОС и программное обеспечение

- Поддерживаемые ОС: Windows 2008 Enterprise Edition и выше, x64.
- Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
- Wildfly 16.0.0

1.4.3.2 Установка и настройка

1. Создан пользователь с правами локального администратора.
2. Создан пользователь, под которым будут работать службы «Единого адреса» и «Фактора».
3. Активирована служба Remote Desktop Services.
4. Установлен Java SE Development Kit (OpenJDK) 11 с последними обновлениями.

1.4.3.3 Доступы и права

1. Открыт доступ к серверу СУБД по порту, на котором слушает Oracle (1521) или Postgre (5432).
2. Открыт доступ к серверам приложений для очистки данных по порту 8080.
3. Открыт доступ к серверу Active Directory по порту 3269.

4. Открыт доступ к SMTP-серверу по порту 25.
5. Открыты порты:
    - 3389 (RDP)
    - 8080 (HTTP-порт «Единого адреса»)
    - 18080 (HTTP-порт «Фактора»)
    - 9990 (порт для мониторинга «Единого адреса»)
    - 19990 (порт для мониторинга «Фактора»).
6. Установка антивируса запрещена. В крайнем случае в настройки исключения антивируса должны быть добавлены:
    - файлы Oracle;
    - CDI_ROOT_DIR;
    - директории Wildfly для «Единого адреса» и «Фактора».

1.4.4 Настройка сервера СУБД Oracle

1.4.4.1 Версия ОС и конфигурация Oracle

- Рекомендуем: CentOS 7+ или Red Hat Enterprise Linux 7+, x64.
- Минимально достаточно: Oracle Database 11g Standard Edition. Версии 12C, 19c поддерживаем.
- Рекомендуемый вариант для базы с количеством исходных адресов более 10 млн: Oracle Database 11g Enterprise Edition.
- Если требуется организация архитектуры с высокой доступностью: Oracle Database 11g Enterprise Edition с включенными опциями Oracle Active Data Guard или Oracle RAC (способ резервирования на усмотрение Заказчика).

1.4.4.2 Установка и настройка

1. Установлены необходимые компоненты Oracle Database
    a. Oracle Database Catalog Views
    b. Oracle Database Packages and Types
2. Установлена кодировка БД (NLS_CHARACTERSET = AL32UTF8, NLS_NCHAR_CHARACTERSET = AL16UTF16).

1.4.4.3 Доступы и права

1. Открыт и прослушивается порт 1521 (или другой порт, используемый Oracle — его можно уточнить у администратора СУБД).
2. Выдан логин/пароль dbo для автоматического развертывания схемы eas.
3. Если dbo не выдают, то создать табличные пространства и пользователя для «Единого адреса».
   Вручную создать (либо запросить скрипт в поддержке):

-
    - Табличное пространство `eas` для таблиц Единого адреса

```
CREATE TABLESPACE eas DATAFILE 'eas_01.dat' SIZE 1000
M REUSE AUTOEXTEND ON NEXT 500 M;
```

-
    - Табличное пространство `eas_idx` для индексов

```
CREATE SMALLFILE TABLESPACE eas_idx DATAFILE
'eas_idx_01.dat' SIZE 500 M REUSE AUTOEXTEND ON NEXT
250 M;
```

    - Пользователь `eas` с табличным пространством по умолчанию `EAS` и правами:

```
CREATE MATERIALIZED VIEW
CREATE PROCEDURE
CREATE SEQUENCE
CREATE SESSION
CREATE SYNONYM
CREATE TABLE
CREATE TRIGGER
CREATE VIEW
SELECT ANY DICTIONARY
QUOTA UNLIMITED ON eas
QUOTA UNLIMITED ON eas_idx
```

1.4.5 Настройка сервера СУБД PostgreSQL — внутренняя

Удобный калькулятор для настройки параметров https://pgtune.leopard.in.ua

Актуальный файл настройки для версии 10.7 — postgresql.conf

1.4.6 Настройка Active Directory

1. В Active Directory (AD) добавлены группы, соответствующие ролям, существующим в системе:
    - Операционист (PERFORMER)
    - Оператор (OPERATOR)
    - Офицер информационной безопасности (GUARD)
    - Администратор (ADMINISTRATOR)
      Желательно, чтобы названия групп AD семантически соответствовали назначению ролей.
2. В AD созданы учетные записи для пользователей системы с соответствующими им ролями.
3. В AD создана тестовая учетная запись (для сотрудников HFLabs, которые будут производить внедрение системы). Тестовая учетная запись добавлена в группы AD, соответствующие ролям PERFORMER и ADMINISTRATOR.
4. В AD создана учетная запись для системы Единый адрес, 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 записи должен быть установлен режим без смены паролей.

1.4.7 Настройка сервера Подсказок

1.4.7.1 ОС и программное обеспечение

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Java SE Development Kit (JDK) 11 с установленными актуальными обновлениями.
- Wildfly 16

1.4.7.2 Установка и настройка

1. Создан пользователь suggestions, под которым будет работать служба «Подсказок».
2. Создан пользователь cdi_user с правами на sudo, под которым будут работать специалисты HFLabs при настройке и поддержке приложения.
3. Активирована служба ssh.
4. Установлен Java SE Development Kit (JDK) 11 с последними обновлениями.

1.4.7.3 Доступы и права

1. Открыты порты:
    - 22 (ssh);
    - 8080 (HTTP-порт «Подсказок»);
    - 9990 (порт для мониторинга «Подсказок»).

1.4.8 Настройка сервера Подсказок с выделенным Фактором

1.4.8.1 ОС и программное обеспечение

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Java SE Development Kit (JDK) 11 с установленными актуальными обновлениями.
- Wildfly 16

1.4.8.2 Установка и настройка

1. Создан пользователь suggestions, под которым будет работать служба «Подсказок».
2. Создан пользователь factor, под которым будет работать служба «Фактора».
3. Создан пользователь hfl с правами на sudo, под которым будут работать специалисты HFLabs при настройке и поддержке приложения.
4. Активирована служба ssh.
5. Установлен Java SE Development Kit (JDK) 11 с последними обновлениями.

1.4.8.3 Доступы и права

1. Открыты порты:
    - 22 (ssh);
    - 8080 (HTTP-порт «Подсказок»);
    - 9990 (порт для мониторинга «Подсказок»).
    - 18080 (HTTP-порт «Фактора»);
    - 19990 (порт для мониторинга «Фактора»).

1.4.9 Настройка сервера приложений для очистки данных (ОС *nix)

1.4.9.1 ОС и программное обеспечение

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Java SE Development Kit (JDK) 11 с установленными актуальными обновлениями.
- Wildfly 16.0.0.

1.4.9.2 Установка и настройка

1. Создан пользователь factor, под которым будет работать служба «Фактора»:
2. Создан пользователь hfl с правами на sudo, под которым будут работать специалисты HFLabs при настройке и поддержке приложения.
3. Активирована служба ssh.
4. Установлен Java SE Development Kit (JDK) 11 с последними обновлениями.

1.4.9.3 Доступы и права

1. Открыты порты:
    - 22 (ssh);
    - 18080 (HTTP-порт «Фактора»);
    - 19990 (порт для мониторинга «Фактора»).

1.4.10 Настройка сервера приложений для очистки данных (ОС Windows)

1.4.10.1 ОС и программное обеспечение

- Windows 7 (x64) и выше или Windows 2008 Enterprise Edition и выше, x64.
- Java SE Development Kit (JDK) 11 с установленными актуальными обновлениями.
- Wildfly 16.0.0.

1.4.10.2 Установка и настройка

1. Создан пользователь с правами локального администратора.
2. Создан пользователь, под которым будет работать служба «Фактора».
3. Активирована служба Remote Desktop Services.
4. Установлен Java SE Development Kit (JDK) 8 с последними обновлениями.

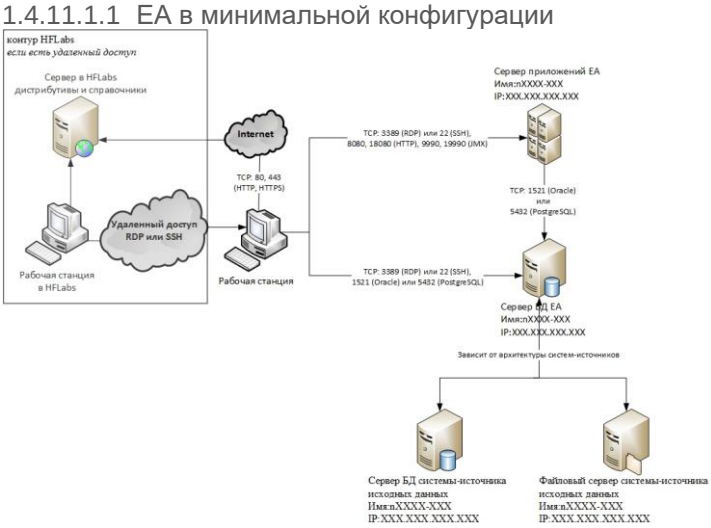
1.4.10.3 Доступы и права

1. Открыты порты:
    - 3389 (RDP);
    - 18080 (HTTP-порт «Фактора»);
    - 19990 (порт для мониторинга «Фактора»).
2. Установка антивируса запрещена. В крайнем случае в настройки исключения антивируса должны быть добавлены директории Wildfly «Фактора».

1.4.11 Логическая схема развертывания Единого адреса

1.4.11.1 Пилотный проект Единый адрес. Логическая схема развертывания

1.4.11.1.1 EA в минимальной конфигурации

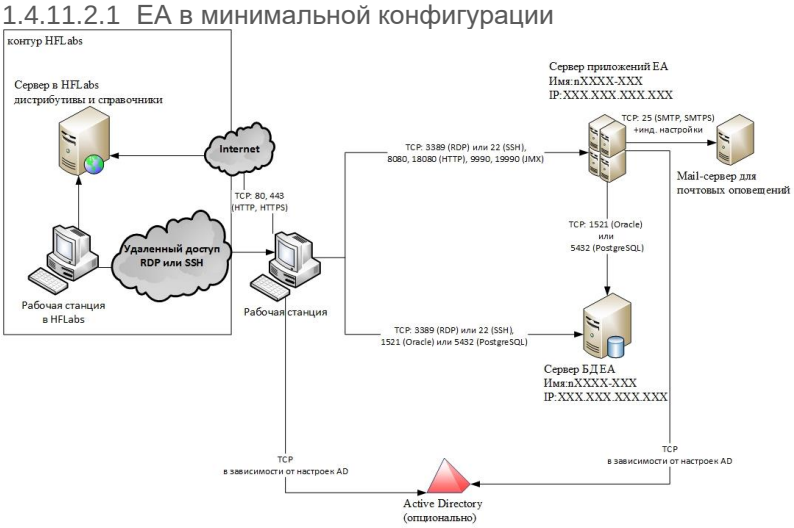


1.4.11.1.2 EA с фермой «Факторов»

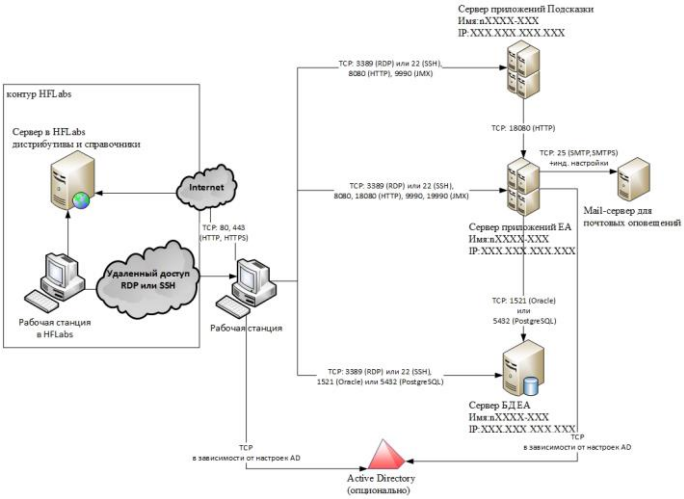
Для очистки большого объема данных в короткий срок требуется несколько серверов приложений для очистки данных. Количество серверов приложений для очистки данных (ферма «Факторов») зависит от объема данных и аппаратных возможностей конкретного проекта.

1.4.11.2 Внедрение проекта Единый адрес. Логическая схема развертывания

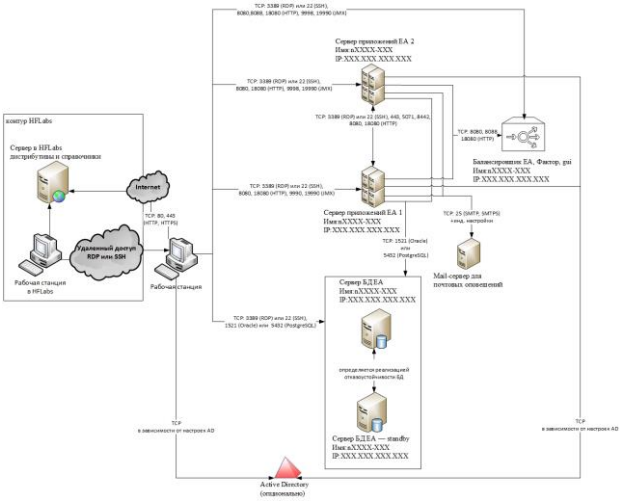
1.4.11.2.1 EA в минимальной конфигурации



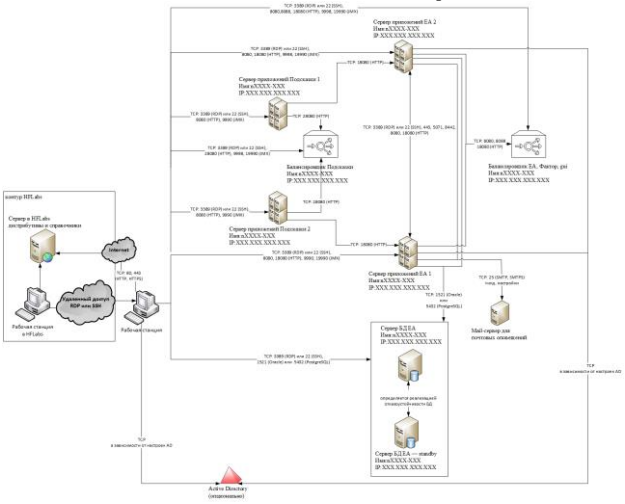
1.4.11.2.2 EA с сервером Подсказок



1.4.11.2.3 EA в отказоустойчивой конфигурации



1.4.11.2.4 EA и подсказки в отказоустойчивой конфигурации



1.4.12 Таблица сетевых доступов

Таблица сетевых доступов для пилотного проекта с развертыванием фермы Факторов для быстрой обработки большого объема данных

№	Источник запроса			Получатель запроса			Протокол	Назначение и описание информационного потока (какой тип данных передается)
	Имя (DNS-имя)	IP-адрес(а)	Порт(ы)	Имя (DNS-имя)	IP-адрес(а)	Порт(ы)		
1	Взаимодействие между различными сегментами безопасности							
1.1.	рабочая станция	XXX.XXX.XXX.XXX	>=1024	Сервера приложения для очистки данных №1-5	XXX.XXX.XXX.XXX	22 или 3389	TCP	Установка и настройка приложений
				Сервер приложений EA	XXX.XXX.XXX.XXX			Установка и настройка приложений
				Сервер БД EA	XXX.XXX.XXX.XXX			Установка и настройка приложений
1.2.	рабочая станция	XXX.XXX.XXX.XXX	>=1024	Сервера приложения для очистки данных №1-5	XXX.XXX.XXX.XXX	18080, 19990	TCP	работа с приложений через веб-интерфейс + мониторинг работы приложения
1.3.	рабочая станция	XXX.XXX.XXX.XXX	>=1024	Сервер приложений EA	XXX.XXX.XXX.XXX	8080, 18080, 9990, 19990	TCP	работа с приложений через веб-интерфейс + мониторинг работы приложения
1.4.	рабочая станция	XXX.XXX.XXX.XXX	>=1024	Сервер БД EA	XXX.XXX.XXX.XXX	1521 (Oracle) или 5432(PostgreSQL)	TCP	Настрйока СУБД для работы приложения, анализ данных
1.5.	рабочая станция	XXX.XXX.XXX.XXX	>=1024	сервер HFLabs		80, 443	TCP	получение дистрибутиво в системы, документации из confluence HFLabs, дополнительных справочников
1.6.	рабочая станция в HFLabs	XXX.XXX.XXX.XXX	>=1024	рабочая станция	XXX.XXX.XXX.XXX	22 или 3389	TCP	установка и настройка приложения
2	Взаимодействия между компонентами подсистемы							

2.1.	сервер приложений EA	XXX.XXX.XXX.XXX	>=1024	Сервера приложения для очистки данных №1-5	XXX.XXX.XXX.XXX	18080	TCP	Выполнение очистки и стандартизации данных
2.2.	сервер приложений EA	XXX.XXX.XXX.XXX	>=1024	сервер БД EA	XXX.XXX.XXX.XXX	1521 (Oracle) или 5432(PostgreSQL)	TCP	Сохранение данных в БД и получение данных для обработки
3	Взаимодействие с иными подсистемами							
3.x.	сервер БД или файловый сервер системы-источника	XXX.XXX.XXX.XXX	>=1024	сервер БД ЕК	XXX.XXX.XXX.XXX	?	TCP	Загрузка данных для пилотного проекта в БД EA

2 Инсталляционный пакет

Файл	Назначение
`wildfly-16.0.0.Final-18080.zip`	JBoss Application Server для системы Фактор.
`wildfly-16.0.0.Final-8080.zip`	JBoss Application Server для системы Единый адрес.
`factor-{customer}-{version}.war`	Система Фактор
`cdi-web-{customer}-{version}.war`	Система Единый адрес

3 Установка системного и специального ПО

3.1 Установка параметров ОС Windows

Команды должны выполняться под пользователем с правами локального администратора.

```
reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters /v
MaxUserPort /t REG_DWORD /d 0xfffe /f
```

3.2 Создание пользователей ОС Linux

3.2.1 Создание пользователей для «Единого адреса» и «Фактора»

Создайте пользователей, под которыми будут работать сервера приложений «Единого клиента» и «Фактора» — `eas` и `factor`:

```
useradd eas
useradd factor
passwd -l eas
passwd -l factor
```

Пользователей нужно объединить в одну группу:

```
groupadd hfl
usermod -a -G hfl eas
usermod -a -G hfl factor
```

3.2.2 Создание пользователей для «Подсказок»

Создайте пользователя, под которым будут работать сервер приложений «Подсказки» — `suggestions`:

```
useradd suggestions
passwd -l suggestions
```

3.2.3 Создание пользователей для «Единого адреса» и «Фактора»

Создайте пользователей, под которыми будут работать сервера приложений «Единого клиента» и «Фактора» — `eas` и `factor`:

```
useradd eas
useradd factor
```

```
passwd -l eas
passwd -l factor
```

Пользователей нужно объединить в одну группу:

```
groupadd hfl
usermod -a -G hfl eas
usermod -a -G hfl factor
```

3.2.4 Создание пользователей для «Подсказок»

Создайте пользователя, под которым будут работать сервер приложений «Подсказки» — `suggestions`:

```
useradd suggestions
passwd -l suggestions
```

3.3 Установка параметров ОС Linux для EA и Фактор

3.3.1 Запрет на выделение памяти сверх того, что есть и отключение SWAP

1. Откройте файл `/etc/sysctl.conf` и добавьте в него строки:

   Code Block 1 /etc/sysctl.conf

   ```
   #Do not overcommit memory
   vm.overcommit_memory=2
   vm.overcommit_ratio=100

   #Max map count
   vm.max_map_count = 16777216


   # Low swap level
   vm.swappiness = 10
   ```

2. Использование SWAP сильно тормозит работу приложений, поэтому его использование лучше честно отключить. Открывайте файл `/etc/fstab` и закомментируйте в нем монтирования раздела swap вида.

   Code Block 2 /etc/fstab

   ```
   %SOME_TEXT% swap                    swap    defaults        0 0
   ```

3. Перезагрузите операционную систему.
4. Проверьте параметры с помощью команды:

```
sysctl -p
либо
systemctl -p
```

Расшифровка параметров:

`vm.swappiness` → при каком значении нужно пытаться перекладывать куски памяти в swap (в процентах). По умолчанию это 60 (т.е. если осталось свободно 60 процентов оперативки, то начать пытаться перекладывать давно неиспользуемые куски в swap). Установка этого параметра в 10 позволит максимально использовать оперативку, без задействования swap-а (0 ставить нельзя, т.к. хоть по документации это и отключает swap вообще, но многие ОС это игнорируют)

3.3.1.1 Определение версии linux

Для дальнейшей работы потребуется определить семейство и версию linux.

Сделать это можно, выполнив команду

```
cat /etc/*-release
```

и проанализировать вывод. Наличие там слова debian будет означать, что это семейство debian, наличие redhat — что это redhat. Цифра даст понимание версии.

К сожалению, какой-то общей и чёткой инструкции дать не получится, слишком велико разнообразие linux.

3.3.2 Увеличение предела открытых дескрипторов файлов

3.3.3 Увеличение предела открытых дескрипторов файлов для redhat-based-6 дистрибутива

1. Откройте файл `/etc/security/limits.conf` и добавьте в него строки:

   Code Block 3 /etc/security/limits.conf

   ```
   eas             hard    nofile  65535
   eas             soft    nofile  65535
   eas             hard    nproc   8192
   eas             soft    nproc   4096
   eas             hard    as      unlimited
   eas             soft    as      unlimited
   eas             hard    rss     unlimited
   eas             soft    rss     unlimited
   factor          hard    nofile  65535
   factor          soft    nofile  65535
   factor          hard    nproc   8192
   factor          soft    nproc   4096
   factor          hard    as      unlimited
   factor          soft    as      unlimited
   factor          hard    rss     unlimited
   factor          soft    rss     unlimited
   ```

   Где `factor` и `eas` — имена пользователей, под которыми работают «Фактор» и «Единый адрес».

2. Перезагрузите ОС, чтобы настройки вступили в силу.
3. Залогиньтесь под пользователем «Фактора» и убедитесь, что настройки применены:

```
su factor -s /bin/sh

sysctl vm.max_map_count
ulimit -n
ulimit -u
ulimit -v
ulimit -m
```

Должно получиться следующее:

```
$ sysctl vm.max_map_count
vm.max_map_count = 16777216

$ ulimit -n
65535

$ ulimit -u
4096

$ ulimit -v
unlimited

$ ulimit -m
unlimited
```

4. Залогиньтесь под пользователем "Единого адреса" и убедитесь, что настройки применены:

```
su cdi -s /bin/sh

$ ulimit -n
65535

$ ulimit -u
4096

$ ulimit -v
unlimited

$ ulimit -m
unlimited
```

3.3.4 Настройка для работы с SSD-дисками

Если на сервере приложений установлены SSD-диски, то нужны дополнительные настройки для увеличения производительности

3.3.4.1 Отключение времени модификации файлов

Если приложение часто и многократно пишет и читает файлы (именно так делают «Единый адрес», «Фактор», «Подсказки»), то на файловых системах **ext3** и **ext4** нужно отключить дополнительные функции работы метаданными файлов.

Для этого нужно изменить параметры монтирования диска, добавив следующие опции:

1. **noatime** - полностью отключает запись времени доступа к файлу. Большинство программ не используют это поле.

2. **data=ordered** - журналирует только изменения метаданных, но обновления данных сбрасываются на жесткий диск до совершения транзакции. Данные записываются не атомарно, но этот режим гарантирует, что после падения файлы не будут содержать блоки данных из устаревших файлов.

В итоге строка в */etc/fstab* должна выглядеть примерно следующим образом (**sdX** - устройство SSD)

Code Block 4 /etc/fstab

```
# <fs>    <mountpoint> <type>  <opts>                          <dump/pass>
/dev/sdX  /opt          ext4
defaults,noatime,data=ordered,errors=remount-ro 0 2
```

3.3.4.2 Выключите IO Scheduller для SSD

Выполните команду и добавьте ее в скрипт автозапуска

```
echo noop > /sys/block/sdX/queue/scheduler
```

для каждого устройства (заменяя **sdX** на нужное имя)

3.3.5 Отключение SWAP

Использование SWAP сильно тормозит работу приложений, поэтому его использование лучше честно отключить.

Откройте файл /etc/fstab и закомментируйте в нем монтирования раздела swap вида.

Code Block 5 /etc/fstab

```
%SOME_TEXT% swap                    swap    defaults        0 0
```

Перезагрузите операционную систему.

3.3.6 Настройка Linux для активной работы с SSD

3.3.6.1 Отключение времени модификации файлов

Если приложение часто и многократно пишет и читает файлы (именно так делают «Единый адрес», «Фактор», «Подсказки»), то на файловых системах **ext3** и **ext4** нужно отключить дополнительные функции работы метаданными файлов.

Для этого нужно изменить параметры монтирования диска, добавив следующие опции:

1. **noatime** - полностью отключает запись времени доступа к файлу. Большинство программ не используют это поле.
2. **data=ordered** - журналирует только изменения метаданных, но обновления данных сбрасываются на жесткий диск до совершения транзакции. Данные записываются не атомарно, но этот режим гарантирует, что после падения файлы не будут содержать блоки данных из устаревших файлов.

В итоге строка в */etc/fstab* должна выглядеть примерно следующим образом (**sdX** - устройство SSD)

Code Block 6 /etc/fstab

```
# <fs>    <mountpoint> <type>  <opts>                              <dump/pass>
/dev/sdX  /opt          ext4
defaults,noatime,data=ordered,errors=remount-ro 0 2
```

3.3.6.2 Выключите IO Scheduller для SSD

Выполните команду и добавьте ее в скрипт автозапуска

```
echo noop > /sys/block/sdX/queue/scheduler
```

для каждого устройства (заменяя **sdX** на нужное имя)

3.3.7 Увеличение предела открытых дескрипторов файлов для redhat-based-6 дистрибутива

1. Откройте файл `/etc/security/limits.conf` и добавьте в него строки:

   Code Block 7 /etc/security/limits.conf

   ```
   eas             hard    nofile  65535
   eas             soft    nofile  65535
   eas             hard    nproc   8192
   eas             soft    nproc   4096
   eas             hard    as      unlimited
   eas             soft    as      unlimited
   eas             hard    rss     unlimited
   eas             soft    rss     unlimited
   factor          hard    nofile  65535
   factor          soft    nofile  65535
   factor          hard    nproc   8192
   factor          soft    nproc   4096
   factor          hard    as      unlimited
   factor          soft    as      unlimited
   factor          hard    rss     unlimited
   factor          soft    rss     unlimited
   ```

   Где `factor` и `eas` — имена пользователей, под которыми работают «Фактор» и «Единый адрес».

2. Перезагрузите ОС, чтобы настройки вступили в силу.
3. Залогиньтесь под пользователем «Фактора» и убедитесь, что настройки применены:

   ```
   su factor -s /bin/sh

   sysctl vm.max_map_count
   ulimit -n
   ulimit -u
   ```

```
ulimit -v
ulimit -m
```

Должно получиться следующее:

```
$ sysctl vm.max_map_count
vm.max_map_count = 16777216

$ ulimit -n
65535

$ ulimit -u
4096

$ ulimit -v
unlimited

$ ulimit -m
unlimited
```

4. Залогиньтесь под пользователем "Единого адреса" и убедитесь, что настройки применены:

```
su cdi -s /bin/sh

$ ulimit -n
65535

$ ulimit -u
4096

$ ulimit -v
unlimited

$ ulimit -m
unlimited
```

3.4 Установка Java

Для работы системы должен использоваться `openJDK` 11 версии не ниже `11.0.4`

3.4.1 Установочный пакет

В случае выбора операционной системы Linux приоритетным вариантом установки является установка из репозитория ОС. Альтернативно возможно использование архива AdoptOpenJDK.

Установочный пакет можно скачать с сайта проекта AdoptOpenJDK по ссылке https://adoptopenjdk.net/?variant=openjdk11&jvmVariant=hotspot:

- удостовериться что выбрана версия `OpenJDK 11 (LTS)` и `JVM Hotspot`;
- Нажать кнопку Latest release;

- Выбрать вид тип установочного пакета, подходящего для ОС сервера.
- Скачать установочный пакет.

3.4.2 Установка JDK

3.4.2.1 Windows

Установите JDK с помощью скачанного установочного пакета.

3.4.2.2 Linux

 Приоритетным является вариант установки через репозиторий ОС.

Пример (CentOS 7 и Red Hat 7):

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

Пример (Debian-based дистрибутивы):

```
sudo apt-get install java-11-openjdk
```

После этого можно перейти к проверке правильности установки JDK

Если доступа к репозиториям нет, то возможно использовать альтернативный вариант установки: установка вручную из архива AdopOpenJDK (при необходимости, заменить ссылку https://github.com/AdoptOpenJDK/openjdk11-binaries/releases/download/jdk-11.0.4+11/OpenJDK11U-jdk_x64_linux_hotspot_11.0.4_11.tar.gz на ссылку на более новую версию установочного пакета):

```
mkdir /usr/java/
cd /usr/java/
wget https://github.com/AdoptOpenJDK/openjdk11-
binaries/releases/download/jdk-11.0.4+11/OpenJDK11U-
jdk_x64_linux_hotspot_11.0.4_11.tar.gz
tar zxvf OpenJDK11U-jdk_x64_linux_hotspot_11.0.4_11.tar.gz
rm OpenJDK11U-jdk_x64_linux_hotspot_11.0.4_11.tar.gz
alternatives --install /usr/bin/java java /usr/java/jdk-
11.0.4+11/bin/java 2
alternatives --install /usr/bin/jar jar /usr/java/jdk-11.0.4+11/bin/jar 2
alternatives --install /usr/bin/javac javac /usr/java/jdk-
11.0.4+11/bin/javac 2
alternatives --set java /usr/java/jdk-11.0.4+11/bin/java
alternatives --set jar /usr/java/jdk-11.0.4+11/bin/jar
alternatives --set javac /usr/java/jdk-11.0.4+11/bin/javac
```

Для Debian-based дистрибутивов вместо `alternatives` необходимо использовать команду `update-alternatives`.

3.4.3 Проверка правильности установки JDK

Выполнить в командной строке команду

```
javac -version
```

Должно появиться сообщение вида

```
javac 11.0.4
```

Версия JDK должна соответствовать версии установочного пакета.

Также нужно проверить версию самой java-машины:

```
java -version
```

Она должна быть идентична версии javac.

3.4.4 Установка переменных окружения

Если в результате проверки правильности установки JDK система вернула ошибку, то необходимо установить переменные окружения вручную. В противном случае этот шаг следует пропустить.

3.4.4.1 Windows

Для пользователя HFL_USER, выполнить следующие команды, предварительно заменив C:\Program Files\AdoptOpenJDK\jdk-11.0.4.11-hotspot на полный путь к каталогу, в который установлен JDK:

```
setx JAVA_HOME "C:\Program Files\AdoptOpenJDK\jdk-11.0.4.11-hotspot"
setx PATH "%PATH%;%JAVA_HOME%\bin"
```

3.4.4.2 Linux

Для пользователей eas, factor в файлах /home/eas/.bash_profile, /home/cdi/.bash_profile (так же в /etc/profile или /etc/skel/profile) добавьте строки, предварительно заменив /usr/java/jdk-11.0.4+11/ на полный путь к каталогу, в который установлен JDK:

```
export JAVA_HOME=/usr/java/jdk-11.0.4+11/
export PATH=$JAVA_HOME/bin:$PATH
```

После добавления строк выполнить одну из комманд приведенных ниже:

```
source /etc/profile
source /etc/skel/.profile
```

Проверить, что путь был добавлен, можно выполнив команду:

```
echo $PATH
```

В ответе должен быть заметен путь к каталогу с Java.

После этого нужно повторно проверить версии java и javac.

3.5 Установка JBOSS

3.5.1 Инструкция для серверов с ОС семейства Linux

Установочный пакет

Установочные пакеты Jboss поставляются совместно с системой в архивах:

- `wildfly-16.0.0.Final-8080.zip` — для «Единого адреса».
- `wildfly-16.0.0.Final-8080-HotReserve.zip` — для «Единого адреса» с горячим резервированием.
- `wildfly-16.0.0.Final-18080.zip` — для «Фактора».

3.5.1.1 Установка WildFly

1. Распаковать архив с WildFly в каталог `JBOSS_HOME`. Здесь и далее используется каталог `/opt` в качестве примера. Вы можете использовать любую другую, паример /home или /data.

```
unzip wildfly-16.0.0.Final-8080.zip -d /opt/eas
unzip wildfly-16.0.0.Final-18080.zip -d /opt/factor

mv /opt/eas/wildfly* /opt/eas/jboss
mv /opt/factor/wildfly* /opt/factor/jboss
```

2. Назначить созданным директориям соответствующих владельцев – `eas` для `/opt/eas/` и `factor` для `/opt/factor/`

```
chown -R eas:eas /opt/eas/
chown -R factor:factor /opt/factor/
```

3. Назначить права на запуск исполняемых файлов:

```
find /opt/{factor,eas}/jboss/ -type d -exec chmod 755 {} \;
find /opt/{factor,eas}/jboss/ -type f -exec chmod 644 {} \;
find /opt/{factor,eas}/jboss/ -type f -name "*.sh" -exec chmod 755 {} \;
```

3.5.1.2 Настройка сервисов

Шаги для настройки сервисов на redhat-based-7:

1. Создать директорию в `/etc` с названием будущей службы (`factor`, eas), скопировать файлы

```
mkdir /etc/eas
mkdir /etc/factor

cp /opt/eas/jboss/docs/contrib/scripts/systemd/wildfly.conf
/etc/eas/
cp /opt/eas/jboss/docs/contrib/scripts/systemd/wildfly.service
/etc/systemd/system/eas.service
cp /opt/eas/jboss/docs/contrib/scripts/systemd/launch.sh
```

```
/opt/eas/jboss/bin/

cp /opt/factor/jboss/docs/contrib/scripts/systemd/wildfly.conf
/etc/factor/
cp /opt/factor/jboss/docs/contrib/scripts/systemd/wildfly.service
/etc/systemd/system/factor.service
cp /opt/factor/jboss/docs/contrib/scripts/systemd/launch.sh
/opt/factor/jboss/bin/
```

2. В `/etc/systemd/system/factor.service` и `/etc/systemd/system/eas.service` переменные заданы по умолчанию. При необходимости заменить параметры `Limit*` и путь к `launch.sh` (параметр `ExecStart`).

Code Block 8 cdi.service

```
[Unit]
Description=EAS WildFly Application Server
After=syslog.target network.target
Before=httpd.service

[Service]
Environment=LAUNCH_JBOSS_IN_BACKGROUND=1
EnvironmentFile=-/etc/eas/wildfly.conf
User=eas
OOMScoreAdjust=-1000
PIDFile=/var/run/eas/wildfly.pid
ExecStart=/opt/eas/jboss/bin/launch.sh $WILDFLY_MODE
$WILDFLY_CONFIG $WILDFLY_BIND
StandardOutput=syslog
StandardError=syslog
LimitNOFILE=65535
LimitNPROC=8192
LimitAS=infinity
LimitRSS=infinity

[Install]
WantedBy=multi-user.target
```

Code Block 9 factor.service

```
[Unit]
Description=Factor WildFly Application Server
After=syslog.target network.target
Before=httpd.service

[Service]
Environment=LAUNCH_JBOSS_IN_BACKGROUND=1
EnvironmentFile=-/etc/factor/wildfly.conf
User=factor
OOMScoreAdjust=-1000
PIDFile=/var/run/factor/wildfly.pid
ExecStart=/opt/factor/jboss/bin/launch.sh $WILDFLY_MODE
$WILDFLY_CONFIG $WILDFLY_BIND
StandardOutput=syslog
StandardError=syslog
LimitNOFILE=65535
LimitNPROC=8192
LimitAS=infinity
LimitRSS=infinity

[Install]
WantedBy=multi-user.target
```

3. Указать путь к домашней директории Jboss в `/opt/factor/jboss/bin/launch.sh`

```
WILDFLY_HOME="/opt/factor/jboss"
```

и в `/opt/eas/jboss/bin/launch.sh`

```
WILDFLY_HOME="/opt/eas/jboss"
```

4. На файлы `launch.sh` и `standalone.sh` выдать права на запуск:

```
chmod +x /opt/eas/jboss/bin/launch.sh
chmod +x /opt/eas/jboss/bin/standalone.sh

chmod +x /opt/factor/jboss/bin/launch.sh
chmod +x /opt/factor/jboss/bin/standalone.sh
```

5. Перезагрузить список доступных сервисов, чтобы systemd мог управлять новым сервисом:

```
systemctl daemon-reload
```

6. Добавить службы в автозапуск:

```
systemctl enable eas.service
systemctl enable factor.service
```

3.5.2 Инструкция для серверов с ОС семейства Windows

3.5.2.1 Установочный пакет

Установочные пакеты JBoss поставляются совместно с системой в архивах:

- `wildfly-16.0.0.Final-8080.zip` — для «Единого адреса».
- `wildfly-16.0.0.Final-8080-HotReserve.zip` — для «Единого адреса» с горячим резервированием.
- `wildfly-16.0.0.Final-18080.zip` — для «Фактора».

3.5.2.2 Установка JBOSS

Распакуйте архивы с JBoss в выбранную директорию, например `C:\jboss\`.

3.5.2.3 Создание системных служб запуска JBOSS

Установите системные службы (команду `service.bat install` следует выполнять из директории `\bin\service\` соответствующего jboss с правами администратора):

```
cd C:\jboss\wildfly-16.0.0.Final-cdi\bin\service
service.bat install

cd C:\jboss\wildfly-16.0.0.Final-factor\bin\service
service.bat install
```

При успешной установке сервиса должно вывестись сообщение следующего вида:

```
Using the X86-64bit version of prunsrv

"C:\jboss\wildfly-16.0.0.Final-cdi\bin\service\amd64\wildfly-service"
install cdi <...>"
Service cdi installed
```

3.6 Настройка Linux для Подсказок

3.6.1 Подсказки

3.6.1.1 Увеличение max_map_count

1. Отредактируйте файл `/etc/sysctl.conf` и добавьте в него параметр:

```
vm.max_map_count = 1677721
```

2. Перезагрузите ОС, чтобы настройки вступили в силу (перезагружать можно после увеличения файловых дескрипторов, чтобы один раз)

3. Залогиньтесь под пользователем подсказок и убедитесь, что настройка применилась:

```
# su - suggestions

$ sysctl vm.max_map_count
vm.max_map_count = 16777216
```

3.6.1.2 Увеличение предела открытых дескрипторов файлов для redhat-based-6 дистрибутива

1. Отредактируйте файл `/etc/security/limits.conf` и добавьте в него строки:

```
suggestions          hard    nofile  65535
suggestions          soft    nofile  65535
suggestions          hard    nproc   16384
suggestions          soft    nproc   8192
suggestions          hard    as      unlimited
suggestions          soft    as      unlimited
suggestions          hard    rss     unlimited
suggestions          soft    rss     unlimited
```

Где suggestions — имя пользователя, под которым будут работать подсказки.

2. Перезагрузите ОС, чтобы настройки вступили в силу

3. Залогиньтесь под пользователем подсказок и убедитесь, что настройка применилась:

```
# su - suggestions

$ sysctl vm.max_map_count
vm.max_map_count = 16777216

$ ulimit -n
65535

$ ulimit -u
4096

$ ulimit -v
unlimited

$ ulimit -m
unlimited
```

3.6.1.3 Увеличение предела открытых дескрипторов файлов для redhat-based-7 дистрибутива

1. Создайте текстовый файл `/etc/systemd/system/suggestions.service.d/limits.conf`
2. Впишите в него текст:

Code Block 10 limits.conf

```
[Service]
LimitNOFILE=65535
LimitNPROC=16384
LimitAS=infinity
LimitRSS=infinity
```

3.6.2 Настройка для оптимальной работы с SSD-дисками

3.6.2.1 Отключение времени модификации файлов

Если приложение часто и многократно пишет и читает файлы (именно так делают «Единый адрес», «Фактор», «Подсказки»), то на файловых системах **ext3** и **ext4** нужно отключить дополнительные функции работы метаданными файлов.

Для этого нужно изменить параметры монтирования диска, добавив следующие опции:

1. **noatime** - полностью отключает запись времени доступа к файлу. Большинство программ не используют это поле.
2. **data=ordered** - журналирует только изменения метаданных, но обновления данных сбрасываются на жесткий диск до совершения транзакции. Данные записываются не атомарно, но этот режим гарантирует, что после падения файлы не будут содержать блоки данных из устаревших файлов.

В итоге строка в */etc/fstab* должна выглядеть примерно следующим образом (**sdX** - устройство SSD)

Code Block 11 /etc/fstab

```
# <fs>    <mountpoint> <type>  <opts>                          <dump/pass>
/dev/sdX  /opt          ext4
defaults,noatime,data=ordered,errors=remount-ro 0 2
```

3.6.2.2 Выключите IO Scheduller для SSD

Выполните команду и добавьте ее в скрипт автозапуска

```
echo noop > /sys/block/sdX/queue/scheduler
```

для каждого устройства (заменяя **sdX** на нужное имя)

4 Установка системы

4.1 Установка Фактора

4.1.1 Копирование исполняемых файлов Фактора

Скопируйте следующие файлы в каталог JBoss Фактора `standalone/deployments`:

```
factor-{customer}-{version}.war
```

4.1.2 Настройка параметров запуска JBoss (Linux)

В директории JBoss Фактора настройте в файле `bin/standalone.conf (Linux)` или в файле `bin\standalone.conf.bat (Windows)` следующие параметры запуска JVM:

```
-Xms8g
-Xmx24g
```

Параметры `Xms` и `Xmx` (минимальный и максимальный размер кучи (heap) в мегабайтах, выделяемый серверу приложений) могут варьироваться в зависимости от доступного объема оперативной памяти на сервере, но не должны превышать его.

4.2 Установка системы Единый адрес

4.2.1 Настройка горячего резерва

Выполните инструкцию.

4.2.2 Настройка datasource для заказчиков, использующих шифрованный пароль к БД

Для шифрования пароля выполнить в командной строке следующую команду из директории JBoss EA:

4.2.2.1 Windows

```
java -cp .\modules\system\layers\base\org\picketbox\main\picketbox-
5.0.3.Final.jar
org.picketbox.datasource.security.SecureIdentityLoginModule
пароль_для_шифрования
```

4.2.2.2 Linux

```
java -cp ./modules/system/layers/base/org/picketbox/main/picketbox-
5.0.3.Final.jar
org.picketbox.datasource.security.SecureIdentityLoginModule
пароль_для_шифрования
```

Результатом выполнения команды будет зашифрованный пароль.

В файле `standalone/configuration/standalone.xml` добавить в блок `security-domains` следующий код, заменив `username` на имя пользователя для доступа к БД и `encrypted_password` на зашифрованный пароль, сформированный до этого:

```
<subsystem xmlns="urn:jboss:domain:security:2.0>
 <security-domains>
    ...
    <security-domain name="EncryptedPassword">
         <authentication>
            <login-module
code="org.picketbox.datasource.security.SecureIdentityLoginModule"
flag="required">
               <module-option name="username" value="username"/>
               <module-option name="password"
value="encrypted_password"/>
            </login-module>
         </authentication>
    </security-domain>
    ...
 <security-domains>
```

В файле `standalone/deployments/cdi-oracle-ds.xml` вместо

```
<user-name>username</user-name>
<password>password</password>
```

использовать

```
<security-domain>EncryptedPassword</security-domain>
```

4.2.3 Указание домена и IP-адреса в hosts

«Единый клиент» часто пытается идентифицировать машину, на которой разворачивается, с помощью вызова метода `java.net.InetAddress.getLocalHost`. Во избежание ошибок запуска при медленном ответе DNS-сервера нужно явно указать адрес и имя машины в hosts.

- Путь для Windows (может отличаться у разных версий): `C:\Windows\System32\Drivers\etc\hosts`
- Путь для Linux: `/etc/hosts`

Пример указания адреса и имени машины:

```
10.0.10.10 name.dev.intranet.host.ru #dev-name
```

4.2.4 Установка системы на Linux

4.2.4.1 Создание рабочих каталогов приложения

1. Создайте рабочий каталог EAS и дайте на него права пользователю `eas`:

```
mkdir -p /opt/eas
chown -R eas:eas /opt/eas
```

2. Создайте каталог, используемый при поиске дубликатов:

```
mkdir /opt/eas/dedup
```

3. Если вы используете отдельных пользователей для служб EAS и FACTOR, выдайте права на чтение и запись в каталог для дубликатов обоим пользователям.
   Пример, когда пользователи входят в одну группу с именем "hfl":

```
chgrp hfl /opt/eas/dedup
chmod 775 /opt/eas/dedup
```

4.2.4.2 Копирование исполняемых файлов

С релиза 20.16 изменился формат имени исполняемого файла, были добавлены дата и время сборки файла: `cdi-web-{customer}-{version}-SNAPSHOT-{data}__{time}-{revision}.war`

Скопируйте файл `cdi-web-{customer}-{version}.war` в каталог сервера приложений WildFly для EA: `/{path-to-WildFly-for-CDI}/standalone/deployments`

4.2.4.3 Настройка параметров запуска WildFly

В директории WildFly для EK настройте в файле `{path-to-wildfly-for-cdi}/bin/standalone.conf` параметры:

```
# EAS root dir
JAVA_OPTS="$JAVA_OPTS -Dcdi.root.folder={PATH_TO_ROOT_DIR} -
Dcdi.dedup.folder={PATH_TO_DEDUP_DIR}"
```

`PATH_TO_ROOT_DIR` — путь до рабочего каталога EAS. Обычно `/opt/eas`
`PATH_TO_DEDUP_DIR` — путь до каталога для дедупликации. Обычно `/opt/eas/dedup`

4.2.4.4 Создание рабочих каталогов приложения

1. Создайте рабочий каталог EAS и дайте на него права пользователю `eas`:

```
mkdir -p /opt/eas
chown -R eas:eas /opt/eas
```

2. Создайте каталог, используемый при поиске дубликатов:

```
mkdir /opt/eas/dedup
```

3. Если вы используете отдельных пользователей для служб EAS и FACTOR, выдайте права на чтение и запись в каталог для дубликатов обоим пользователям.
   Пример, когда пользователи входят в одну группу с именем "hfl":

```
chgrp hfl /opt/eas/dedup
chmod 775 /opt/eas/dedup
```

4.2.4.5 Копирование исполняемых файлов

С релиза 20.16 изменился формат имени исполняемого файла, были добавлены дата и время сборки файла: `cdi-web-{customer}-{version}-SNAPSHOT-{data}__{time}-{revision}.war`

Скопируйте файл `cdi-web-{customer}-{version}.war` в каталог сервера приложений WildFly для EA: `/{path-to-WildFly-for-CDI}/standalone/deployments`

4.2.4.6 Настройка параметров запуска WildFly

В директории WildFly для ЕК настройте в файле `{path-to-wildfly-for-cdi}/bin/standalone.conf` параметры:

```
# EAS root dir
JAVA_OPTS="$JAVA_OPTS -Dcdi.root.folder={PATH_TO_ROOT_DIR} -
Dcdi.dedup.folder={PATH_TO_DEDUP_DIR}"
```

`PATH_TO_ROOT_DIR` — путь до рабочего каталога EAS. Обычно `/opt/eas`
`PATH_TO_DEDUP_DIR` — путь до каталога для дедупликации. Обычно `/opt/eas/dedup`

4.2.5 Копирование исполняемых файлов

С релиза 20.16 изменился формат имени исполняемого файла, были добавлены дата и время сборки файла: `cdi-web-{customer}-{version}-SNAPSHOT-{data}__{time}-{revision}.war`

Скопируйте файл `cdi-web-{customer}-{version}.war` в каталог сервера приложений WildFly для EA: `/{path-to-WildFly-for-CDI}/standalone/deployments`

4.2.5.1 Настройка параметров запуска JBoss

В директории JBoss EA настройте в файле `bin/standalone.conf (Linux)` или в файле `bin\standalone.conf.bat (Windows)` следующие параметры:

```
:: EAS root dir
set "JAVA_OPTS=%JAVA_OPTS% -Dcdi.root.folder={PATH_TO_ROOT_DIR}"
```

`CDI_ROOT_DIR` - см раздел "дополнительный каталог" ниже

4.2.5.2 Дополнительные каталоги (Windows)

Создайте дополнительные каталоги, которые будут использоваться при работе системы:

```
mkdir C:\eas
```

Убедитесь, что у пользователя `HFL` есть полные права к этому каталогу. В случае отдельных пользователей для служб EAS и FACTOR нужно дать полный доступ пользователю EAS, и обеспечить доступ на чтение и запись к подкаталогу "\dedup" для пользователя FACTOR.

Пример: (под `%HFL%` имеется в виду имя единого пользователя, под которым будут работать ФАКТОР и Единый адрес).

```
icacls C:\eas /grant %HFL%:F
```

4.3 Настройка доступа к БД

4.3.1 Настройка доступа к БД

Отредактируйте настройки доступа к БД Единого адреса в файле `{path-to-wildfly-for-cdi}/standalone/deployments/cdi-oracle-ds.xml` директории WildFly EA:

- `connection-url`.
  для Oracle SID: `jdbc:oracle:thin:@{db-hostname}:{port}:{sid}`
  для `SERVICE NAME`: `jdbc:oracle:thin:@//{db-hostname}:{port}/{service-name}`
    - `{db-hostname}` — IP-адрес или доменное имя сервера БД.
    - `{port}` — порт, на котором слушает сервер БД (по умолчанию 1521).
    - `{sid}` — `SID` (системный идентификатор базы данных — имя БД) экземпляра БД.
    - `{service-name}` — имя используемого сервиса Oracle.
- `driver - oracle.jdbc.OracleDriver`
- `user-name` – имя пользователя для доступа системы к БД.
- `password` – пароль пользователя для доступа системы к БД.

Пример:

```
[...]
<connection-url>jdbc:oracle:thin:@{host}:{port}:{sid}</connection-url>
<driver>oracle.jdbc.OracleDriver</driver>
[...]
<security>
    <user-name>username</user-name>
    <password>password</password>
</security>
[...]
```

Пример файла:

cdi-oracle-ds.xml

Для первого автосоздания схемы БД используйте настройки из статьи — Автоматическое создание БД с нуля.

4.3.2 Настройка доступа к БД

Отредактируйте настройки доступа к БД Единого адреса в файле `{path-to-wildfly-for-cdi}/standalone/deployments/cdi-postgresql-ds.xml` директории WildFly EA:

- `connection-url`.
  для postgresql: jdbc:postgresql://{db-hostname}:{port}/{db-name}
    - `{db-hostname}` — IP-адрес или доменное имя сервера БД.
    - `{port}` — порт, на котором слушает сервер БД.

- {db-name} — имя используемой базы.

- driver - org.postgresql.Driver
- user-name – имя пользователя для доступа системы к БД.
- password – пароль пользователя для доступа системы к БД.

Пример:

```
[...]
 <datasource jndi-name="cdi-dataSource-test" pool-name="cdi-dataSource-
test" use-java-context="true" jta="false" spy="true">
        <connection-
url>jdbc:postgresql://192.168.1.1:11/test</connection-url>
        <driver>org.postgresql.Driver</driver>
[...]
<security>
    <user-name>username</user-name>
    <password>password</password>
</security>
[...]
```

cdi-postgresql-ds.xml - пример файла

Для первого автосоздания схемы БД используйте настройки из статьи — Автоматическое создание БД с нуля.

4.4 Инструкция для сервера Подсказок (Linux)

4.4.1 Установить приложение

```
su - factor
cd /opt/suggestions
wget https://fs.hflabs.ru/sgt-flight/wildfly/suggestions.zip
unzip suggestions.zip
```

4.4.2 Настроить сервис

Под пользователем root.

Подготовить конфигурацию для запуска Подсказок как сервиса:

```
mkdir /etc/suggestions
cp
/opt/suggestions/appserver/docs/contrib/scripts/systemd/suggestions.conf
/etc/suggestions/
cp
/opt/suggestions/appserver/docs/contrib/scripts/systemd/suggestions.servi
ce /etc/systemd/system/
cp /opt/suggestions/appserver/docs/contrib/scripts/systemd/launch.sh
/opt/suggestions/appserver/bin/
chmod +x /opt/suggestions/appserver/bin/launch.sh
```

Настроить автостарт при запуске ОС:

```
systemctl enable suggestions.service
```

4.4.3 Скачать сборку

```
su - factor
wget https://fs.hflabs.ru/sgt-flight/suggestions/build/20.10/suggestions-
web-20.10-SNAPSHOT.war -P
/opt/suggestions/appserver/standalone/deployments/
```

4.4.4 Установить лицензию

Скопировать лицензию (файл вида nnn_licence.sgt, предоставляет техническая поддержка HFLabs) в каталог `/opt/suggestions/configuration/`

4.4.5 Запустить приложение

Под пользователем root.

```
service suggestions start
```

4.5 Подключение обогащенных Подсказок

Из коробки обогащение Подсказок через Фактор не работает. Обратитесь в службу технической поддержки ХФЛабс, чтобы они настроили билды

4.5.1 Настройка подключения Фактора к подсказкам

1. В `standalone.conf` Фактора добавить параметр протухания кеша мэппингов фактора

```
# Параметр для обогащения Подсказок через Фактор
JAVA_OPTS="$JAVA_OPTS -Dfactor.mapping.cacheTimeout=1440"
```

2. В `standalone.conf` Подсказок добавить ссылку на сервис стандартизации (Фактор), указав значения `HOST` и `PORT`

```
# Параметр для обогащения Подсказок через Фактор
JAVA_OPTS="$JAVA_OPTS -Denrich.url=http://HOST:PORT/factor-service-
customer"
```

4.5.2 Как проверить, что подсказки обогащаются Фактором?

Введите адрес с квартирой.

Если подсказка есть — обогащение настроено и работает. Если нет — то увы.

Адрес

г Москва, Турчанинов пер, д 6 стр 2, кв 8

Выберите вариант или продолжите ввод

г Москва, Турчанинов пер, д 6 стр 2, кв 8
Хамовники р-н

Адрес одной строкой (полный)

г Москва, Хамовники р-н, Турчанинов пер, д 6 стр 2, кв 8

5 Запуск системы

5.1 Linux

5.1.1 Запуск системы ФАКТОР

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

```
$ service factor start
```

5.1.2 Остановка системы ФАКТОР

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

```
$ service factor stop
```

5.1.3 Запуск системы Единый адрес

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

```
$ service eas start
```

5.1.4 Остановка системы Единый адрес

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

```
$ service eas stop
```

5.1.5 Добавление службы в автозапуск

```
# chkconfig eas on && chkconfig factor on
```

5.1.6 Запуск и остановка в redhat 7

```
systemd start factor.service
systemd stop factor.service
systemd enable factor.service

-- Аналогичные:
systemctl start factor.service
```

```
systemctl stop factor.service
systemctl enable factor.service

-- Но и старые команды будут работать, сделав редирект на новые
service factor start
service factor stop
```

Просмотреть сообщения службы с момента запуска:

```
journalctl -u factor
```

Пример логов

```
[root@dev-touch bin]# journalctl -u factor
-- Logs begin at Fri 2017-10-06 10:29:54 MSK, end at Fri 2017-10-06
12:10:01 MSK. --
Oct 06 10:30:05 dev-touch systemd[1]: Started Factor WildFly Application
Server.
Oct 06 10:30:05 dev-touch systemd[1]: Starting Factor WildFly Application
Server...
Oct 06 10:30:05 dev-touch systemd[1]: factor.service: main process
exited, code=exited, status=203/EXEC
Oct 06 10:30:05 dev-touch systemd[1]: Unit factor.service entered failed
state.
Oct 06 10:30:05 dev-touch systemd[1]: factor.service failed.
Oct 06 10:31:30 dev-touch systemd[1]: Started Factor WildFly Application
Server.
Oct 06 10:31:30 dev-touch systemd[1]: Starting Factor WildFly Application
Server...
Oct 06 10:31:30 dev-touch systemd[1054]: Failed at step EXEC spawning
/opt/factor/wildfly-10.1.0.Final-18080/bin/launch.sh: Permission denied
Oct 06 10:31:30 dev-touch systemd[1]: factor.service: main process
exited, code=exited, status=203/EXEC
Oct 06 10:31:30 dev-touch systemd[1]: Unit factor.service entered failed
state.
Oct 06 10:31:30 dev-touch systemd[1]: factor.service failed.
Oct 06 10:31:43 dev-touch systemd[1]: Started Factor WildFly Application
Server.
Oct 06 10:31:43 dev-touch systemd[1]: Starting Factor WildFly Application
Server...
Oct 06 10:31:43 dev-touch systemd[1]: factor.service: main process
exited, code=exited, status=203/EXEC
Oct 06 10:31:43 dev-touch systemd[1]: Unit factor.service entered failed
state.
Oct 06 10:31:43 dev-touch systemd[1]: factor.service failed.
Oct 06 10:36:46 dev-touch systemd[1]: Started Factor WildFly Application
Server.
Oct 06 10:36:46 dev-touch systemd[1]: Starting Factor WildFly Application
Server...
```

5.2 Windows

5.2.1 Запуск системы ФАКТОР

```
net start factor
```

5.2.2 Остановка системы ФАКТОР

```
net stop factor
```

5.2.3 Запуск системы Единый адрес

```
net start eas
```

5.2.4 Остановка системы Единый адрес

```
net stop eas
```

6 Дополнительные шаги

6.1 Подключение экспорта через JMS

Для того, чтобы Единый адрес экспортировал любые изменения контрагентов по протоколу JMS во внешнюю очередь сообщений, следует выполнить нижеперечисленные шаги.

6.1.1 Настройка JBoss

1. Активировать подсистему обмена сообщениями JBoss.
2. В файле `standalone/configuration/standalone.xml` директории JBoss EA добавить очередь сообщений `cdi.event` в раздел `jms-destinations`:

```
<subsystem xmlns="urn:jboss:domain:messaging-activemq:1.0">
    <server name="default">
        [...]
        <jms-queue name="cdi.event"
entries="java:jboss/exported/queue/cdi/event queue/cdi/event"/>
    </server>
</subsystem>
```

6.1.2 Создание пользователя

Вызвать из директории JBoss EA файл `bin/add_user.bat` и пройти следующие шаги:

1. Выбор типа пользователя: `Application User (b)`
2. Выбор прав: `ApplicationRealm`
3. Username: event_client
4. Password: указать пароль
5. Role: `guest`
6. Correct: `yes`

6.1.3 Подключение внешних слушателей очереди

Для того, чтобы получать сообщения из очереди по протоколу JMS, следует использовать следующие параметры:

- Имя сервера: {`доменное имя сервера приложений Единого клиента`}.
- Порт: `8080`
- Фабрика: `jms/RemoteConnectionFactory`
- Имя очереди: `queue/cdi/event`
- Имя пользователя: `event_client`

6.2 Синхронизация между экземплярами EA (настройка горячего резерва)

6.2.1 Настройка Wildfly 16

Для каждого экземпляра EA в файле `standalone/configuration/standalone.xml` директории JBoss EA выполнить настройки:

1. Активировать подсистему обмена сообщениями JBoss
2. Внести изменения в раздел `messaging-activemq`:

```
<subsystem xmlns="urn:jboss:domain:messaging-activemq:1.0">
    <server name="default">
        [...]
     <http-connector name="node-sync" socket-binding="node-sync-
binding" endpoint="http-acceptor">
                <param name="nioRemotingThreads" value="8"/>
     </http-connector>
     <jms-queue name="cdi.nodeSync"
entries="java:jboss/exported/queue/cdi/nodeSync
queue/cdi/nodeSync"/>
     <connection-factory name="NodeSyncRemoteConnectionFactory"
connectors="node-sync"
entries="java:/nodeSyncRemoteConnectionFactory" use-global-
pools="false" thread-pool-max-size="8"/>
    </server>
</subsystem>
```

3. Внести изменения в раздел `socket-binding-group`:

```
<socket-binding-group name="standard-sockets" default-
interface="public" port-offset="${jboss.socket.binding.port-
offset:0}">
     [...]
     <outbound-socket-binding name="node-sync-binding">
         <remote-destination host="{доменное имя второго экземпляра
EK}" port="{http порт второго экземпляра EK}"/>
     </outbound-socket-binding>
</socket-binding-group>
```

Примечание: в параметре `port` элемента `remote-destination` нужно учитывать смещение порта на втором экземпляре. Например если на втором экземпляре указано

```
    <!-- конфигурация "второго" экземпляра -->
    <socket-binding-group name="standard-sockets" default-
interface="public" port-offset="${jboss.socket.binding.port-
offset:0}">
        <socket-binding name="http"
port="${jboss.http.port:8080}"/>
    </socket-binding-group>
```

и при этом он запускается со смещением т. е. запускается с параметром напр. `-Djboss.socket.binding.port-offset=8`, то для текущего экземпляра он будет доступен как:

```
        <!-- конфигурация "первого" экземпляра -->
        <outbound-socket-binding name="node-sync-binding">
            <remote-destination host="{доменное имя второго экземпляра
   ЕК}" port="8088"/>
        </outbound-socket-binding>
```

4. Включить поддержку синхронизации между экземплярами системы на уровне приложения (делается сотрудниками ХФЛабс)
5. Настроить запуск периодических задач (делается сотрудниками ХФЛабс)

6.2.2 Пользователь sync

Для работы с очередью синхронизации система использует пользователя `sync` (пароль `cdi`, роль `guest`). Он уже входит в сборку JBoss EA.

6.2.3 Синхронизация системного времени

Системное время на обоих экземплярах ЕА должно быть синхронизировано с минимальной погрешностью.

Для этого нужно развернуть локальный NTP сервер и настроить синхронизацию с ним раз в час для каждого экземпляра ЕА.

6.2.4 Активация подсистемы обмена сообщениями в Wildfly 16

Все настройки выполняются в файле `standalone/configuration/standalone.xml` директории JBoss EA и одинаковы для обоих JBoss-ов, если они находятся на разных машинах

6.2.4.1 Добавить в блок extensions модуль messaging

```
<extensions>
 [...]
 <extension module="org.wildfly.extension.messaging-activemq"/>
</extensions>
```

6.2.4.2 Добавить приведенный ниже код в блок profile

```
<profile>
    [...]
    <subsystem xmlns="urn:jboss:domain:messaging-activemq:1.0">
            <server name="default" thread-pool-max-size="16">
                <security-setting name="#">
                    <role name="guest" send="true" consume="true" create-
non-durable-queue="true" delete-non-durable-queue="true"/>
                </security-setting>
                <address-setting name="#" dead-letter-
address="jms.queue.DLQ" expiry-address="jms.queue.ExpiryQueue" max-size-
bytes="10485760" page-size-bytes="2097152" message-counter-history-day-
limit="10"/>
                <http-connector name="http-connector" socket-
binding="http" endpoint="http-acceptor">
                        <param name="nioRemotingThreads" value="8"/>
                 </http-connector>
                <in-vm-connector name="in-vm" server-id="0"/>
                <http-acceptor name="http-acceptor" http-
listener="default"/>
                <in-vm-acceptor name="in-vm" server-id="0"/>
```

```
                <jms-queue name="ExpiryQueue"
entries="java:/jms/queue/ExpiryQueue"/>
                <jms-queue name="DLQ" entries="java:/jms/queue/DLQ"/>
                <connection-factory name="InVmConnectionFactory"
entries="java:/jmsConnectionFactory" connectors="in-vm" use-global-
pools="false" thread-pool-max-size="8"/>
            </server>
        </subsystem>
</profile>
```

6.2.5 Создание пользователя

При необходимости создать нового пользователя (или изменить пароль старого) нужно вызвать из директории JBoss файл `bin/add_user.bat ()` и пройти следующие шаги:

1. Выбор типа пользователя: `Application User (b)`
2. Выбор прав: `ApplicationRealm (`Если оно выбрано по-умолчанию, просто нажать `Enter)`
3. Username: <имя_пользователя>
4. Password: `<пароль_пользователя>`
5. Role: `<роль_пользователя>`
6. Correct: `yes`

6.3 Настройка SSL (https) в Wildfly

6.3.1 Настройка сервера приложений

В `standalone/configuration/standalone.xml` директории JBoss EA описать `HttpsSecuredRealm`, использующий предоставленные ключи:

Code Block 12 standalone.xml

```
<management>
    <security-realms>
    ...
        <security-realm name="HttpsSecuredRealm">
            <server-identities>
                <ssl>
                    <keystore path="keystore.jks" relative-
to="jboss.server.config.dir" keystore-password="qwerty"
alias="selfsigned"/>
                </ssl>
            </server-identities>
        </security-realm>
    </security-realms>
</management>
```

И добавить `https`-коннектор, использующий этот `HttpsSecuredRealm`:

Code Block 13 standalone.xml

```
<subsystem xmlns="urn:jboss:domain:undertow:3.1">
    <buffer-cache name="default"/>
    <server name="default-server">
```

```
        <http-listener name="default" socket-binding="http"/>
        <https-listener name="https" socket-binding="https" security-
realm="HttpsSecuredRealm"/>
        ...
    </server>
    ...
</subsystem>
```

6.3.2 Описание параметров HttpsSecuredRealm

- `keystore.path` — путь к хранилищу ключей, корневая директория определяется параметром `relative.to`;
- `alias` — алиас, под которым ключи доступны в хранилище;
- `keystore-password` — пароль к хранилищу;
- `key-password` — пароль к ключам (если не указан, используется `keystore-password`).

6.3.3 Настройка приложения

Для корректной работы CDM и автоматического перенаправления запроса к http://cdi.domain:8080/cdi на защищенный адрес https://cdi.domain:8443/cdi модифицировать корневой `pom.xml` заказчика:

Code Block 14 standalone.xml

```
<!-- CDM -->
<cdm.server.protocol>https</cdm.server.protocol>
<cdm.server.port>8443</cdm.server.port>

<!-- Redirect -->
<securityConstraints.transportGuarantee>${securityConstraints.transportGu
arantee.confidential}</securityConstraints.transportGuarantee>
```

6.3.4 Где же взять хранилище ключей?

Запросить у заказчика, конечно же.

Ключи могут быть переданы в виде:

- `jks` — Java Key Store. Лучший вариант, для настройки потребуется только скопировать файл на сервер и указать реквизиты доступа к нему.
- `p12` — PKCS#12. Стандартное хранилище цепочки сертификатов и закрытого ключа. Из него легко генерируется jks.
- `cer, p7b, key` — Закрытый и открытый ключи в виде отдельных файлов. Из них можно сгенерировать p12-хранилище.

Просить стоит PKCS#12 хранилище, готовый jks обычно ни у кого не хранится. Если с PKCS#12 возникают трудности, нужно запросить отдельные файлы для закрытого и открытого ключа.

6.3.5 Генерация jks-файла

Выполняется при помощи утилиты keytool, входящей в поставку JRE. Первая команда формирует jks-файл, вторая меняет пароль от конкретной записи таким образом, чтобы он совпадал с паролем хранилища.

```
keytool -importkeystore -destkeystore cdi.jks -srckeystore cdi.p12 -
srcstoretype pkcs12 -alias cdi.domain -storepass qwerty
keytool -keypasswd -keystore cdi.jks -storepass qwerty -alias cdi.domain
-new qwerty
```

6.3.6 Генерация p12-файла

Скачать утилиту для работы с ключами — например, XCA. Создать базу данных, импортировать в неё p7b (цепочку публичных сертификатов) и key (приватный ключ), экспортировать хранилище в формате PKSC12 with Certificate chain.

6.4 Подключение CORS

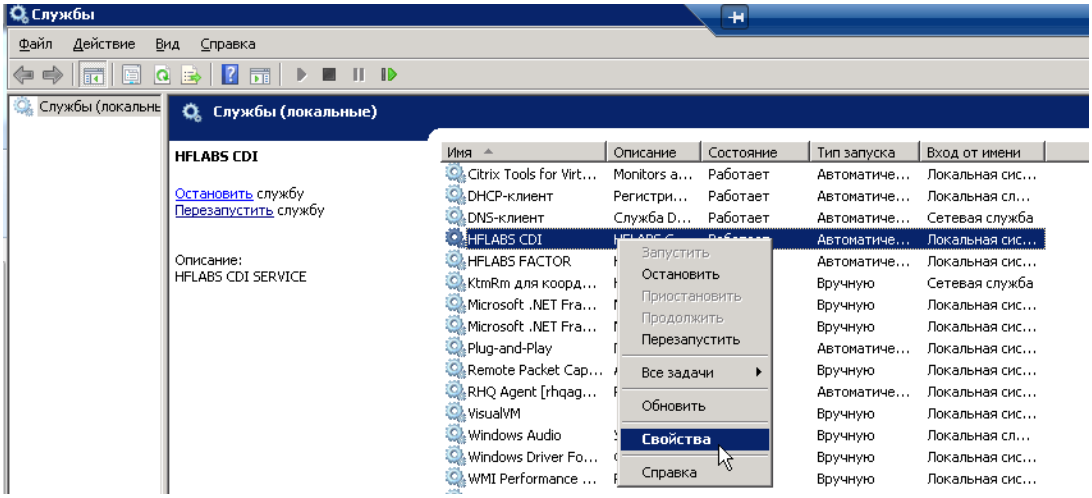
Cross-origin resource sharing (CORS) — технология современных браузеров, которая позволяет предоставить веб-странице доступ к ресурсам другого домена.

Для добавления CORS-заголовков достаточно немного модифицировать `standalone.xml` — в блок `filters` скопировать приведенные строки `response-header`, в блок `server` — ссылки на них.

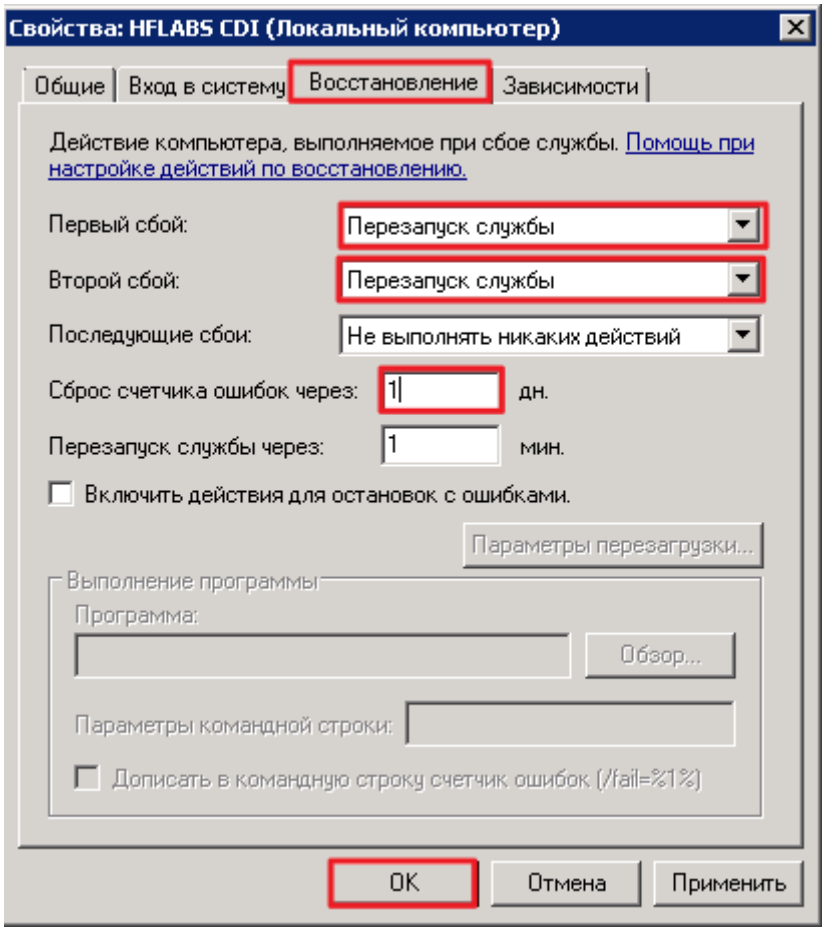
```
        <subsystem xmlns="urn:jboss:domain:undertow:1.2">
            <buffer-cache name="default"/>
            <server name="default-server">
                <http-listener name="default" socket-binding="http"/>
                <host name="default-host" alias="localhost">
                    ...
                    <filter-ref name="cors-origin"/>
                    <filter-ref name="cors-methods"/>
                    <filter-ref name="cors-headers"/>
                </host>
            </server>
            <filters>
                ...
                <response-header name="cors-origin" header-name="Access-
Control-Allow-Origin" header-value="*"/>
                <response-header name="cors-methods" header-name="Access-
Control-Allow-Methods" header-value="OPTIONS, GET, POST, PUT, DELETE"/>
                <response-header name="cors-headers" header-name="Access-
Control-Allow-Headers" header-value="origin, content-type, accept,
authorization, access-control-allow-origin, access-control-allow-methods,
access-control-allow-headers, allow, content-length, date, last-modified,
if-modified-since"/>
            </filters>
        </subsystem>
```

6.5 Настройка перезапуска серверов приложений в ОС Windows

1. Открыть «Службы» и найти службу «HFLABS CDI» или «HFLABS EAS».
2. Вызвать на службе контекстное меню по правой кнопке мыши и выбрать "Свойства":



3. Открыть вкладку "Восстановление" (Recovery) и задать следующие параметры:
   a. Перезапуск службы в случае первых двух сбоев.
   b. Сброс счетчика ошибок через 1 день.



4. Повторить шаги для службы "HFLABS FACTOR".

6.6 Использование LDAPS с самоподписанным сертификатом

Требования ИБ могут подразумевать взаимодействие с ActiveDirectory по безопасному протоколу — LDAPS. Spring-security чудесно работает с LDAP over SSL, в интерфейсе администратора достаточно заменить протокол и порт доступа:
`ldap://domain.com:383 → ldaps://domain.com:3689`

Но чаще всего ключ шифрования является самоподписанным, поэтому нужно убедить EAS в том, что такому ключу можно доверять.

6.6.1 Выгрузка публичного ключа

В получении публичного ключа поможет утилита openssl, которая входит во все стандартные дистрибутивы unix-систем. Для Win-серверов дистрибутив openssl доступен на сайте gnuwin32.

Ключ можно получить такой командой (вместо host и port подставить соответствующие значения сервера LDAP):

Code Block 15 Запрос для получения ключа

```
echo "" | openssl s_client -showcerts -connect host:port -prexit
2>/dev/null | sed -n -e '/BEGIN\ CERTIFICATE/,/END\ CERTIFICATE/ p' >
ldaps.cert
```

Сформированный файл будет выглядеть следующим образом:

```
-----BEGIN CERTIFICATE-----
QI9GWDCCBECgAwIBAgIQC5cxE68zwsnRDfWE1f0TIzANBgkqhkiG9w0BAQwFADCB
...
p2w31Ff+gA5JQwKaRcbkEMlsxXaxqwLOyv7YhHbEAW0DscFfuFTsb02wGps=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
QI9ENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
...
p2w31Ff+gA5JQwKaRcbkEMlsxXaxqwLOyv7YhHbEAW0DscFfuFTsb02wGps=
-----END CERTIFICATE-----
```

6.6.2 Формирование jks-хранилища

Полученный cer-файл надо превратить в jks, понятный java-приложениям, попутно указав пароль для хранилища:

Code Block 16 Создание jks

```
keytool -import -alias ldaps -file ldaps.cert -keystore ldaps.jks
```

6.6.3 Настройка wildfly

Осталось указать в `standalone.conf` или `standalone.conf.bat` ссылку на созданный jks, задав две переменных:

```
-Djavax.net.ssl.trustStore=path/to/ldaps.jks -
Djavax.net.ssl.trustStorePassword=password
```

6.7 Шифрование паролей

6.7.1 Актуализация пароля к AD и почтовому серверу

Для замены пароля к AD и почтовому серверу необходимо выполнить следующие шаги:

1. Сгенерировать новый зашифрованный пароль с помощью приложенного jar - файла. Выполнить следующую команду из директории JBoss EA:

   ```
   java -cp utils-crypto-1.7.8-SNAPSHOT.jar
   ru.hflabs.crypto.cipher.EncodeRunner пароль_для_шифрования
   ```

2. Для замены пароля к почтовому серверу в АРМ Администратора зайдите на вкладку *Конфигурация,* раздел *Параметры отправки email*.
   Установите параметр `mail.password` равным новому зашифрованному паролю:

   `mail.password = зашифрованный_пароль`

3. Для замены пароля к AD в АРМ Администратора зайдите на вкладку *Конфигурация,* раздел *Параметры LDAP.*
   Установите параметр `ldap.password` равным новому зашифрованному паролю:

   `ldap.password = зашифрованный_пароль`

6.7.2 Шифрование пароля к AD и почтовому серверу

1. Для шифрования пароля к AD в директории заказчика `cdi-security/src/main/resources` разместить файл `security-ldap.xml`:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <beans xmlns="http://www.springframework.org/schema/beans"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

   xsi:schemaLocation="http://www.springframework.org/schema/beans
   http://www.springframework.org/schema/beans/spring-beans.xsd">

       <!-- Пароль к ldap хранится в шифрованном виде -->
       <bean id="ldap.password.custom"
   class="ru.hflabs.cdi.util.PasswordEncodeUtil" factory-
   method="decodePassword">
           <constructor-arg value="$security.ldap{ldap.password}"/>
       </bean>

   </beans>
   ```

2. Для шифрования пароля к почтовому серверу в директории заказчика `cdi-services/src/main/resources` разместить файл `services-mail.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd">

    <!-- Пароль к mail хранится в шифрованном виде -->
    <bean id="mail.password.custom"
class="ru.hflabs.cdi.util.PasswordEncodeUtil" factory-
method="decodePassword">
        <constructor-arg value="$mail{mail.password}"/>
    </bean>

</beans>
```

3. Сгенерировать зашифрованный пароль с помощью приложенного jar - файла. Выполнить следующую команду из директории JBoss EA:

```
java -cp utils-crypto-1.7.8-SNAPSHOT.jar
ru.hflabs.crypto.cipher.EncodeRunner пароль_для_шифрования
```

4. В файл `pom.xml` добавить в блок `properties` следующий код:

```
<mail.password>зашифрованный_пароль</mail.password>
```

```
<!-- Настройки соединения с LDAP сервером -->
<ldap.password>зашифрованный_пароль</ldap.password>
```

6.7.3 Настройка datasource для заказчиков, использующих шифрованный пароль к БД

Для шифрования пароля выполнить в командной строке следующую команду из директории JBoss EA:

6.7.3.1 Windows

```
java -cp .\modules\system\layers\base\org\picketbox\main\picketbox-
5.0.3.Final.jar
org.picketbox.datasource.security.SecureIdentityLoginModule
пароль_для_шифрования
```

6.7.3.2 Linux

```
java -cp ./modules/system/layers/base/org/picketbox/main/picketbox-
5.0.3.Final.jar
org.picketbox.datasource.security.SecureIdentityLoginModule
пароль_для_шифрования
```

```
```

Результатом выполнения команды будет зашифрованный пароль.

В файле `standalone/configuration/standalone.xml` добавить в блок `security-domains` следующий код, заменив `username` на имя пользователя для доступа к БД и `encrypted_password` на зашифрованный пароль, сформированный до этого:

```
<subsystem xmlns="urn:jboss:domain:security:2.0>
 <security-domains>
    ...
    <security-domain name="EncryptedPassword">
         <authentication>
            <login-module
code="org.picketbox.datasource.security.SecureIdentityLoginModule"
flag="required">
               <module-option name="username" value="username"/>
               <module-option name="password"
value="encrypted_password"/>
            </login-module>
         </authentication>
    </security-domain>
    ...
 <security-domains>
```

В файле `standalone/deployments/cdi-oracle-ds.xml` вместо

```
<user-name>username</user-name>
<password>password</password>
```

использовать

```
<security-domain>EncryptedPassword</security-domain>
```

6.8 Настройка взаимодействия с Microsoft Exchange

Если у Заказчика используются почтовый сервер Microsoft Exchange, то необходимо чуть подкрутить настройки EA. Поля, которые нужно заполнить, даны в <> с пояснениями в скобках.

6.8.1 Выгрузка публичного ключа

В получении публичного ключа поможет утилита openssl, которая входит во все стандартные дистрибутивы unix-систем. Для Win-серверов дистрибутив openssl доступен на сайте gnuwin32.

Ключ можно получить такой командой:

Code Block 17 Запрос для получения ключа

```
openssl s_client -showcerts -smarttls smtp -connect
<customer_host>:<port(по умолчанию 25)> > cert.txt
```

Сформированный файл будет выглядеть следующим образом:

```
-----BEGIN CERTIFICATE-----
QI9GWDCCBECgAwIBAgIQC5cxE68zwsnRDfWE1f0TIzANBgkqhkiG9w0BAQwFADCB
...
p2w31Ff+gA5JQwKaRcbkEMlsxXaxqwLOyv7YhHbEAW0DscFfuFTsb02wGps=
-----END CERTIFICATE-----
 3 s:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust
External CA Root
   i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust
External CA Root
-----BEGIN CERTIFICATE-----
QI9ENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
...
p2w31Ff+gA5JQwKaRcbkEMlsxXaxqwLOyv7YhHbEAW0DscFfuFTsb02wGps=
-----END CERTIFICATE-----
```

Создать текстовый файл `smtp.cer` и скопировать в него все блоки с сертификатами, исключив текст, находящийся между блоками -----END CERTIFICATE----- и -----BEGIN CERTIFICATE-----. Получится так:

```
-----BEGIN CERTIFICATE-----
QI9GWDCCBECgAwIBAgIQC5cxE68zwsnRDfWE1f0TIzANBgkqhkiG9w0BAQwFADCB
...
p2w31Ff+gA5JQwKaRcbkEMlsxXaxqwLOyv7YhHbEAW0DscFfuFTsb02wGps=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
QI9ENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU
...
p2w31Ff+gA5JQwKaRcbkEMlsxXaxqwLOyv7YhHbEAW0DscFfuFTsb02wGps=
-----END CERTIFICATE-----
```

6.8.2 Формирование jks-хранилища

Полученный cer-файл надо превратить в jks, понятный java-приложениям, попутно указав пароль для хранилища:

Code Block 18 Создание jks

```
keytool -import -alias smtp -file smtp.cer -keystore smtp.jks
```

6.8.3 Настройка wildfly

Указать в `standalone.conf` или `standalone.conf.bat` ссылку на созданный jks, задав две переменных и два параметра для почты:

```
-Djavax.net.ssl.trustStore=<path/to/smtp.jks>
-Djavax.net.ssl.trustStorePassword=password
-Dmail.smtp.ssl.trust=<host>
-Dmail.smtp.starttls.enable=true
```

6.8.4 Настройка EA

В веб-интерфейсе в конфигурации, pom или БД указать свойство:

```
mail.protocol = smtp
```

7 Проверка доступности системы

Для мониторинга доступности используется URL
`http://{hostname}:{port}/cdi/api/manage/health:`

- не создает ненужных сессий в таблице SPRING_SESSION и не идет через фильтры авторизации, максимально легкий;
- есть проверка доступности БД (`dbHealthIndicator`);
- есть проверка доступности Фактора (`factorHealthIndicator`).

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.