

Выгрузка LDAP информации в словарь KUMA

Предварительно нужно выполнить настройку обогащения по этой статье
<https://kb.kuma-community.ru/books/integracii/page/ldap-obogashhenie>

Шаг 1.

Нам нужно выгрузить сопоставление, например login(sAMAccountName)-mail. Создаете словарь типа таблица (важно), ключ login, колонка mail. Добавляете одну запись любую, чтобы сохранить словарь можно было.

[Словари](#) >
Изменить словарь

*Название

*Тенант

Описание

Описание

*Тип

*Значения Всего: 1

login

mail

+

login_test

mail_test

+

Если нужно выгрузить другое поле, посмотрите его название по примеру вывода одной записи из обогащения:

```
/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.findOne({"archived":false})"
```

Шаг 2.

Выбираете пользователя в KUMA, даете ему права на запрос POST /dictionaries/update, генерируете токен и записываете себе куда-нибудь (например в блокнот).

Шаг 3.

На коре выполняете скрипт (нужно поставить утилиту jq):

```
echo 'login,mail' > /tmp/accounts.csv; /opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --eval
'DBQuery.shellBatchSize=<SIZE>; db.accounts.find({"archived":false},{ "displayName":1,
"sAMAccountName":1, "_id":0})' | grep -E '^{' | jq '.sAMAccountName,.displayName' | sed 'N;s/\n/,/' | sed 's/\n//g'
>> /tmp/accounts.csv; curl -k --request POST
'https://<KUMA_IP>:7223/api/v1/dictionaries/update?dictionaryID=<DICTIONARY_ID>' --header 'Content-Type:
multipart/form-data' --header 'Authorization: Bearer <TOKEN>' --form 'file=@"/tmp/accounts.csv"; rm -rf
/tmp/accounts.csv'
```

- где **<SIZE>** - число записей в выводе, нужно ставить значение кол-во пользователей*1.1
/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval
"db.accounts.find({"archived":false},{ "displayName":1, "sAMAccountName":1, "_id":0}).count()" полученное число умножить на 1.1 Или сразу посчитать с помощью: perl -w -e "use POSIX; print ceil(\$(/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.find({"archived":false},{ "displayName":1, "sAMAccountName":1, "_id":0}).count()")*1.1), qq{\n}"
- **<KUMA_IP>** - ip-адрес ядра KUMA
- **<DICTIONARY_ID>** - id словаря, можно скопировать из строки браузера, если зайти в словарь
- **<TOKEN>** - токен для доступа к API, скопированный на Шаге 2.

После выполнения скрипта, в словарь запишутся логины и их электронная почта, импортированные из AD.

Более продвинутый заполненный запрос с автоподсчетом **<SIZE>**:

```
SIZE=$(perl -w -e "use POSIX; print ceil($(/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval 'db.accounts.find({'archived':false},{\"sAMAccountName\":1, \"mail\":1, \"_id\":0}).count()\")*1.1), qq{\\n}");
echo 'login,mail' > /tmp/accounts.csv; /opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --eval
'DBQuery.shellBatchSize='$SIZE'; db.accounts.find({'archived':false},{\"sAMAccountName\":1, \"mail\":1,
\"_id\":0}))' | grep -E '^{' | jq '.sAMAccountName,.mail' | sed 'N;s\\n/,/' | sed 's\\/\\/g' >> /tmp/accounts.csv; curl -k --
request POST 'https://10.68.85.125:7223/api/v1/dictionaries/update?dictionaryID=72323930-c4fb-43c7-9360-
5f8d5d929bbb' --header 'Content-Type: multipart/form-data' --header 'Authorization: Bearer
29ed4e42e25f7877c5ceb435736f860f' --form 'file=@"/tmp/accounts.csv"; rm -rf /tmp/accounts.csv
```

Revision #4

Created 1 November 2023 11:05:39 by Boris RZR

Updated 19 July 2024 14:37:44 by Koala