H F Labs

«Центр управления согласиями»

Руководство по развертыванию

Оглавление

1 Информация для старта внедрения

1.1 Рабочая станция для HFLabs

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

1.2 Сервер приложений «Центр управления согласиями»

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

1.3 СУБД

1. Hostname и IP-адрес;
2. Порт, на котором слушает PostgreSQL;
3. SID или Service name PostgreSQL;
4. Логин и пароль пользователя СУБД «Центра управления согласиями».

1.4 Сервер Standby СУБД (в случае отказоустойчивой конфигурации)

1. Hostname и IP-адрес;
2. Порт, на котором слушает PostgreSQL;
3. SID или Service name PostgreSQL;
4. Логин и пароль пользователя СУБД «Центра управления согласиями».

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.

1.6 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.

1.7 Сервер балансировки (при наличии в отказоустойчивой конфигурации)

Имя сервера и его IP-адрес.

2 Требования к промышленной программно-аппаратной платформе

2.1 Сервер приложений «Центр управления согласиями»

- Процессор Intel(R) Xeon(R) Silver 4114 или выше – 16 CPU;
- 64 Гб оперативной памяти;
- SSD-диск объемом 400 Гб;
- Рекомендуемые операционные системы: ОС Альт Сервер 10 x64.
- Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями.

2.2 Сервер БД

- Процессор Intel(R) Xeon(R) Silver 4114 или выше – 10 CPU;
- 24 Гб оперативной памяти;
- SSD-диск объемом 400 Гб;
- СУБД — PostgreSQL 11+.

2.3 Рабочее место менеджера согласий (клиентская часть)

Для работы менеджеров согласий нужно выделить им клиентские машины:

- Процессор Intel Core i3 или новее;
- Оперативная память 4 Гб;
- Свободное место на жёстком диске 10 Гб;
- Сетевая карта 100 Мбит;
- Операционная система Windows 7 и выше;
- Разрядность ОС 64-bit;
- Рекомендуемый браузер: Mozilla Firefox Quantum версии 67+ или Google Chrome версии 75+.

2.4 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 «Центра управления согласиями» в отказоустойчивой конфигурации.

Требования к пропускной способности каналов между компонентами:

Компонент 1	Компонент 2	Ширина канала

Рабочая станция HFLabs	Сервер приложений «Центр управления согласиями»	100 Мбит/с
Рабочая станция HFLabs	Сервер СУБД	100 Мбит/с
Сервер приложений «Центр управления согласиями»	Сервер СУБД	1 Гбит/с
Сервер приложений «Центр управления согласиями» 1	Сервер приложений «Центр управления согласиями» 2	1 Гбит/с

2.5 Доступы и права

1. Рабочие станции внесены в домен.
2. Создан пользователь с правами локального администратора.
3. Открыт доступ к серверу приложений «Центр управления согласиями» по портам:
    a. 3389 (RDP) или 22 (SSH), в зависимости от платформы сервера приложений;
    b. 8080 (HTTP-порт «Центра управления согласиями»).
4. Доступна возможность копирования файлов на сервер приложений «Центра управления согласиями» (по RDP или иным способом).
5. В случае СУБД PostgreSQL: открыт доступ к серверу СУБД по порту 5432.
6. Доступ к ресурсам HFLabs через сеть Интернет — Confluence и Jira.
7. Доступы к второму экземпляру сервера «Центра управления согласиями» в случае отказоустойчивой конфигурации.

3 Требования к настройке программно-аппаратной платформы

3.1 Настройка рабочей станции для HFLabs

ОС и программное обеспечение:

- ОС Альт Сервер 10 x64;
- 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.

3.2 Настройка сервера приложений «Центр управления согласиями» (ОС *nix)

3.2.1 ОС и программное обеспечение

- ОС Альт Сервер 10 x64.
- Java SE Development Kit (OpenJDK) 11, с установленными актуальными обновлениями;
- Wildfly 16.0.0.

3.2.2 Установка и настройка

1. Создан пользователь, под которым будут работать службы «Центра управления согласиями». Пользователь добавлен в группу — hfl.
2. Создан пользователь consent_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.
5. Установка антивируса запрещена.

3.5 Настройка сервера СУБД PostgreSQL — внутренняя

Актуальный файл настройки для версии 10.7 — postgresql.conf.

3.6 Настройка Active Directory

1. В Active Directory (AD) добавлены группы, соответствующие ролям, определенным в ролевой модели. 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 роли ADMINISTRATOR или аналогу.
4. В AD создана учетная запись для системы «Центр управления согласиями», которая имеет права на чтение записей AD из следующих веток:

a. ветки AD, в которой заведены учетные записи пользователей;
b. ветки AD, в которой заведены группы.

5. Для этой записи должен быть установлен режим без смены паролей.

3.7 Отключение SWAP

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

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

Перезагрузите операционную систему.

3.8 Настройка Linux для активной работы с SSD

Отключение времени модификации файлов
Если приложение часто и многократно пишет и читает, то на файловых системах 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):

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

4 Установка системы

Используемый дистрибутив: «Альт Сервер 10.0» alt-server-10.0-x86_64

Порядок установки

Установка любой программы выполняется на чистой системе только после обновления системы и ядра до актуального состояния:
$su-
#apt-get update && apt-get dist-upgrade
#update-kernel [-t std-def|un-def]
#reboot

Установка Liberica

*все действия выполняются от супер пользователя
# apt-get update
# apt-get install apt-https apt-repo
# apt-repo add "rpm https://altlinux.bell-sw.com $(uname -m) liberica"
# apt-get update
# apt-get install bellsoft-java11
$ export JAVA_HOME=/usr/lib/jvm/bellsoft-java11.x86_64

Установка WildFly

Перенести полученный дистрибутив необходимый для установки и настройки программ в директорию /opt

1. Создать необходимый рабочий каталог, пользователя и назначить созданной директории владельца и группу hflabs
#mkdir -p /opt/perecoder
#chown -R hflabs:hflabs /opt/perecoder/
2. Распаковать архив с WildFly из скачанного репозитория в каталог /opt/perecoder/
#unzip cmc-distrib.zip

3. Создать директорию в /etc с названием будущей службы (perecoder), скопировать файлы:
#cp /opt/perecoder/appserver/docs/contrib/scripts/systemd/perecoder.conf /etc/perecoder/
#cp /opt/perecoder/appserver/docs/contrib/scripts/systemd/perecoder.service /etc/systemd/system/perecoder.service

#cp /opt/perecoder/appserver/docs/contrib/scripts/systemd/launch.sh /opt/perecoder/appserver/bin/

4. На файлы launch.sh и standalone.sh выдать права на запуск:
   #chmod +x /opt/perecoder/appserver/bin/{launch,standalone}.sh

5. Перезагрузить список доступных сервисов, чтобы systemd мог управлять новым сервисом:
   #systemctl daemon-reload

6. Добавить службы в авто запуск:
   #systemctl enable perecoder.service

7. Скопировать следущие файлы в каталог сервера приложений (JBoss/Wildfly) standalone/deployments:

a. cmc-web-{version}.war;
b. cmc-{database}-ds.xml.

8. Скорректировать содержимое файла cmc-{database}-ds.xml согласно настройкам БД.

9. В директории сервера приложений bin/standalone.conf установить следующие параметры запуска JVM: -Xms8g -Xmx8g.

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