Кайдзен

Система автоматизированного управления заседаниями

РУКОВОДСТВО ПО УСТАНОВКЕ ПО КАЙДЗЕН

Тюмень, 2021

Содержание

1. Установка клиентской части

Клиентская часть «Кайдзен» работает под операционной системой Windows и требует установки. Для установки клиента необходимо 2 раза кликнуть по «Клиент Кайдзен.exe» и ПО автоматически установится в нужную папку.

Для корректной работы клиента необходимо наличие в папке клиента файла настроек *config.json* со следующим содержимым:

```
    {
  "serverApi": "http://kaizen-srv:8082/api/v1",
  "notifyApi": "http://kaizen-srv:8081/api/v1",
  "serverEventSource": "http://kaizen-srv:8180/api/v1",
  "notifyEventSource": "http://kaizen-srv:8180/api/v1",
  "keycloak": {
    "url": "http://keycloak.asusp.corp:8080/auth/",
    "realm": "kai",
    "clientId": "electron"
  }
}
```

Где «kaizen-srv» – имя сервера «Кайдзен».

«keycloak.asusp.corp» — имя сервера keycloak в домене ASUSP.CORP (в штатной установке совпадает с сервером «Кайдзен»).

realm – имя профиля настроек в keycloak.

Чтобы перейти в папку клиента, необходимо кликнуть правой кнопкой по ярлыку ПО «Кайдзен» и выбрать «Расположение файла».

2. Установка серверной части на Linux

2.1. Требования

Необходим сервер с Centos 7/8

1. Для установки базы данных и Keycloak
2. Для установки трех приложений:
   2.1. Сервер для бэкенда
   2.2. Сервер для отправки уведомлений
   2.3. Прокси-сервер.

2.2. Установка и настройка PostgreSQL 12

1) Установка PostgreSQL 12

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

Установите клиентские и серверные пакеты PostgreSQL:

```
sudo yum -y install epel-release yum-utils
sudo yum-config-manager --enable pgdg12
sudo yum install postgresql12-server postgresql12
```

После установки требуется инициализация базы данных, прежде чем можно будет запустить службу.

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

Запустите и включите службу сервера базы данных.

```
sudo systemctl enable --now postgresql-12
```

2) Настройка Postgresql

1) Создать две роли в postgresql

- asusp — для основного сервера
- notify — для сервера оповещений

выполнить в терминале:

для `asusp`

```
sudo -u postgres createuser --interactive -P
```

```
[root@localhost etc]# sudo -u postgres createuser --interactive -P
Enter name of role to add: asusp
Enter password for new role:
Enter it again:
Shall the new role be a superuser? (y/n) n
Shall the new role be allowed to create databases? (y/n) n
Shall the new role be allowed to create more new roles? (y/n) n
```

Рисунок 1 Создание пользователя asusp

для `notify`

```
sudo -u postgres createuser --interactive -P
```

```
[root@localhost etc]# sudo -u postgres createuser --interactive -P
Enter name of role to add: notify
Enter password for new role:
Enter it again:
Shall the new role be a superuser? (y/n) n
Shall the new role be allowed to create databases? (y/n) n
Shall the new role be allowed to create more new roles? (y/n) n
```

Рисунок 2 Создание пользователя notify

Для смены пароля у роли отдельно выполнить

```
su postgres
psql
```

дальше выполнить

```
ALTER USER asusp WITH PASSWORD 'password';
ALTER USER notify WITH PASSWORD 'password';
```

2) Создать две базы данных

В консоли postgresql(psql) создать две бд:

```
su postges
cd ~
psql
CREATE DATABASE asusp OWNER asusp;
CREATE DATABASE notify OWNER notify;
```

3) Настроить pg_hba.conf, прописать доступ по паролю к серверам:

прописать сеть, из которой приходят запросы на `listen_addresses` `postgresql`

- если сервер один то 127.0.0.1/32
- если серверов несколько (один для бд, другой для серверных приложений) то либо сеть в котором сервера 192.168.104.0/24 либо конкретный адрес сервера с маской 32: 192.168.104.14/32

```
su postges
```

```
cd ~/
nano ~/12/data/pg_hba.conf
host all all 127.0.0.1/32 md5
```

Если в файле присутствуют записи, где вместо md5 написано ident, то их необходимо удалить.

4) Настройка listen_addresses

```
su postges
cd ~/
nano ~/12/data/postgresql.conf
listen_addresses = '*'
```

5) Настройка firewall для postgresql если сетевой интерфейс в зоне public:

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

6) Рестарт сервера

```
sudo systemctl restart postgresql-12
```

2.3. Установка и настройка Keycloak

1) Перевод selinux в режим permissive

В файле `/etc/sysconfig/selinux изменить:`

```
SELINUX=enforcing
```

Выполнить:

```
sudo setenforce 0
```

2) Установить openjdk

```
sudo yum install java-latest-openjdk
```

Удостовериться, что установлена только последняя версия java. Минимальная версия 14.0.1.

3) Установить дополнительные утилиты wget

```
sudo yum install wget tar
```

4) Установить keycloak

```
wget
http://downloads.jboss.org/keycloak/10.0.1/keycloak-
10.0.1.tar.gz
tar -xzf keycloak-10.0.1.tar.gz
sudo mv keycloak-10.0.1 /opt
```

5) Создать пользователя

```
sudo useradd -r keycloak
```

6) Настроить владельца на директорию с keycloak

```
sudo chown -R keycloak: /opt/keycloak-10.0.1
```

7) Создать файл `systemd unit` в /etc/systemd/system/keycloak.service с содержимым:

```
[Unit]
Description=Keycloak Server
After=network.target

[Service]
Type=idle
User=keycloak
Group=keycloak
ExecStart=/bin/bash -c '/opt/keycloak-
10.0.1/bin/standalone.sh -b 0.0.0.0'
TimeoutStartSec=600
TimeoutStopSec=600

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

8) Включить и запустить keycloak:

```
systemctl enable keycloak
systemctl start keycloak
```

9) Настройка firewall для keycloak если сетевой интерфейс в зоне public:

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

10) Пользователь для входа в интерфейс keycloak

```
/opt/keycloak-10.0.1/bin/add-user-keycloak.sh -r master -u
admin -p secret
systemctl restart keycloak
```

11) Зайти в интерфейс для администрирования по адресу http://localhost:8080 и проверить, что авторизация проходит корректно

12) Установка krb5-workstation для работы с kerberos на keycloak

```
sudo dnf install krb5-workstation
```

15) Создать и настроить пользователя Keycloak на контроллере домена по главе 6.

16) Создать krb5.keytab на контроллере домена, используя главу 6, и скопировать на сервер с keycloak в

```
/etc/krb5.keytab
```

17) Создать файл настроек /etc/krb5.conf вместо KAI.ZEN, текущий realm домена, 192.168.1.10 – адрес контролера домена (тут можно указывать несколько)

```
# To opt out of the system crypto-policies configuration of
krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will
not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 rdns = false
 default_realm = KAI.ZEN
 dns_lookup_realm = false
 dns_lookup_kdc = false
 default_tkt_enctypes = rc4-hmac,aes256-cts-hmac-sha1-
96,aes128-cts-hmac-sha1-96
 default_tgs_enctypes = rc4-hmac,aes256-cts-hmac-sha1-
96,aes128-cts-hmac-sha1-96
 ticket_lifetime = 8h
 renew_lifetime = 7d
 forwardable = true

[realms]
 KAI.ZEN = {
  kdc = 192.168.1.10
  admin_server = 192.168.1.10
 }

[domain_realm]
 .kai.zen = KAI.ZEN
 kai.zen = KAI.ZEN

[appdefaults]
pam = {
  debug = true
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
}
```

18) Выполнить настройку Keycloak, использую главу 5.

2.4. Установка серверных приложений

В архиве Linux лежит 4 папки:
kaizen-server – основной сервер с реализацией
kaizen-notify – сервер оповещения

kaizen-proxy – прокси сервер для server sent event
kaizen-infotable – инфотабло

Для установки необходимо выполнить команды:

Создать системных пользователей для работы приложения:

```
useradd -r kaizen-server
useradd -r kaizen-notify
useradd -r kaizen-proxy
```

Установить серверную часть

```
unzip -o Linux.zip -d install
sudo cp -rf install/Linux/*/opt/* /opt
sudo cp -rf install/Linux/*/etc/systemd/system/*
/etc/systemd/system
sudo systemctl daemon-reload
```

Выдать командой chmod 777 права файлу /opt/kaizen-proxy/bin/kaizen-proxy

Включение сервиса для автостарта:

```
sudo systemctl enable kaizen-server
sudo systemctl enable kaizen-notify
sudo systemctl enable kaizen-proxy
```

Запуск сервиса:

```
sudo systemctl start kaizen-server
sudo systemctl start kaizen-notify
sudo systemctl start kaizen-proxy
```

Если сервис не может запуститься, то необходимо по расположению /etc/system/system у `kaizen-server.service и kaizen-notify.service` поменять bash на /bin/bash.

Просмотр прошедших логов:

```
journalctl -u kaizen-server
journalctl -u kaizen-notify
journalctl -u kaizen-proxy
```

Просмотр логов в реалтайме:

```
journalctl -f -u kaizen-server
journalctl -f -u kaizen-notify
journalctl -f -u kaizen-proxy
```

Настройка firewall:

```
sudo firewall-cmd --permanent --zone=public --add-
port=8081/tcp
sudo firewall-cmd --zone=public --add-port=8081/tcp
```

```
sudo firewall-cmd --permanent --zone=public --add-
port=8082/tcp
sudo firewall-cmd --zone=public --add-port=8082/tcp
sudo firewall-cmd --permanent --zone=public --add-
port=8180/tcp
sudo firewall-cmd --zone=public --add-port=8180/tcp
sudo firewall-cmd --permanent --zone=public --add-
port=80/tcp
sudo firewall-cmd --zone=public --add-port=80/tcp
```

2.5. Конфигурация серверных приложений

Файлы конфигурации хранятся по следующим путям:

Kaizen-server - /opt/kaizen-server/conf/properties.yml

Kaizen-notify - /opt/kaizen-notify/conf/properties.yml

Kaizen-proxy - /opt/kaizen-proxy/conf/properties.yml

Infotable - /opt/kaizen-infotable/conf.json

Подробная информация по настройке приложений находится в главе 4 данного руководства.

2.6. Установка nginx для раздачи статики

Создать файл `/etc/yum.repos.d/nginx.repo` с содержимым:

```
[nginx-stable]
name=nginx stable repo
baseurl=http://nginx.org/packages/centos/$releasever/$basea
rch/
gpgcheck=1
enabled=1
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true
```

Установить nginx:

```
sudo yum install nginx
```

Добавить в автозапуск и запустить:

```
sudo systemctl enable nginx
sudo systemctl start nginx
```

Изменить файл `/etc/nginx/conf.d/default.conf`

```
server {
    listen       80;
    server_name  localhost;
```

```
    location /sounds/ {
        alias /opt/kaizen-notify/sounds/;
    }

    location /infotable {
        alias /opt/kaizen-infotable/;
    }
}
```

3. Установка серверной части на Windows

3.1. Требования

Необходим сервер с Windows 7/8/10. Все компоненты «Кайдзен» кроме Keycloak можно установить на сервер с Контроллером домена. Keycloak должен быть на другом ПК, который находится в домене, чтобы корректно работал Kerberos. Все компьютеры, взаимодействующие с «Кайдзен» должны находиться в домене. Создать на контроллере домена пользователя с именем adjudge (с правами администратора) и производить настройку от его имени.

1. Для установки базы данных и Keycloak
2. Для установки трех приложений:
   2.1. Сервер для бэкенда
   2.2. Сервер для отправки уведомлений
   2.3. Прокси сервер.

3.2. Установка PostgreSQL

1. На сервер необходимо установить PostgreSQL. Скачать можно по ссылке: http://www.enterprisedb.com/postgresql-tutorial-resources-training?cid=48

2. Изменить конфигурационный файл C:\Program Files\PostgreSQL\12\data\postgresql.conf:

```
listen_addresses = 'localhost'
```

3. Изменить C:\Program Files\PostgreSQL\12\data\pg_hba.conf, прописать доступ по паролю к серверам (если такой настройки там нет):

прописать сеть, из которой приходят запросы на listen_addresses postgresql

- если сервер один то 127.0.0.1/32
- если серверов несколько (один для бд, другой для серверных приложений) то либо сеть в котором сервера 192.168.104.0/24 либо конкретный адрес сервера с маской 32: 192.168.104.14/32

```
host all all 127.0.0.1/32 md5
```

4. В консоли psql (**требуются права администратора**, запускается через Пуск-PostgreSQL 12-SQL Shell (psql)), создать пользователей и базы данных:

```
CREATE USER asusp WITH PASSWORD 'password';
CREATE USER notify WITH PASSWORD 'password';
CREATE DATABASE asusp OWNER asusp;
CREATE DATABASE notify OWNER notify;
```

Желательно заменить пароль 'password' на более защищенный.

Чтобы войти в консоль необходимо заполнить данные по умолчанию или те, которые были указаны (пароль пользователя заполнялся при регистрации):

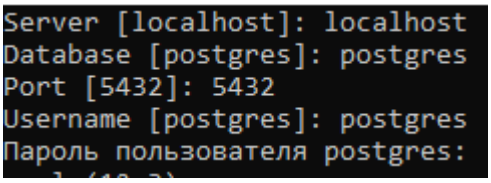

Рисунок 3 Вход в консоль postgres

После добавления пользователей и баз данных перезапустить postgresql через службы Windows (**требуются права администратора)**.

3.3. Установка Java - AdoptOpenJDK 14

Скачать можно по ссылке: https://github.com/AdoptOpenJDK/openjdk14-binaries/releases/download/jdk-14.0.1%2B7.1/OpenJDK14U-jdk_x64_windows_hotspot_14.0.1_7.msi. Во время установки при выборе дополнительных параметров нужно выбрать в списке «Set JAVA_HOME variable» и выбрать «Will be installed on local hard drive». Для установки требуются права администратора.

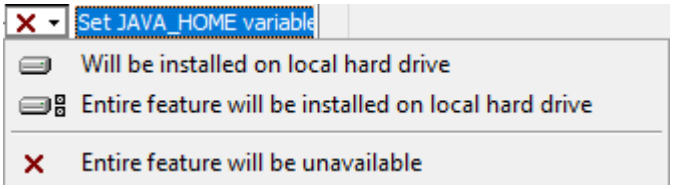

Рисунок 4 Set JAVA_HOME

3.4. Установка Keycloak

До установки приложения Kaizen-keycloak необходимо выполнить следующие действия:

1. Скопировать полученный файл krb5.keytab с контроллера домена на сервер, куда будет установлен Keycloak (как создать keytab файл см. пункт 6).
2. Запустить Kaizen-keycloak.exe на сервере и установить.

3. Создать пользователя для входа в keycloak (secret пароль). Выполнить в командной строке от имени администратора

```
"C:\Program Files\Kaizen-keycloak\bin\add-user-keycloak.bat" -r master -u admin -p secret
```

После выполнения команды перезапустить службу kaizen-keycloak. Зайти по адресу http://localhost:8080/auth/admin/master/console/ и используя данные учетной записи войти в панель администрирования.

3.5. Настройка Keycloak

Для настройки Keycloak следует обратиться к пункту 5 текущей документации.

3.4. Установка ПО Кайдзен

Установить приложения:

- kaizen-server.exe
- kaizen-notify.exe
- kaizen-proxy.exe
- kaizen-nginx.exe

Открыть порты на файерволе или отключить его:

```
8081
8082
8180
8080
80
```

Файлы конфигурации хранятся по следующим путям:

```
Kaizen-server  - C:\Program Files\Kaizen-server\conf\properties.yml

Kaizen-notify - C:\Program Files\Kaizen-notify\conf\properties.yml

Kaizen-proxy  - C:\Program Files\Kaizen-proxy\config.yaml

Infotable - C:\Program Files\Kaizen-nginx\html\infotable\conf.json
```

Подробная информация по настройке приложения находится в п.4 данного руководства.

Запускать через Службы:

- Kaizen-nginx
- Kaizen-notify

- Kaizen-proxy
- Kaizen-server

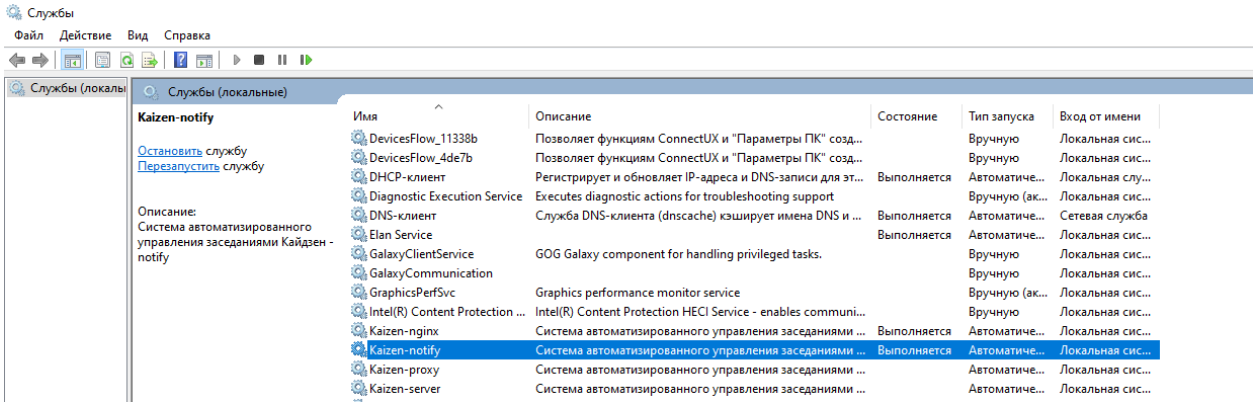

Рисунок 5 Службы Kaizen

Перед обновлением программ необходимо остановить службы

Логи хранятся в папках logs:

```
Kaizen-server  - C:\Program Files\Kaizen-server\logs
Kaizen-notify - C:\Program Files\Kaizen-notify\logs
Kaizen-proxy  - C:\Program Files\Kaizen-proxy\logs
Infotable - C:\Program Files\Kaizen-nginx\logs
```

Порядок старта служб под Windows:

1) postgresql-x64-12 — PostgreSQL Server 12
2) Kaizen-keycloak
3) Kaizen-proxy
4) Kaizen-notify
5) Kaizen-server
6) Kaizen-nginx

Для автоматического восстановления после сбоя необходимо настроить во вкладке «Восстановление» у служб «Перезапуск» в случае ошибки:

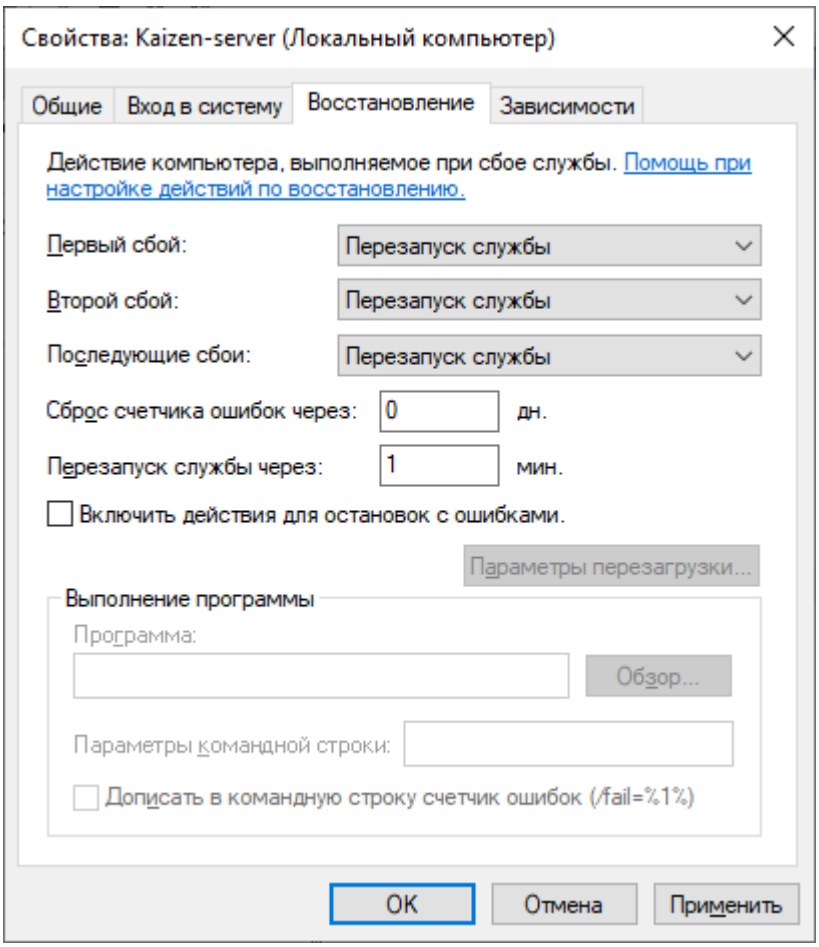

Рисунок 6 Восстановление службы

4. Конфигурация приложений

4.1. Конфигурация kaizen-server

Файл конфигурации находится по следующему пути:

- для Linux /opt/kaizen-server/conf/properties.yml
- для Windows «C:/Program Files/Kaizen-server/conf/properties.yml»

Основные параметры, необходимые для корректной работы приложения:

- api/notify/baseUrl — адрес сервера для оповещений
- aura/baseUrl — адрес сервера модуля АУРА. Если параметр пустой, то модуль отсутствует
- aura/appDir – папка приложения. Для windows - «C:/Program Files/Kaizen-server», для Linux - /opt/kaizen-server/
- spring/datasource/url — url конекта к базе данных
- spring/security/issuer-uri — uri для конекта к keycloak имя хоста должно совпадать с именем по которому подключается клиент к серверу.

```yaml
server:
  port: 8082

app:
  api:
    arbitr:
      baseUrl: "https://schedule.arbitr.ru"
      connectTimeOut: 50s
      readTimeOut: 120s
      court-tag: "FASZSO"
      writeTimeOut: 120s
    notify:
      baseUrl: "http://127.0.0.1:8081/api/v1/notification"
      connectTimeOut: 50s
      readTimeOut: 120s
      writeTimeOut: 120s
  asusp:
    async-events:
      poolSize: 20
    async-stream:
      timeOut: 180000
      poolSize: 20
    scheduler:
      enabled: true
    zone-id: "Asia/Yekaterinburg"
    notSyncBefore: "00:10:00+05:00"
  aura:
    name: "Kaizen"
    courtName: "АС Западно-Сибирского округа"
    baseUrl:
    connectTimeOut: 50s
    readTimeOut: 120s
    writeTimeOut: 120s
    soundDir: "/sounds"
    appDir: "C:/Program Files/Kaizen-server"
    delayAllowed: 10s
    recordStateDelay: 10s
    monthsToStore: 3
    numberOfAttemptsCheckRecording: 3
spring:
  datasource:
    hikari:
      connectionTimeout: 30000
      maximumPoolSize: 30
    url: jdbc:postgresql://127.0.0.1:5432/asusp
    username: asusp
    password: password
  security:
    oauth2:
      resourceserver:
        jwt:
          issuer-uri: http://keycloak.kai.zen:8080/auth/realms/KAI.ZEN
```

Рисунок 7. Конфигурация kaizen-server

4.2. Конфигурация kaizen-notify

Файл конфигурации находится по следующему пути:

- для Linux /opt/kaizen-notify/conf/properties.yml
- для Windows «C:/Program Files/Kaizen- notify/conf/properties.yml»

Основные параметры, необходимые для корректной работы приложения:

spring/datasource/url — url конекта к базе данных

app/file-directory – путь до папки со звуковыми файлами. Для windows - «C:\\Program Files\\Kaizen-nginx\\html\\sounds», для Linux - /opt/kaizen- nginx /html/sounds.

```yaml
server:
  port: 8081

spring:
  datasource:
    hikari:
      connectionTimeout: 30000
      maximumPoolSize: 20
      auto-commit: false
    url: jdbc:postgresql://127.0.0.1:5432/notify
    username: notify
    password: password

app:
  ttl-reminder-info-tablo: 120s
  ttl-reminder-client: 120s
  restart-scheduler-delay: 10s
  file-directory: "C:\\Program Files\\Kaizen-nginx\\html\\sounds"
  async-stream:
    timeOut: 180s
    poolSize: 20
```

Рисунок 8 Конфигурация kaizen-notify

4.3. Конфигурация kaizen-proxy

Файл конфигурации находится по следующему пути:

- для Linux /opt/kaizen-proxy/conf/properties.yml
- для Windows «C:/Program Files/Kaizen-proxy/conf/config.yml»

Основные параметры, необходимые для корректной работы приложения:

- long/url - url конекта к kaizen-server к long эвентам
- short/url - url конекта к kaizen-server к short эвентам
- notify/url - url конекта к kaizen-notify к эвентам.

Рисунок 9 Конфигурация kaizen-proxy

4.3. Конфигурация kaizen-infotable

Файл конфигурации находится по следующему пути:

- для Linux /opt/kaizen-infotable/conf.json
- для Windows «C:/Program Files/Kaizen-nginx/html/infotable/conf.json »

Основные параметры, необходимые для корректной работы приложения:

- countPlaySoundStartHearing - количество воспроизведений
- cardViewCount – количество заседания, отображаемых для зала на инфотабло
- serverApi - url конекта к kaizen-server
- notifyApi - url конекта к kaizen-notify
- soundFileUrl – url nginx с статикой

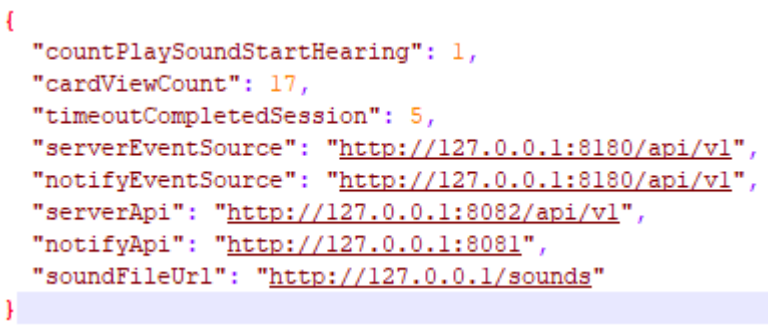

Рисунок 10 Конфигурация kaizen-infotable

5. Конфигурация Keycloak

Для настройки необходимо выполнить следующие действия:

1. Добавить новый realm и перейти к его настройке

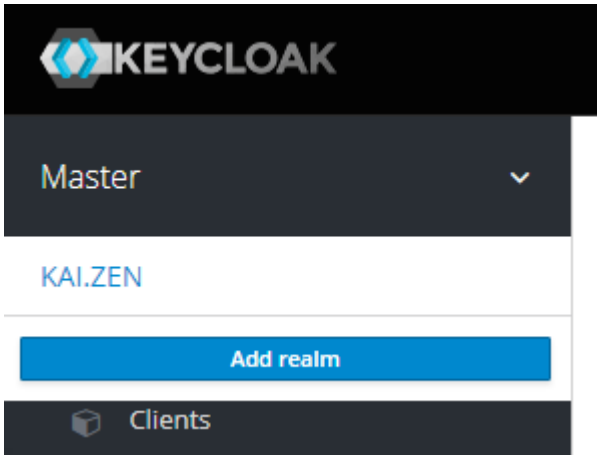

Рисунок 11 Добавление realm

2. Во вкладке «Clients» добавить нового клиента с именем «Electron»

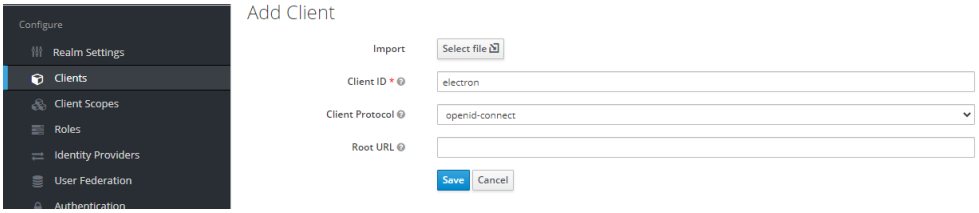

Рисунок 12 Добавление нового client

3. Заполнить форму следующим образом и нажать кнопку Save

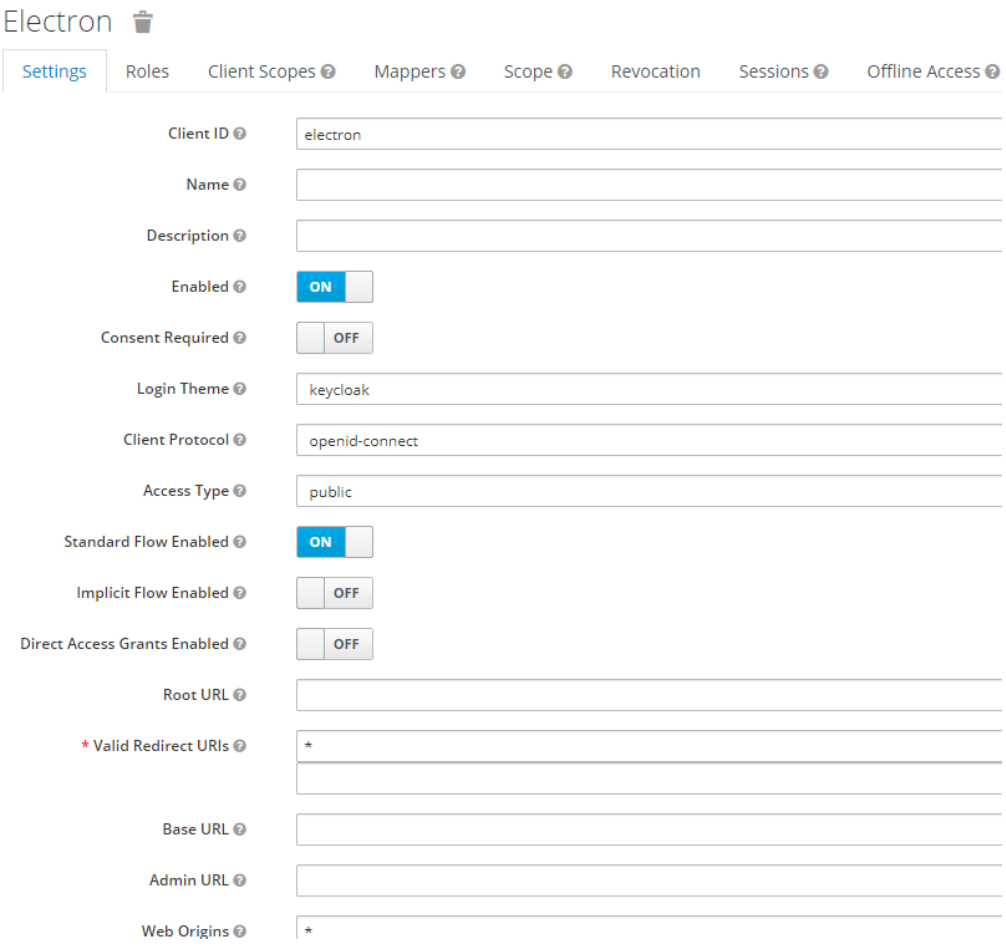

Рисунок 13 Форма Electron

4. Удалить всех клиентов, кроме electron

Рисунок 14 Удаление клиентов

5. Добавить «User Federation» с провайдером ldap

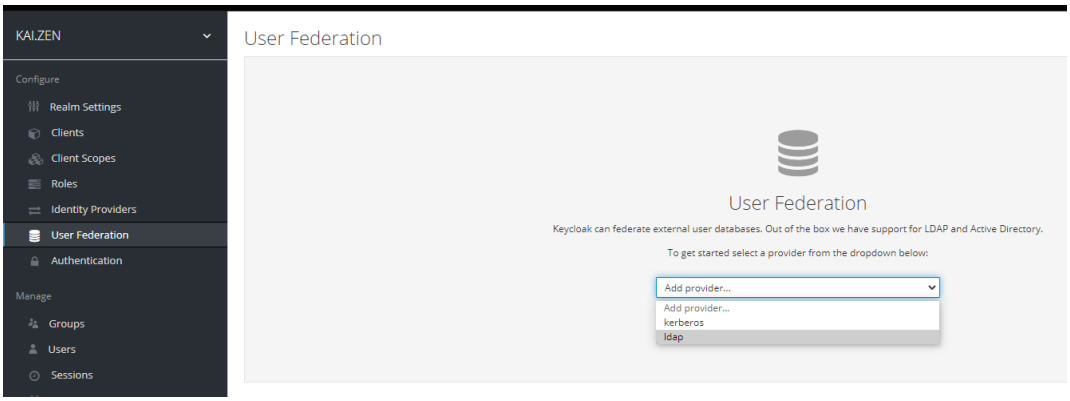

Рисунок 15 Добавление LDAP

6. Заполнить форму следующим образом:

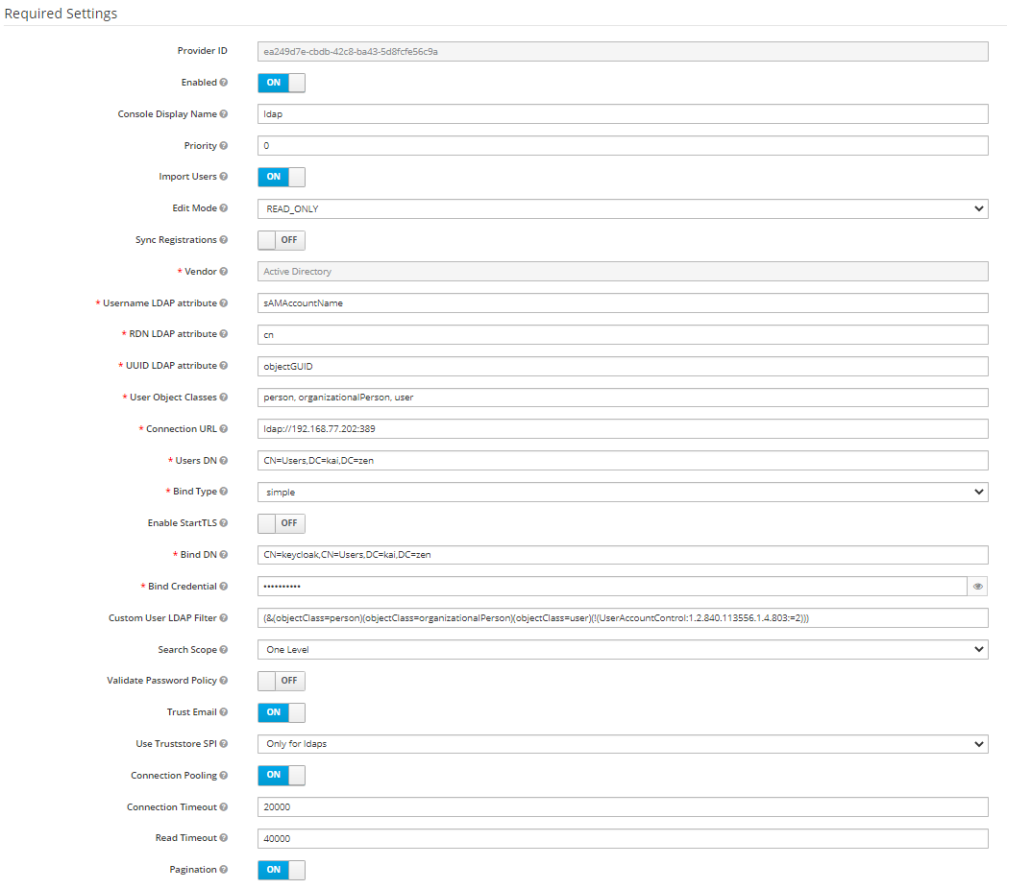

Рисунок 16 Заполнение формы LDAP

В Connection URL указать IP адрес контроллера домена. В Bind Credential записывается пароль от учетной записи Keycloak.

Заполнить информацию по Kerberos Integration. Если сервер установлен на ОС Linux, то расположение файла keytab - /etc/krb5.keytab.

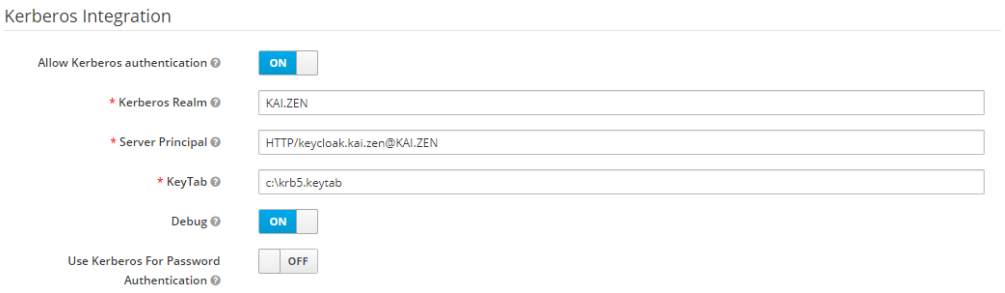

Рисунок 17 Заполнение информации по Kerberos

Настройки синхронизации

Рисунок 18 Настройка синхронизации

Проверить через Test Connection, Test autentification что настройки корректно работают и, синхронизировать список пользователей:

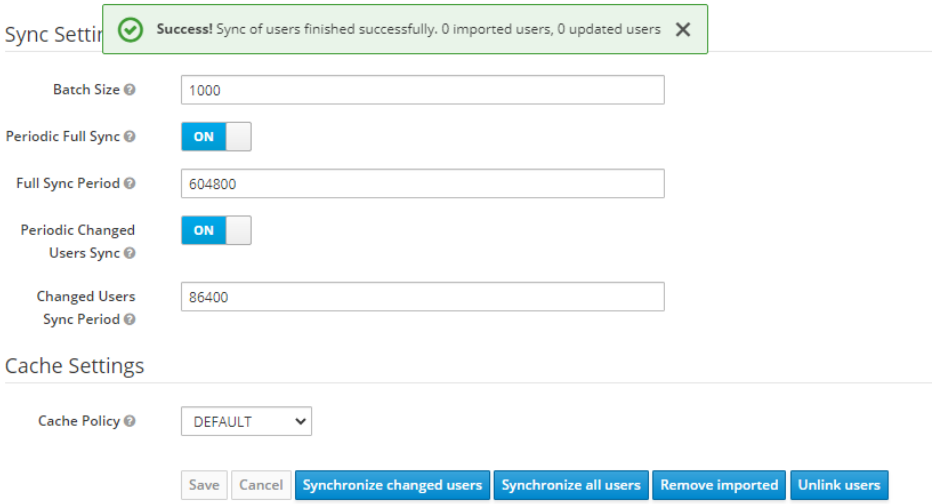

Рисунок 19 Синхронизация списка пользователей

7. Проверить, что все пользователи синхронизировались во вкладке «Users»:

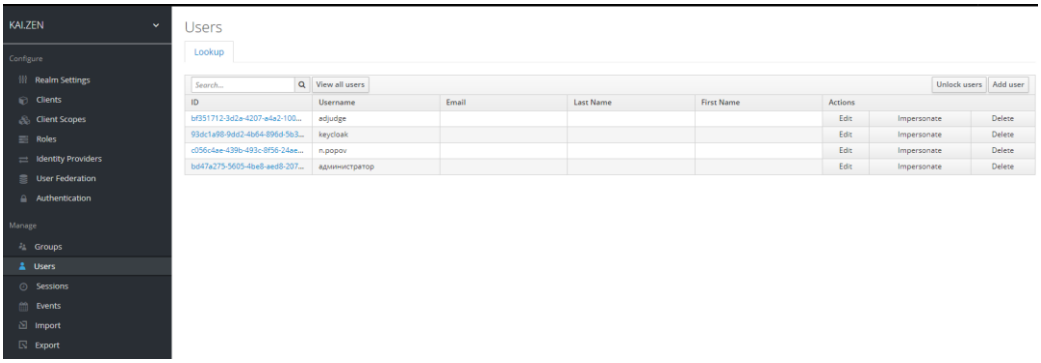

Рисунок 20 Проверка синхронизации пользователей

6. Генерация keytab файла и настройка Keycloak пользователя

1. Добавить пользователя keycloak в контроллере домена

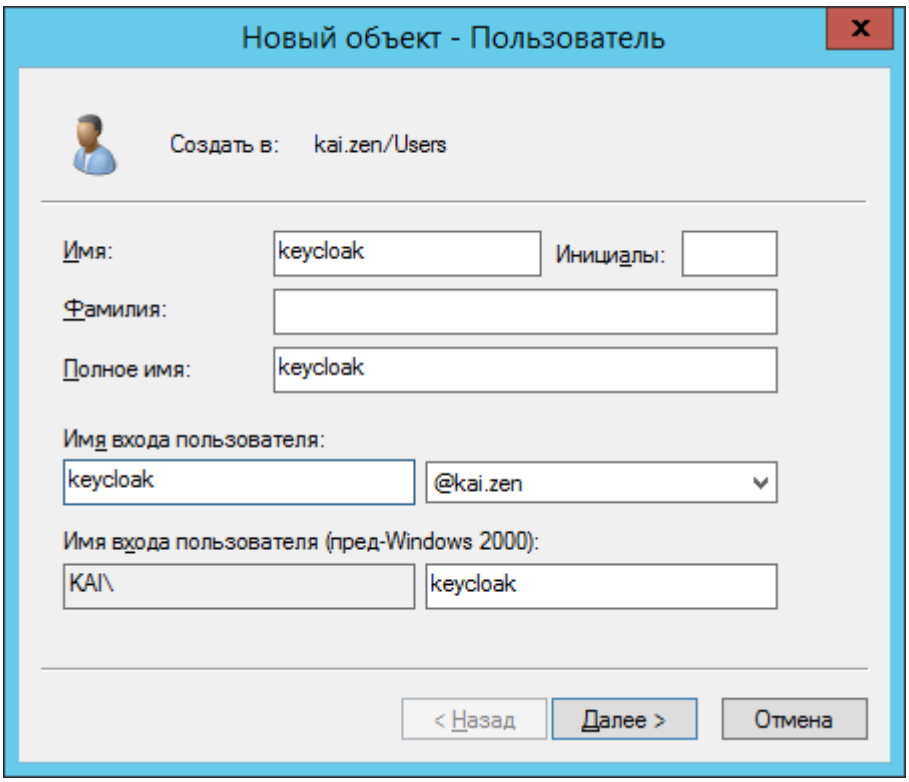

Рисунок 21 Добавление нового пользователя

2. Устанавливаем галочки «Параметры учетной записи»:

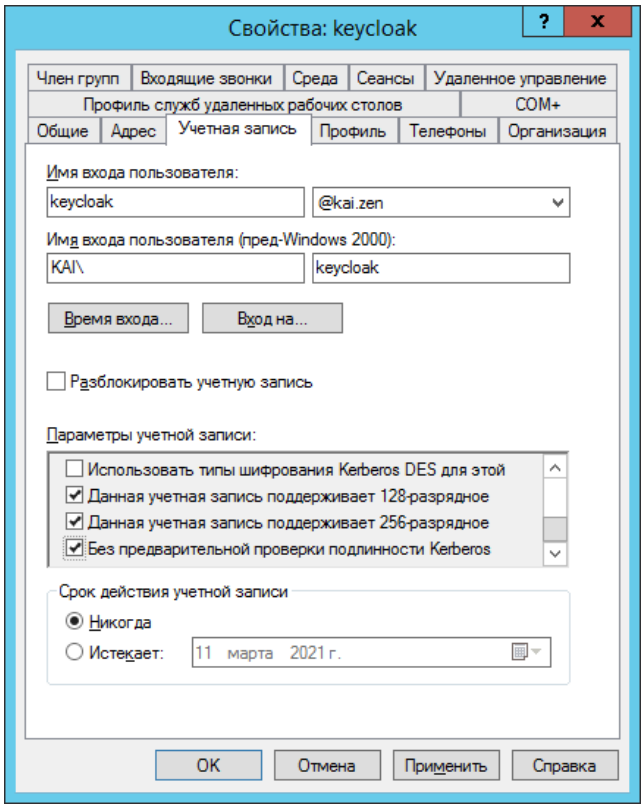

Рисунок 22 Параметры учетной записи

3. Сгенерировать на контроллере домена keytab файл командой:

```
ktpass -princ HTTP/keycloak.kai.zen@KAI.ZEN -mapuser keycloak -pass secret -ptype KRB5_NT_PRINCIPAL -crypto AES256-SHA1 -out C:\krb5.keytab
```

   Параметр –pass должен совпадать с паролем учетной записи Keycloak. @KAI.ZEN обязательно писать большими буквами.

4. Проверить групповую политику: Сетевая безопасность: настройка типов шифрования, разрешенных kerberos, должна совпадать с типами шифрования в keytab (AES256_HMAC_SHA1). Чтобы попасть в редактор, нужно в поиске Windows ввести «Изменение групповой политики» и отрыть конфигурацию.

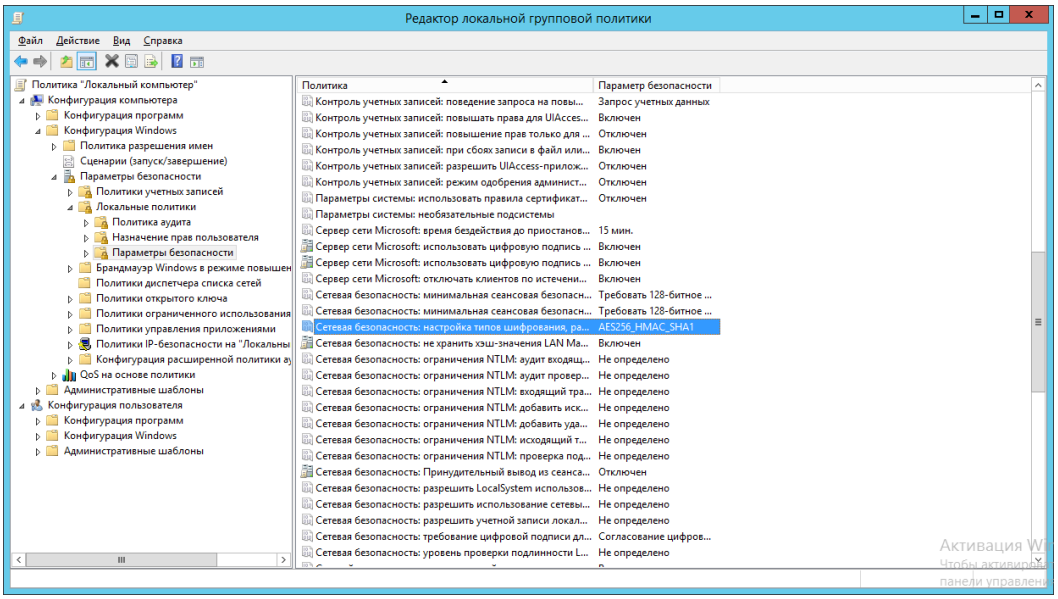

Рисунок 23 Групповая политика

5. Каждый ПК должен подключаться к серверу по адресу keycloak.kai.zen. Для этого необходимо в «Диспетчере DNS» на контроллере домена создать узел А, либо на каждом ПК прописывать в файле host следующее: 192.168.77.130 keycloak.kai.zen (где ip-адрес это адрес сервера с keycloak)

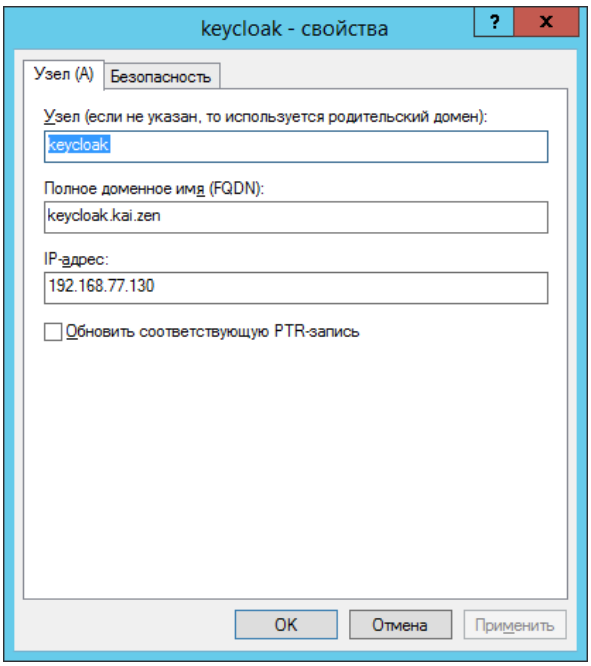

Рисунок 24 Создание узла A.