H F Labs

Руководство по развертыванию

Документация Единого клиента

17 дек 2019

Оглавление

1 Подготовка к развертыванию

1.1 Методика расчета требований к аппаратному обеспечению

Внутренняя страница. Недоступна пользователям извне. Для отправки требований используйте готовые конфигурации в зависимости от числа записей.

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

Требования к процессору

Сервер приложений:

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

Сервер СУБД:

- Минимально Intel(R) Xeon(R) Silver 4114 или выше
- 1 – 10 млн исходных клиентских записей: 10 ядер на сервер.
- более 10 млн исходных клиентских 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 клиентских записей: 32 Гб.
- 5 — 10 млн исходных клиентских записей: 64 Гб
- более 10 млн. исходных клиентских записей: 64 Гб + 0.5*число записей (в млн) + 0.1*число связей (в млн).

СУБД:

- 1 – 10 млн. исходных клиентских записей: 32 Гб.
- более 10 млн. исходных клиентских записей: 48 Гб
- более 30 млн исходных клиентских записей: 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 контрагентов.
Пример: для 20 млн контрагентов 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 клиентских записей.

1.1.3 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 клиента».

1.1.4 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 клиента».

1.1.5 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.

1.1.6 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.

1.1.7 Сервер балансировки (при наличии в отказоустойчивой конфигурации)

1. Имя сервера и его ip-адрес.

1.2 Требования к аппаратной платформе

> В данном разделе представлены *минимальные* системные требования

Минимальная конфигурация состоит из сервера ЕК, 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 ЕК и сервер Standby для СУБД, по конфигурации равнозначный основному серверу.

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

1.2.1 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 ЕК в отказоустойчивой конфигурации;
4. сервером Подсказок и сервером приложений ЕК;
5. сервером приложений ЕК и серверами приложения для очистки данных.

Требования к пропускной способности каналов между компонентами:

Компонент 1	Компонент 2	Ширина канала
Рабочая станция HFLabs	Сервер приложений ЕК	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 ЕК	Сервер СУБД	1 Гбит/с

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

1.2.2 Сервера ЕК и СУБД до 1 млн записей

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

1.2.2.1 Сервер приложений ЕК

Параметр	Требование
Процессор	Intel(R) Xeon(R) Silver 4114 и выше, 8 ядер
Оперативная память	24 Гб
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 10.0.1
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.2.2.2 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
Операционная система	• **Рекомендуем**: CentOS 6+ или Red Hat Enterprise Linux 6+, x64. • Поддерживаем: Windows 2008 Enterprise Edition и выше, x64.
СУБД	На выбор: • Oracle Database 12c Standard Edition. • PostgreSQL 11 версии
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.2.3 Сервера ЕК и СУБД от 1 до 10 млн исходных записей

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

1.2.3.1 Сервер приложений ЕК

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.

Параметр	Требование
	• 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 10.0.1
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.2.3.2 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
Операционная система	• **Рекомендуем**: CentOS 7+ или Red Hat Enterprise Linux 7+, x64. • Поддерживаем: Windows 2008 Enterprise Edition и выше, x64.
СУБД	На выбор: • Oracle Database 12c Standard Edition. • PostgreSQL 11 версии
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.2.4 Сервера ЕК и СУБД от 10 до 50 млн исходных записей

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

1.2.4.1 Сервер приложений ЕК

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 10.0.1
Виртуальная среда	Нежелательна, рекомендуем аппаратную платформу.
Прочие требования	Запрещена установка антивируса

1.2.4.2 Сервер СУБД

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

Параметр	Требование
	• Минимум 10 000 TBW Поддерживаем: SAS 15K (аппаратный RAID 10)
Сетевая карта	1 Гбит
Операционная система	• **Рекомендуем**: CentOS 6+ или Red Hat Enterprise Linux 6+, x64. • Поддерживаем: Windows 2008 Enterprise Edition и выше, x64.
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

1.2.5 Сервера ЕК и СУБД более 50 млн исходных записей

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

1.2.5.1 Сервер приложений ЕК

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
Сетевая карта	1 Гбит

Параметр	Требование
Операционная система	CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
Java	Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.
Сервер приложений	Wildfly 10.0.1
Виртуальная среда	Не допускается, только аппаратная платформа

1.2.5.2 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
Операционная система	CentOS 7+ или Red Hat Enterprise Linux 7+, x64
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

1.2.6 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+

1.2.7 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
Операционная система	• Red Hat Enterprise Linux 7+ • CentOS 7+
Разрядность ОС	64-bit

1.2.8 Сервер Подсказок с выделенным Фактором

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

1.2.8.1 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
Операционная система	• Red Hat Enterprise Linux 7+ • CentOS 7+

Параметр	Требование

1.2.9 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 10.0.1
Виртуальная среда	Допускается

1.2.10 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 ЕК в отказоустойчивой конфигурации;
4. сервером Подсказок и сервером приложений ЕК;
5. сервером приложений ЕК и серверами приложения для очистки данных.

Требования к пропускной способности каналов между компонентами:

Компонент 1	Компонент 2	Ширина канала
Рабочая станция HFLabs	Сервер приложений ЕК	100 Мбит/с
Рабочая станция HFLabs	Сервер СУБД	100 Мбит/с

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

1.3 Требования к настройке программно-аппаратной платформы

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

1.3.1 Настройка рабочей станция для HFLabs

1.3.1.1 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.

1.3.1.2 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 ЕК по портам:
    - 22 (ssh) или 3889 (RDP);
    - 8080 (HTTP-порт «Единого клиента»);
    - 18080 (HTTP-порт «Фактора»);
    - 9990 (порт для мониторинга «Единого клиента»);

   - 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»).

1.3.2 Настройка сервера приложений ЕК (ОС *nix)

1.3.2.1 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

1.3.2.2 Установка и настройка

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

   Пользователи объединены в одну группу — hfl_cdi.
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 (OpenJDK) 11 с последними обновлениями.

1.3.2.3 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 клиента»);
- 18080 (HTTP-порт «Фактора»);
- 9990 (порт для мониторинга «Единого клиента»);
- 19990 (порт для мониторинга «Фактора»).

6. Установка антивируса запрещена.

1.3.3 Настройка сервера приложений ЕК для ОС Windows

1.3.3.1 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

1.3.3.2 Установка и настройка

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

1.3.3.3 Доступы и права

1. Открыт доступ к серверу СУБД по порту, на котором слушает Oracle (1521) или MariaDB (3306).
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 клиента»)
   - 18080 (HTTP-порт «Фактора»)
   - 9990 (порт для мониторинга «Единого клиента»)
   - 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 клиента» и «Фактора».

1.3.4 Настройка сервера СУБД Oracle

1.3.4.1 Версия ОС и конфигурация Oracle

- **Рекомендуем**: CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Поддерживаем: Windows 2008 Enterprise Edition и выше, x64.

- Минимально достаточно: Oracle Database 11g Standard Edition. Версию 12C поддерживаем.
- Рекомендуемый вариант для базы с количеством исходных клиентских записей более 10 млн: Oracle Database 11g Enterprise Edition с включенной опцией Oracle Partitioning.
- Если требуется организация архитектуры с высокой доступностью: Oracle Database 11g Enterprise Edition с включенными опциями Oracle Active Data Guard или Oracle RAC (в зависимости от выбранного способа резервирования).

1.3.4.2 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).

1.3.4.3 Доступы и права

1. Открыт и прослушивается порт 1521 (или другой порт, используемый Oracle — его можно уточнить у администратора СУБД).
2. В БД созданы табличные пространства и пользователь для «Единого клиента». Для создания можно использовать скрипт `schema_oracle_cdi_create_user.sql`, либо вручную создать:

-
    - Табличное пространство `cdi` для таблиц Единого клиента

```
CREATE TABLESPACE cdi DATAFILE 'cdi_01.dat' SIZE 1000
M REUSE AUTOEXTEND ON NEXT 500 M;
```

-
    - Табличное пространство `cdi_idx` для индексов

```
CREATE SMALLFILE TABLESPACE cdi_idx DATAFILE
'cdi_idx_01.dat' SIZE 500 M REUSE AUTOEXTEND ON NEXT
250 M;
```

    - Пользователь `cdi` с табличным пространством по умолчанию `CDI` и правами:

```
CREATE MATERIALIZED VIEW
CREATE PROCEDURE
CREATE SEQUENCE
CREATE SESSION
CREATE SYNONYM
CREATE TABLE
CREATE TRIGGER
CREATE VIEW
EXECUTE ON dbms_lock
SELECT ANY DICTIONARY
QUOTA UNLIMITED ON CDI
QUOTA UNLIMITED ON CDI_idx
```

1.3.5 Настройка сервера СУБД MariaDB

1.3.5.1 Версия ОС и конфигурация Oracle

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- MySQL MariaDB версии 10.1 или выше

1.3.5.2 Установка и настройка

1. Создан пользователь cdi_user с правами на sudo, под которым будут работать специалисты HFLabs для установки и настройки СУБД.
2. Активирована служба ssh.

1.3.5.3 Доступы и права

- Открыт и прослушивается порт 3306.
- Открыт порт 22 (ssh).

1.3.5.4 Настройка MariaDB внутренняя

Внутренняя страница для настройки MariaDB силами специалистами HFLabs. Не видна Заказчикам.

Конфигурация приведена для версии >= 10.1 (пример конфигурации для версии 10.3 можно глянуть на настройках egrdb.)

По умолчанию директория с данными живет в */var/lib/mysql* , где достаточно мало места. Нужно создать директорию на другом диске и сделать symlink */var/lib/mysql* → */path/to/data/dir* (содержимое mysql, естественно, предварительно перенести в новую директорию)

```
# MariaDB-specific config file.
# Read by /etc/mysql/my.cnf

[mysqld]
bind-address        = 0.0.0.0

max_connections        = 200
max_allowed_packet     = 1G

lower_case_table_names= 1

wait_timeout        = 28800
net_read_timeout    = 28800
net_write_timeout      = 28800
net_buffer_length      = 65536

table_open_cache    = 256

thread_cache_size      = 32
query_cache_limit      = 2M

sort_buffer_size    = 8M
read_rnd_buffer_size   = 16M
max_heap_table_size    = 512M
tmp_table_size      = 512M

binlog_cache_size      = 16M
binlog_format       = MIXED
skip-log-bin

# SQL modes
sql_mode                = NO_ENGINE_SUBSTITUTION
```

```
# *** Tmp
tmpdir           = /path/to/data/dir/tmp
slave_load_tmpdir     = /path/to/data/dir/tmp

# *** Logs
general_log_file    = /var/log/mysql/mysql-general.log
general_log         = 0
log-error           = /var/log/mysql/mysql.log
log_warnings        = 1
slow_query_log      = 0
slow_query_log_file    = /var/log/mysql/mariadb-slow.log
long_query_time       = 10

# *** MyISAM Specific options
bulk_insert_buffer_size  = 64M
key_buffer_size       = 32M
myisam_sort_buffer_size  = 128M

# *** INNODB Specific options, начиная с 10.3 innodb_file_format_max и
innodb_file_format не используются
innodb_file_format_max= Barracuda
innodb_file_format    = Barracuda
innodb_strict_mode    = 1

innodb_buffer_pool_instances  = 12
innodb_buffer_pool_size       = 24G
innodb_rollback_on_timeout    = 1

innodb_flush_log_at_trx_commit   = 2
innodb_flush_method         = O_DIRECT

innodb_log_buffer_size   = 256M
innodb_log_file_size     = 512M
innodb_log_files_in_group   = 4

innodb_thread_concurrency   = 32
innodb_read_io_threads   = 32
innodb_write_io_threads     = 32


innodb_lru_scan_depth       = 256
```

1.3.5.4.1 Галера

```
[galera]
wsrep_on=ON
wsrep_provider=/usr/lib64/galera/libgalera_smm.so
wsrep_cluster_address=gcomm://host1,host2?pc.wait_prim=no&pc.bootstrap=tr
ue
wsrep_provider_options="evs.keepalive_period = PT5S;evs.suspect_timeout =
PT30S;evs.install_timeout= PT45S;evs.inactive_timeout = PT1M"
binlog_format=row
default_storage_engine=InnoDB
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0
```

1.3.5.5 Обновление mariadb 10.1 - 10.3

Инструкция по обновлению:

1. Обновить марию до последней версии установленного релиза, убедиться, что все работает.
2. Тушим сервер, меняем репозиторий на 10.3
3. Закомментить строчки

```
#innodb_file_format_max = Barracuda
#innodb_file_format = Barracuda
```

4. Обновляем марию, если ошибка при обновлении — грохаем юниты `systemd`, выставляем права на бд. Проверить в юните `systemd` от какого пользователя идет запуск бд, по умолчанию обычно `mysql`.
5. Запустить марию 10.3, проверить лог, если `mysql_upgrade` не был выполнен — пройтись обновлялкой

```
mysql_upgrade -u root -p
```

6. Версия mariadb-java-connector должна быть свежей, с 1.5.5 не работает

1.3.6 Настройка сервера СУБД PostgreSQL — внутренняя

Внутренняя страница для настройки PostgreSQL силами специалистами HFLabs. Не видна Заказчикам.

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

Актуальный файл настройки для версии 10.7 — postgresql.conf

1.3.7 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 клиент, 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.

1.3.8 Настройка сервера Подсказок

1.3.8.1 ОС и программное обеспечение

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Java SE Development Kit (JDK) 8 с установленными актуальными обновлениями.
- Wildfly 12

1.3.8.2 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) 8 с последними обновлениями.

1.3.8.3 Доступы и права

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

1.3.9 Настройка сервера Подсказок с выделенным Фактором

1.3.9.1 ОС и программное обеспечение

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Java SE Development Kit (JDK) 8 с установленными актуальными обновлениями.
- Wildfly 12

1.3.9.2 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 cdi_user 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) 8 с последними обновлениями.

1.3.9.3 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»).

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

1.3.10.1 ОС и программное обеспечение

- CentOS 6+ или Red Hat Enterprise Linux 6+, x64.
- Java SE Development Kit (JDK) 8 с установленными актуальными обновлениями.
- Wildfly 10.0.1.

1.3.10.2 Установка и настройка

1. Создан пользователь factor, под которым будет работать служба «Фактора»:
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) 8 с последними обновлениями.

1.3.10.3 Доступы и права

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

1.3.11 Настройка сервера приложений для очистки данных (ОС Windows)

1.3.11.1 ОС и программное обеспечение

- Windows 7 (x64) и выше или Windows 2008 Enterprise Edition и выше, x64.
- Java SE Development Kit (JDK) 8 с установленными актуальными обновлениями.
- Wildfly 10.0.1.

1.3.11.2 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.

1.3.11.3 Доступы и права

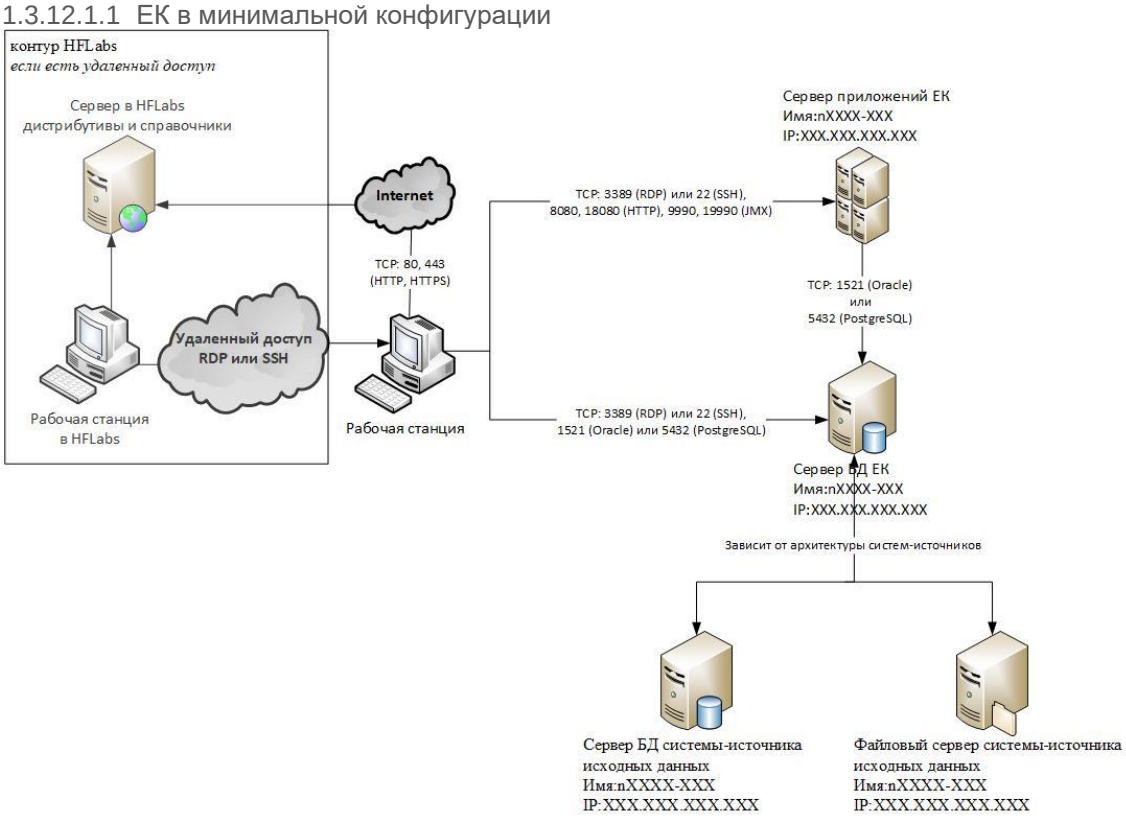
1. Открыты порты:
    - 3389 (RDP);
    - 18080 (HTTP-порт «Фактора»);
    - 19990 (порт для мониторинга «Фактора»).
2. Установка антивируса запрещена. В крайнем случае в настройки исключения антивируса должны быть добавлены директории Wildfly «Фактора».

1.3.12 Логическая схема развертывания Единого клиента

1.3.12.1 Пилотный проект Единый клиент. Логическая схема развертывания

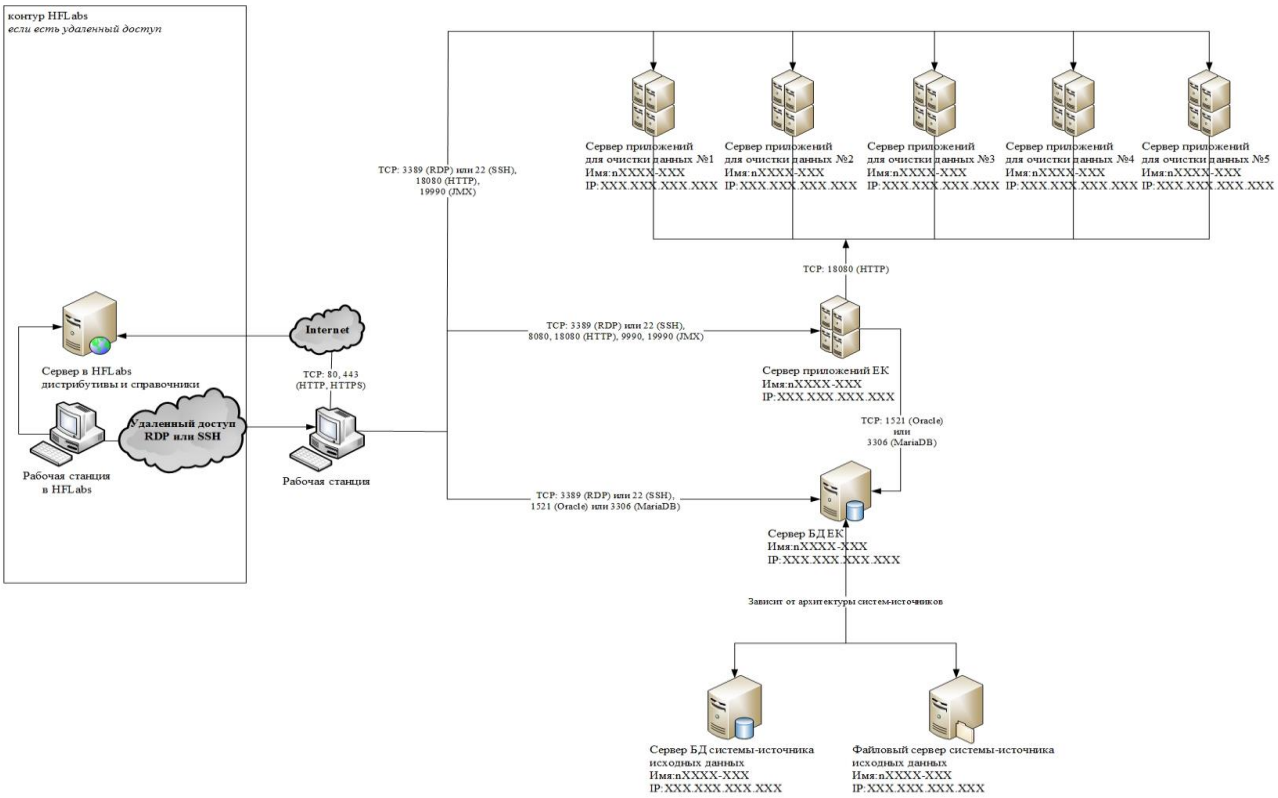
Схема логической структуры для пилота ЕК.vsdx

1.3.12.1.1 ЕК в минимальной конфигурации



1.3.12.1.2 ЕК с фермой «Факторов»

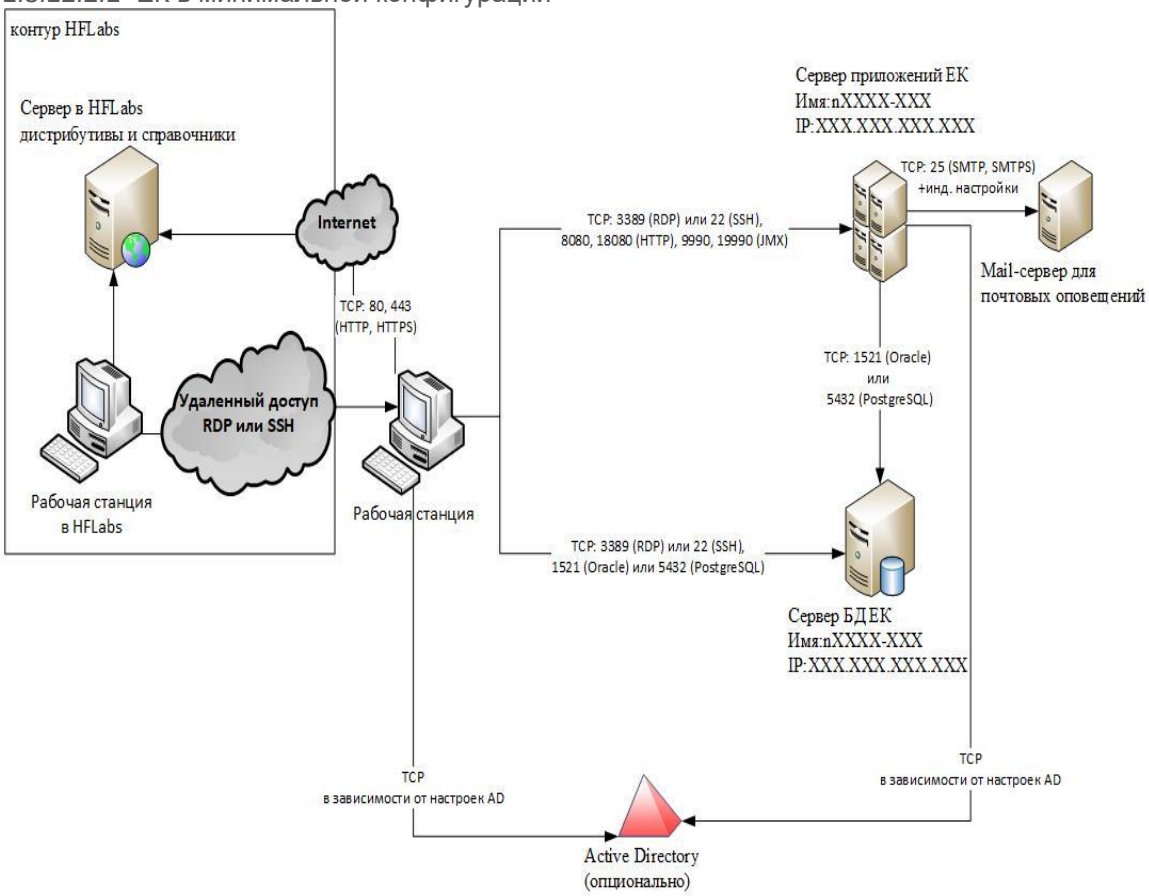
Для очистки большого объема данных в короткий срок требуется несколько серверов приложений для очистки данных. Количество серверов приложений для очистки данных (ферма «Факторов») зависит от объема данных и аппаратных возможностей конкретного проекта.



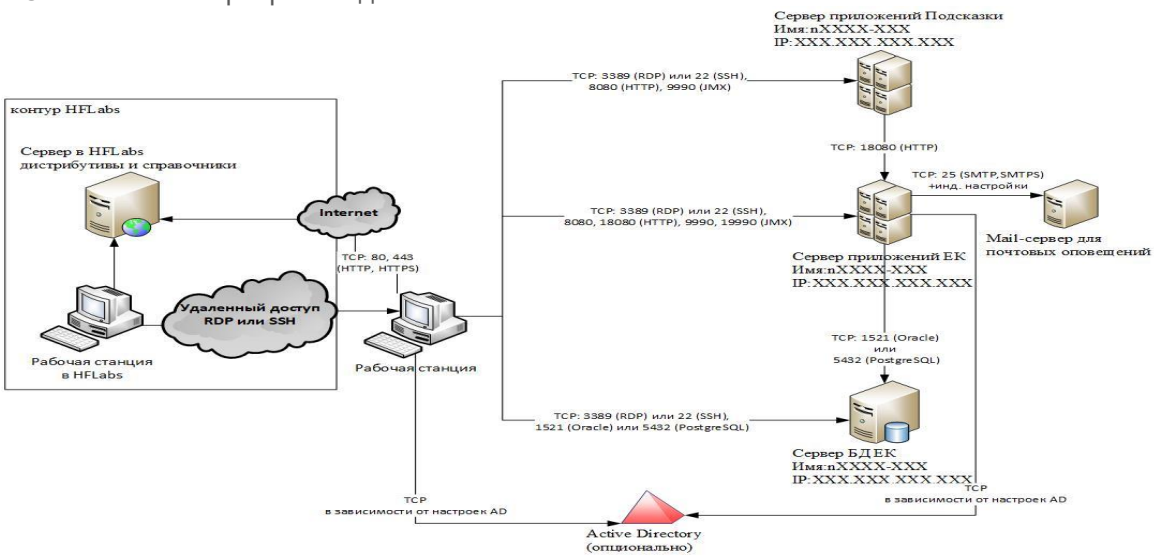
1.3.12.2 Внедрение проекта Единый клиент. Логическая схема развертывания

[Схема логической структуры для внедрения Единого Клиента.vsdx]

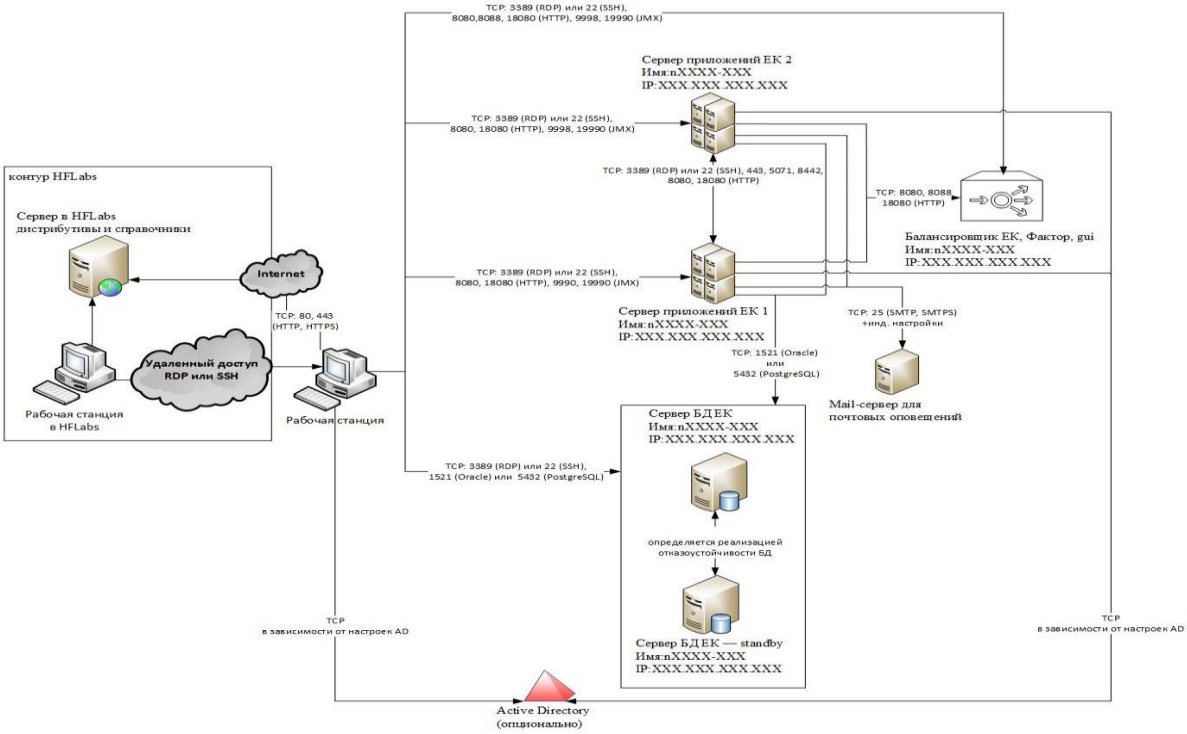
1.3.12.2.1 ЕК в минимальной конфигурации



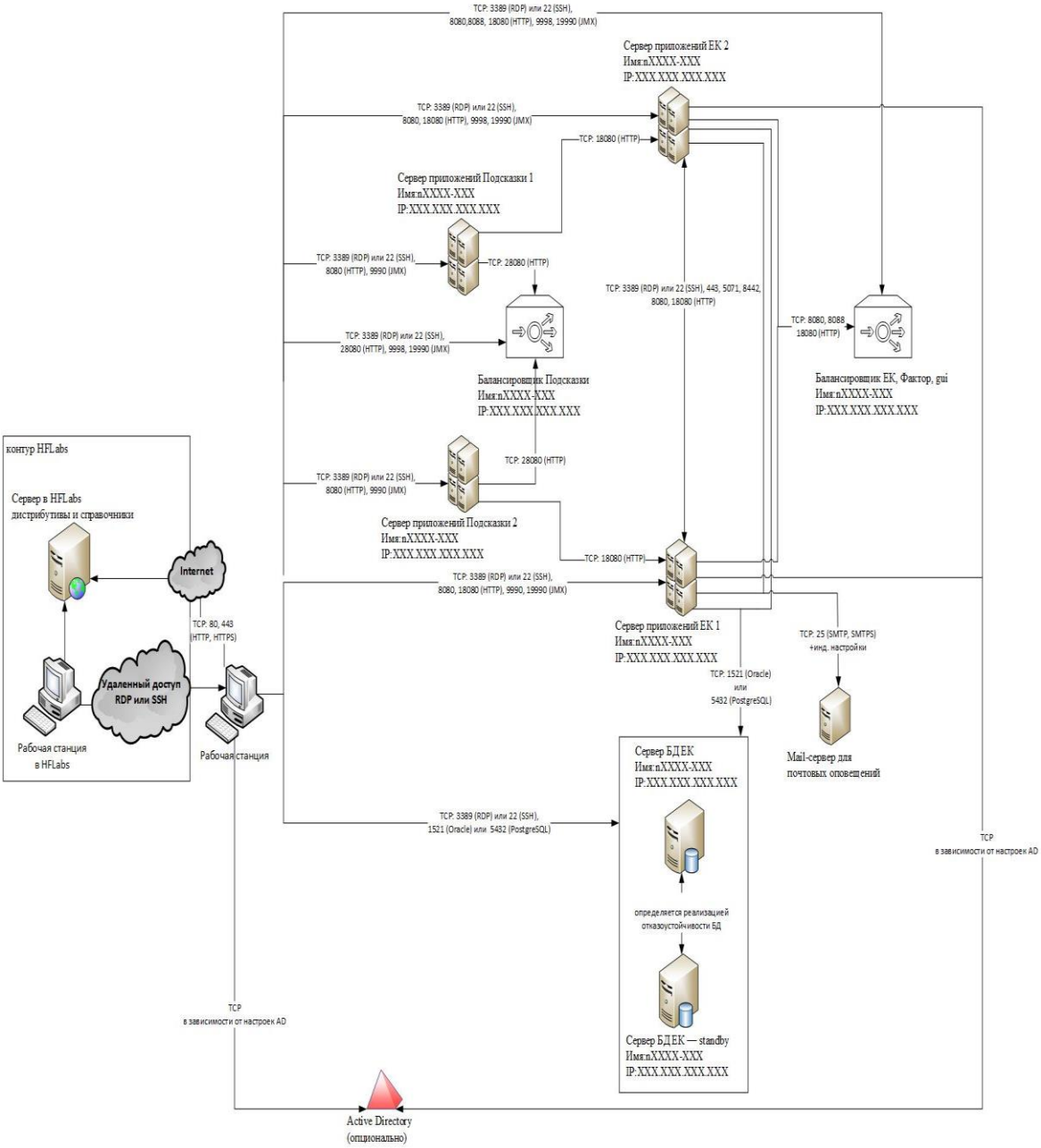
1.3.12.2.2 ЕК с сервером Подсказок



1.3.12.2.3 ЕК в отказоустойчивой конфигурации



1.3.12.2.4 ЕК и подсказки в отказоустойчивой конфигурации



1.3.13 Таблица сетевых доступов

Внутренняя страница с шаблонами. Недоступна пользователям извне.Перед отправкой требований Заказчику не забудьте проверить и дополнить представленные здесь шаблоны

1. **Таблица сетевых доступов для пилотного проекта с развертыванием фермы Факторов для быстрой обработки большого объема данных. (Первоисточник в Экселе)**
2.

№	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 ЕК	XXX.XXX.XXX.XXX			Установка и настройка приложений
				Сервер БД ЕК	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 ЕК	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 ЕК	XXX.XXX.XXX.XXX	1521 (Oracle) или 3306 (Maria DB)	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, документаци и из confluence HFLabs, дополнитель ных 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 ЕК	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 ЕК	XXX.XXX.XXX.XXX	>=1024	сервер БД ЕК	XXX.XXX.XXX.XXX	1521 (Oracle) или 3306 (Maria DB)	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 ЕК

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 клиент.
`factor-{customer}-{version}.war`	Система Фактор
`cdi-web-{customer}-{version}.war`	Система Единый клиент

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 клиента» и «Фактора»

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

```
useradd cdi
useradd factor
passwd -l cdi
passwd -l factor
```

Пользователей нужно объединить в одну группу:

```
groupadd hfl_cdi
usermod -a -G hfl_cdi cdi
usermod -a -G hfl_cdi factor
```

3.2.2 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 ЕК

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

```
cdi             hard    nofile  65535
cdi             soft    nofile  65535
cdi             hard    nproc   8192
cdi             soft    nproc   4096
cdi             hard    as      unlimited
cdi             soft    as      unlimited
cdi             hard    rss     unlimited
cdi             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 `cdi` — имена пользователей, под которыми работают «Фактор» и «Единый клиент».

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 клиента" 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 ЕК, 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.

Открывайте 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 ЕК, 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

```
cdi             hard    nofile  65535
cdi             soft    nofile  65535
cdi             hard    nproc   8192
cdi             soft    nproc   4096
cdi             hard    as      unlimited
cdi             soft    as      unlimited
cdi             hard    rss     unlimited
cdi             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 `cdi` — имена пользователей, под которыми работают «Фактор» и «Единый клиент».

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 клиента" 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 пользовател`ей cdi, factor` в файлах `/home/cdi/.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

3.5.1.1 Установочный пакет

Установочные пакеты Jboss поставляются совместно с системой в архивах:

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

3.5.1.2 Установка JBOSS

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/cdi
unzip wildfly-16.0.0.Final-18080.zip -d /opt/factor

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

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

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

3. Назначить права на запуск исполняемых файлов:

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

3.5.1.3 Настройка сервисов

Дистрибутив redhat-based-7

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

```
mkdir /etc/cdi
mkdir /etc/factor

cp /opt/cdi/jboss/docs/contrib/scripts/systemd/wildfly.conf
/etc/cdi/
cp /opt/cdi/jboss/docs/contrib/scripts/systemd/wildfly.service
/etc/systemd/system/cdi.service
cp /opt/cdi/jboss/docs/contrib/scripts/systemd/launch.sh
/opt/cdi/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/cdi.service` переменные заданы по умолчанию. При необходимости заменить параметры `Limit*` и путь к `launch.sh` (параметр `ExecStart`).

   cdi.service

Code Block 8 cdi.service

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

[Service]
Environment=LAUNCH_JBOSS_IN_BACKGROUND=1
EnvironmentFile=-/etc/cdi/wildfly.conf
User=cdi
OOMScoreAdjust=-1000
PIDFile=/var/run/cdi/wildfly.pid
ExecStart=/opt/cdi/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
```

factor.service

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/cdi/jboss/bin/launch.sh`

```
WILDFLY_HOME="/opt/cdi/jboss"
```

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

```
chmod +x /opt/cdi/jboss/bin/launch.sh
chmod +x /opt/cdi/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 cdi.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 клиента».
- `wildfly-16.0.0.Final-8080-HotReserve.zip` — для «Единого клиента» 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
```

3.5.3 Инструкция для сервера Подсказок (Linux)

3.5.3.1 Установить приложение

```
su - factor
cd /data
wget https://fs.hflabs.ru/sgt-flight/wildfly/suggestions-wildfly16.zip
unzip suggestions-wildfly16.zip
```

3.5.3.2 Настроить сервис

Под пользователем root.

Подготовить конфигурацию для запуска Подсказок как сервиса:

```
mkdir /etc/suggestions
cp /data/suggestions/docs/contrib/scripts/systemd/suggestions.conf
/etc/suggestions/
cp /data/suggestions/docs/contrib/scripts/systemd/suggestions.service
/etc/systemd/system/
cp /data/suggestions/docs/contrib/scripts/systemd/launch.sh
/data/suggestions/bin/
chmod +x /data/suggestions/bin/launch.sh
```

Настроить автостарт при запуске ОС:

```
systemctl enable suggestions.service
```

3.5.3.3 Скачать сборку

```
su - factor
wget https://fs.hflabs.ru/sgt-flight/suggestions/build/19.11/suggestions-
web-19.11-SNAPSHOT.war -P /data/suggestions/standalone/deployments/
```

3.5.3.4 Установить лицензию

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

3.5.3.5 Запустить приложение

Под пользователем root.

```
service suggestions start
```

3.5.4 Подключение обогащенных Подсказок

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

3.5.4.1 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"
```

3.5.4.2 Как проверить, что подсказки обогащаются Фактором?

Введите адрес с квартирой.

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

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 ЕК, 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 системы Единый клиент

4.1.1 Настройка горячего резерва

Выполните инструкцию.

4.1.2 Настройка datasource для заказчиков, использующих шифрованный пароль к БД

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

4.1.2.1 Windows

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

4.1.2.2 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>
```

4.1.3 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
```

4.1.4 Установка системы на Linux

4.1.4.1 Создание рабочих каталогов приложения

1. Создайте рабочий каталог CDI и дайте на него права пользователю `cdi`:

```
mkdir -p /home/cdi
chown -R cdi:cdi /home/cdi
```

2. Создайте каталог, используемый при поиске дубликатов:

```
mkdir /home/cdi/dedup
```

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

```
chgrp hfl_cdi /home/cdi/dedup
chmod 775 /home/cdi/dedup
```

4.1.4.2 Копирование исполняемых файлов

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

4.1.4.3 Настройка параметров запуска WildFly

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

```
# CDI 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 CDI. Обычно `/home/cdi`
`PATH_TO_DEDUP_DIR` — путь до каталога для дедупликации. Обычно `/home/cdi/dedup`

4.1.4.4 Создание рабочих каталогов приложения

1. Создайте рабочий каталог CDI и дайте на него права пользователю `cdi`:

```
mkdir -p /home/cdi
chown -R cdi:cdi /home/cdi
```

2. Создайте каталог, используемый при поиске дубликатов:

```
mkdir /home/cdi/dedup
```

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

```
chgrp hfl_cdi /home/cdi/dedup
chmod 775 /home/cdi/dedup
```

4.1.4.5 Копирование исполняемых файлов

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

4.1.4.6 Настройка параметров запуска WildFly

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

```
# CDI 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 CDI. Обычно `/home/cdi`
`PATH_TO_DEDUP_DIR` — путь до каталога для дедупликации. Обычно `/home/cdi/dedup`

4.1.5 Копирование исполняемых файлов

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

4.1.5.1 Настройка параметров запуска JBoss

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

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

`CDI_ROOT_DIR` - см раздел "дополнительный каталог" ниже

4.1.5.2 Дополнительные каталоги (Windows)

Создайте дополнительные каталоги, которые будут использоваться при работе системы:

```
mkdir C:\cdi
```

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

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

```
icacls C:\cdi /grant %HFL_USER%:F
```

4.2 Настройка доступа к БД

4.2.1 Настройка доступа к БД

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

- `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>
[...]
```

4.2.2 Настройка доступа к БД

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

- `connection-url` — параметры соединения с БД в одну строку формата `jdbc:mariadb://{db-hostname}:{port}/{name_of_database}?tinyInt1isBit=false`
    - `{db-hostname}` — IP-адрес или доменное имя сервера БД.
    - `{port}` — порт, на котором слушает сервер БД (по умолчанию 3306).
    - `{name_of_database}` — название схемы БД.
- `driver - org.mariadb.jdbc.Driver`
- `user-name` – имя пользователя для доступа системы к БД.
- `password` – пароль пользователя для доступа системы к БД.

Пример:

```
[...]
<connection-url>jdbc:mariadb://{db-hostname}:{port}/{name_of_database}?tinyInt1isBit=false</connection-url>
<driver>org.mariadb.jdbc.Driver</driver>
[...]
<security>
    <user-name>username</user-name>
    <password>password</password>
</security>
[...]
```

cdi-mariadb-ds.xml - пример файла

4.2.3 Настройка доступа к БД

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

- `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>
[...]
```

5 Запуск системы

5.1 Linux

5.1.1 Запуск системы Единый клиент

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

```
$ service cdi start
```

5.1.2 Остановка системы Единый клиент

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

```
$ service cdi stop
```

5.1.3 Добавление службы в автозапуск

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

5.1.4 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 Единый клиент

```
net start cdi
```

5.2.2 Остановка системы Единый клиент

```
net stop cdi
```

6 Дополнительные шаги

6.1 Подключение экспорта через JMS

Для того, чтобы Единый клиент 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 ЕК 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 ЕК 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 ЕК (настройка горячего резерва)

6.2.1 Настройка Wildfly 16

Для каждого экземпляра ЕК в файле `standalone/configuration/standalone.xml` директории JBoss ЕК 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
ЕК}" port="{http порт второго экземпляра ЕК}"/>
     </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 ЕК.

6.2.3 Синхронизация системного времени

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

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

6.2.4 Активация подсистемы обмена сообщениями в Wildfly 16

Все настройки выполняются в файле `standalone/configuration/standalone.xml` директории JBoss ЕК 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 EK 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

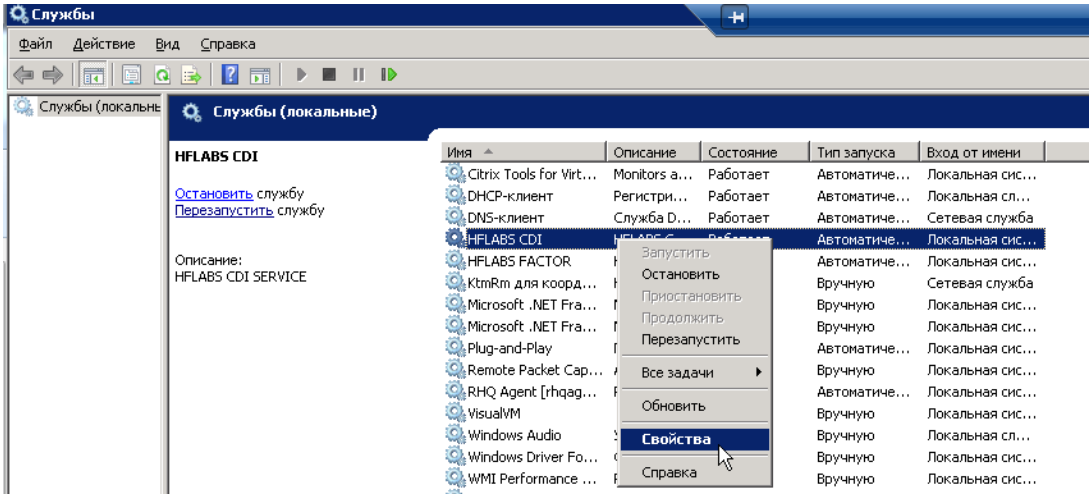
Cross-origin resource sharing (CORS) — технология современных браузеров, которая позволяет предоставить веб-странице доступ к ресурсам другого домена.

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

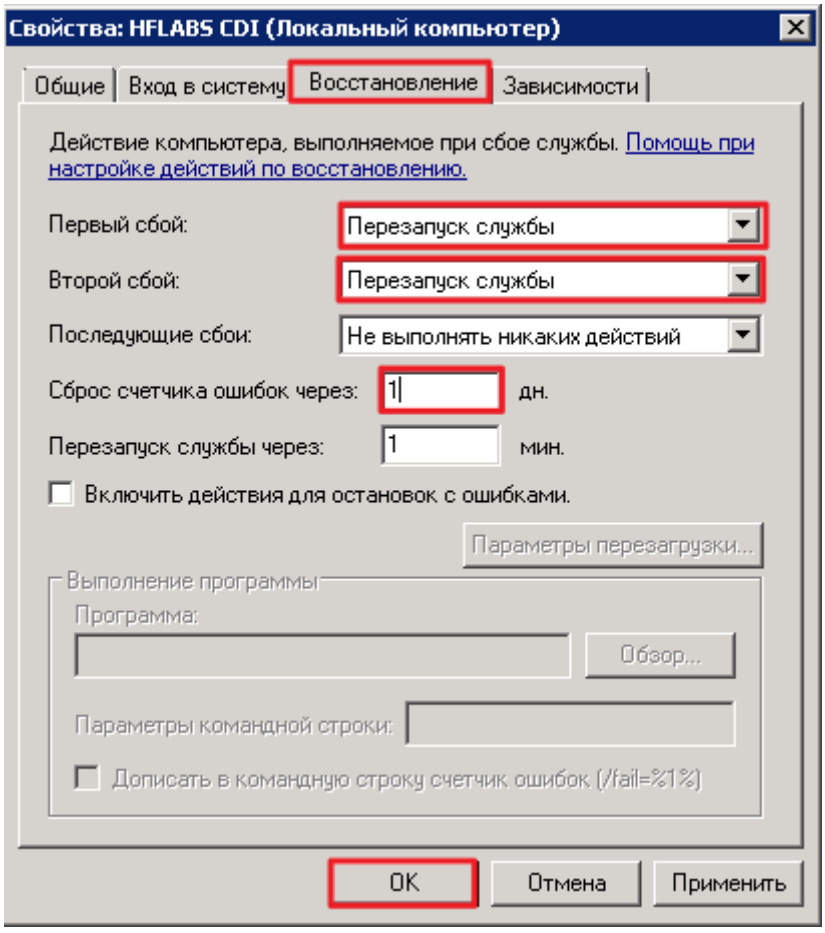
```
        <subsystem xmlns="urn:jboss:domain:undertow:1.2">
            <buffer-cache name="default"/>
            <server name="default-server">
                <http-listener name="default" socket-binding="http"/>
                <host name="default-host" alias="localhost">
                    ...
                    <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"
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 CDI 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 (хост и порт для ldaps и openssl совпадают):

Code Block 15 Запрос для получения ключа

```
openssl s_client -showcerts -connect domain.com:3869 > 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 `ldaps.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-----
```

6.6.2 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.cer -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 EK:

   ```
   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 EK:

```
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 EK:

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 шифрования для MariaDB

Статья для Windows. Для Linux принципиально не отличается.

6.8.1 Генерирование ключей

Для генерирования ключей можно использовать пакет OpenSSL. Для Linux есть в репозиториях. Скачать его для Windows можно по ссылкам:

http://slproweb.com/products/Win32OpenSSL.html
http://slproweb.com/download/Win64OpenSSL_Light-1_1_0h.exe

Возможно (в ходе настроек я это делал, но не уверен, что это прямо обязательно), понадобится создать конфигурационный файл для OpenSSL. Пример приаттачен к статье (openssl.cnf). Далее в консоли надо указать его местоположение:

```
set OPENSSL_CONF=c:\OpenSSL-Win64\ssl\openssl.cnf
```

Также в консоли лучше выполнить

```
set path=%path%;c:\OpenSSL-Win64\bin
```

6.8.2 Шифрование датафайлов

Движок InnoDB, который мы используем, поддерживает шифрование файлов данных. Ему нужны ключи шифрования, которые поставляет один из плагинов. Самый простой плагин называется File Key Management plugin и встроен в марию. Для него создаётся файлик со списком ключей симметричного шифрования. Чтобы этот файл не был доступен всем и каждому, он шифруется. Пароль кладётся в другой файл, который может быть на подключаемом носителе. Например, на флешке. Файл пароля необходим только в момент запуска марии.

6.8.2.1 Создание файла с ключами

Несколько раз выполнить

```
openssl rand -hex 32 >> c:\OpenSSL-Win64\keys\keys.txt
```

Затем в получившемся файле ключи пронумеровать, должно получиться примерно так:

Code Block 17 keys.txt

```
1;4cd49d01...
2;a33d0876...
3;55fc81de...
```

Дальше надо этот файл зашифровать, а пароль положить ещё в один текстовик (в этом примере keys.pwd).

```
openssl enc -aes-256-cbc -md sha1 -k MyCoolPassword -in c:\OpenSSL-
Win64\keys\keys.txt -out c:\OpenSSL-Win64\keys\keys.enc
```

6.8.2.2 Настройка maria

Скопировать файлы keys.enc и keys.pwd в доступное для марии место. В идеале, pwd на отключаемый носитель. Добавить в конфиг марии в секцию mysql следующее:

```
# File Key Management settings
# note: AES_CTR is supported in some MariaDB distributions
# note: use innodb-encrypt-tables=FORCE to disable an ability of
unencoded tables creation
plugin_load_add = file_key_management
file_key_management_filename = C:/OpenSSL-Win64/keys/keys.enc
file_key_management_filekey = FILE:C:/OpenSSL-Win64/keys/keys.pwd
file_key_management_encryption_algorithm = AES_CBC
innodb-encrypt-tables
innodb-encrypt-log
innodb-encryption-threads = 4
innodb-tablespaces-encryption
```

Если после этого перезапустить марию, то можно увидеть, как файлы постепенно шифруются.

6.8.2.3 Дополнительно

Основной минус шифрования файлов данных: усложняется или становится невозможной работа многих механизмов для резервного копирования.

6.8.3 Шифрование соединения

Если передача данных производится не в рамках одной подсети, имеет смысл настраивать шифрование соединения, чтобы избежать перехвата трафика. Версия TLS (наследник SSL) зависит от того, с каким движком шифрования собрана мария. Здесь и далее SSL и TLS используются как синонимы.

Community на Windows собрана с yaSSL и поддерживает TLS 1.0 (достаточно старый формат).

Enterprise на Windows и все сборки для Linux используют библиотеку OpenSSL и поддерживают TLS 1.0, 1.1 и 1.2.

MariaDB последних версий для Windows поддерживает шифрование из коробки. Для Linux, возможно, понадобится установить OpenSSL дополнительно, но это не точно.

6.8.3.1 Варианты шифрования

Просто шифровать соединение. Не избавляет от атаки MITM.

Шифрование соединения с проверкой сертификата сервера. Клиент после установки соединения проверяет сертификат, которым подписывается сервер. Для этого клиент этот сертификат должен знать. Есть несколько разных способов, но проще всего просто скопировать его на клиент. Собственно, описано в данной статье.

Шифрование соединения с двусторонней проверкой. Как предыдущее, но помимо этого ещё и сервер проверяет сертификат клиента. Требует плясок с бубнами и хранилищами сертификатов java, поэтому не использовалось.

6.8.3.2 Создание сертификатов

Всё делается в консоли.

```
set dst=c:\OpenSSL-Win64\ssl

openssl genrsa 2048 > %dst%\ca-key.pem
openssl req -new -x509 -nodes -days 365000 -key %dst%\ca-key.pem -out
%dst%\ca-cert.pem
openssl req -newkey rsa:2048 -days 365000 -nodes -keyout %dst%\server-
key.pem -out %dst%\server-req.pem

openssl rsa -in %dst%\server-key.pem -out %dst%\server-key.pem
openssl x509 -req -in %dst%\server-req.pem -days 365000 -CA %dst%\ca-
cert.pem -CAkey %dst%\ca-key.pem -set_serial 01 -out %dst%\server-
cert.pem
openssl req -newkey rsa:2048 -days 365000 -nodes -keyout %dst%\client-
key.pem -out %dst%\client-req.pem
```

Строка 1: для упрощения жизни, чтобы много не писать.

Строки 3-5: генерация корневого самоподписанного сертификата.

Строки 7-9: генерация сертификата сервера.

6.8.3.3 Настройка maria

Скопировать ca.pem, server-cert.pem, server-key.pem в доступное для марии место и добавить в конфиг марии в секцию mysql следующее:

```
ssl
ssl-ca=C:/Program Files/MariaDB 10.2/ssl/ca.pem
ssl-cert=C:/Program Files/MariaDB 10.2/ssl/server-cert.pem
ssl-key=C:/Program Files/MariaDB 10.2/ssl/server-key.pem
```

Кроме этого, server-cert.pem надо будет скопировать на клиент.

6.8.3.4 Строка соединения

Строка соединения в датасорсе принимает следующий вид:

```
jdbc:mariadb://localhost:3306/testdb?useSSL=true&requireSSL=true&verifySe
rverCertificate=true&disableSslHostnameVerification=true&serverSslCert=se
rver-cert.pem
```

useSSL — по возможности, использовать SSL. При этом по решению сервера SSL может не использоваться.

requireSSL — обрывать соединение, если сервер не согласился на SSL.

verifyServerSertificate — сверять сертификат сервера (локально сохранённый) с тем, что отдаёт сервер. Нужно для исключения атаки MITM.

disableSslHostnameVerification — сверять имя сервера с именем, на который выписан сертификат. Для простоты тут проверка выключена.

serverSslCert — где искать локальную копию сертификата для сверки. В данном случае я копировал сразу в корневую директорию WildFly и в bin. Не знаю, что из них сработало.

trustServerSertificate — «шунтирование» проверок сертификата сервера, можно использовать при настройке, в бою не надо. В примере не используется.

6.8.3.5 Пользователь

Необходимость шифрования на стороне сервера указывается для конкретного пользователя.

Если пользователь новый, то создаём его с опцией:

```
GRANT ...
    ON ... TO '...' IDENTIFIED BY '...' REQUIRE SSL;
```

Если пользователь уже создан, то надо сделать следующее:

```
update mysql.user set ssl_type = 'ANY' where user='cdi';
commit;
flush privileges;
```

Последняя строка для того, чтобы мария перечитала привилегии пользователей.

6.8.3.6 Как проверить

С помощью какого-нибудь SQL-клиента, который использует JDBC.

1. Попытаться соединиться с сервером без TLS. Не должно получаться.
2. Соединиться со строкой из datasource. Должно пройти соединение. После этого выполнить запрос

   ```
   show status like '%ssl%';
   ```

   Интересуют конкретно параметры Ssl_version (должен быть «TLSv1» или подобное) и Ssl_cipher (не должен быть пустой).

6.8.3.7 Дополнительно

Для использования шифрования соединения потребовалось поднять версию mariadb-коннектора в WildFly до mariadb-java-client-2.2.3.jar. Используемый сейчас 1.1.7 заставить работать не получилось.

6.9 Настройка взаимодействия с Microsoft Exchange

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

6.9.1 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 18 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-----
```

6.9.2 Формирование jks-хранилища

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

Code Block 19 Создание jks

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

6.9.3 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
```

6.9.4 Настройка ЕК

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

```
mail.protocol = smtp
```

7 Установка системного и специального ПО в Linux

7.1 Создание пользователей для «Единого клиента» и «Фактора»

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

```
useradd cdi
useradd factor
passwd -l cdi
passwd -l factor
```

Пользователей нужно объединить в одну группу:

```
groupadd hfl_cdi
usermod -a -G hfl_cdi cdi
usermod -a -G hfl_cdi factor
```

7.2 Создание пользователей для «Подсказок»

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

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

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

7.3 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.

7.4 Установка JDK

7.4.1 Windows

Установите JDK с помощью скачанного установочного пакета.

7.4.2 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`.

7.5 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.

7.6 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.

7.6.1 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"
```

7.6.2 Linux

Для пользователей cdi, factor в файлах /home/cdi/.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.