

Мессенджер и ВКС

Интеграция с контроллером домена по протоколу LDAP

Назначение документа	3
Управление параметрами синхронизации LDAP	4
Добавить новое LDAP-подключение	4
Удалить LDAP-подключение	5
Получить список LDAP-серверов	6
Обновить LDAP-сервер	6
Настроить синхронизацию LDAP-сервера	6
Получить информацию о текущем состоянии сервиса Keycloak	6

Назначение документа

В данной инструкции представлена информация по управлению параметрами синхронизации LDAP.

Документ предназначен для использования администраторами организации.

Управление параметрами синхронизации LDAP

LDAP-подключения создаются либо в GUI Keycloak, либо конфигурационным файлом **/usr/local/etc/premsetup/ldap/ldap.yaml**.

Для управления подключениями используется либо GUI Keycloak, либо утилита `kccli`.

Если LDAP-подключение редактируется в GUI Keycloak, то файл конфигурации **/usr/local/etc/premsetup/ldap/ldap.yaml** должен быть приведен в соответствие внесенным изменениям, чтобы при обновлении сервера подтянулись сертификаты LDAP.

Добавить новое LDAP-подключение

Если необходимо добавить LDAP-подключение, а не удалить или модифицировать, то необходимо:

1. Скопировать дополнительный CA-сертификат в каталог **/usr/local/etc/premsetup/ldap**. Сертификат должен быть PEM-кодированным X.509 сертификатом с расширением `.pem`.



Примечание

При добавлении нешифрованного канала цепочка сертификатов не требуется.

2. Выполнить `im_deployer -t`.

Пропустите этот шаг при добавлении нешифрованного канала.

3. Если ошибок при проверке нет, выполнить:

```
rm -f /var/tmp/premsetup.run && im_deployer --install -m ldap
```

При добавлении зашифрованного канала выполнится добавление нового CA-сертификата.

4. Через несколько минут после добавления сертификата можно добавлять новый LDAP-сервер.

Создайте файл `.yaml`, в котором пропишите конфигурацию нового LDAP-сервера.

Пример настройки LDAP-сервера в файле `.yaml`:

```
name: onpremise
config:
  connectionUrl: "ldaps://ad.ad.on-premise.ru:636" //при добавлении зашифрованного канала
  connectionUrl: "ldap://ad.ad.on-premise.ru:389" //при добавлении нешифрованного канала
  usersDn: "OU=ad,DC=ad,DC=onpremise,DC=ru"
  bindDn: "CN=VKTeams Syncer,CN=Users,DC=ad,DC=onpremise,DC=ru"
  bindCredential: "PASSWORD"
  searchScope: 1
```

```
fullSyncPeriod: 600
changedSyncPeriod: -1
```

В случае если одно из полей не заполнено, то устанавливается значение по умолчанию для сервиса Keycloak.

Основные доступные поля:

- **name** — имя LDAP-сервера. Данное имя уникально, может быть заведен только один сервер с определенным именем.
- **connectionUrl** — адрес подключения к LDAP-серверу.
- **usersDn** — указание на точку входа для поиска в LDAP.
- **bindDn** — пользователь, под которым осуществляется подключение к LDAP-серверу.
- **bindCredential** — пароль для подключения к LDAP-серверу.
- **searchScope** — использование рекурсивного поиска по дереву LDAP:
 - 1 — искать в одном уровне (по умолчанию);
 - 2 — искать по всем уровням.
- **fullSyncPeriod** — частота полной синхронизации с LDAP-сервером, в секундах.
- **changedSyncPeriod** — частота частичной синхронизации с LDAP-сервером, в секундах (значение **-1** — отключить).
- **batchSizeForSync** — максимальное количество пользователей, обновляемых одной транзакцией. Изменяйте в случае, если ваш LDAP-сервер отказывается отдавать пользователей с ошибкой о превышении размера транзакции.
- **customUserSearchFilter** — фильтр для получения пользователей. Позволяет получать не всех пользователей из указанного дерева. По умолчанию выборка пользователей не ограничена.

Скопируйте созданный файл `.yaml` с конфигурацией нового сервера в `/usr/local/etc/premsetup/ldap/`.

1. Запустить `im_deployer -t`.
2. Если тестирование завершилось без ошибок, выполнить команду:

```
rm -f /var/tmp/premsetup.run && im_deployer --install -m ldap
```

Удалить LDAP-подключение

Для удаления используйте:

```
>kcccli ldap delete --name <имя вашего LDAP сервера> //удаление по имени
>kcccli ldap delete --id <id вашего LDAP сервера> //удаление по ID
```

Используйте удаление по ID в случае, если ранее было заведено несколько LDAP-серверов с неуникальными именами. Получить ID подключений можно, выполнив команду:

```
kccli ldap get
```

Получить список LDAP-серверов

Для вывода полного списка LDAP-серверов выполните:

```
kccli ldap get
```

Обновить LDAP-сервер

1. Обновите файл `.yaml`, находящийся в `/usr/local/etc/premsetup/ldap/`.
2. Выполните команду:

```
kccli ldap update -f /usr/local/etc/premsetup/ldap/ldap.yaml
```

Можно использовать дополнительные фильтры `--name` и `--id`.

Настроить синхронизацию LDAP-сервера

Синхронизация всех серверов:

```
kccli ldap sync
```

Синхронизация одного сервера:

```
kccli ldap sync --name <имя подключения>
```

Получить информацию о текущем состоянии сервиса Keycloak

```
kccli server info
```

```
>kccli server info
2022-07-25T14:40:37+03:00 INF SystemInfo: {
  "fileEncoding": "UTF-8",
  "javaHome": "/usr/lib/jvm/java-17-openjdk-17.0.3.0.7-2.el8_6.x86_64",
  "javaRuntime": "OpenJDK Runtime Environment",
  "javaVendor": "Red Hat, Inc.",
  "javaVersion": "17.0.3",
  "javaVm": "OpenJDK 64-Bit Server VM",
  "javaVmVersion": "17.0.3+7-LTS",
  "osArchitecture": "amd64",
  "osName": "Linux",
  "osVersion": "5.16.14-1.el7.elrepo.x86_64",
  "serverTime": "Mon Jul 25 14:40:37 MSK 2022",
  "uptime": "2 days, 18 hours, 41 minutes, 21 seconds",
  "uptimeMillis": 240081852,
  "userDir": "/",
  "userLocale": "us_EN",
  "userName": "keycloak",
  "userTimezone": "Europe/Moscow",
  "version": "18.0.2"
}
```

kccli server memory

```
>kccli server memory
2022-07-25T14:41:27+03:00 INF MemoryInfo: {
  "free": 460703232,
  "freeFormatted": "439 MB",
  "freePercentage": 88,
  "total": 518979584,
  "totalFormatted": "494 MB",
  "used": 58276352,
  "usedFormatted": "55 MB"
}
```

 Технический писатель: Белова Ирина

 26 ноября 2025 г.