Локальная база пользователей и интеграция с серверами каталогов

Локальная база пользователей

Интеграция с серверами каталогов

Содержание

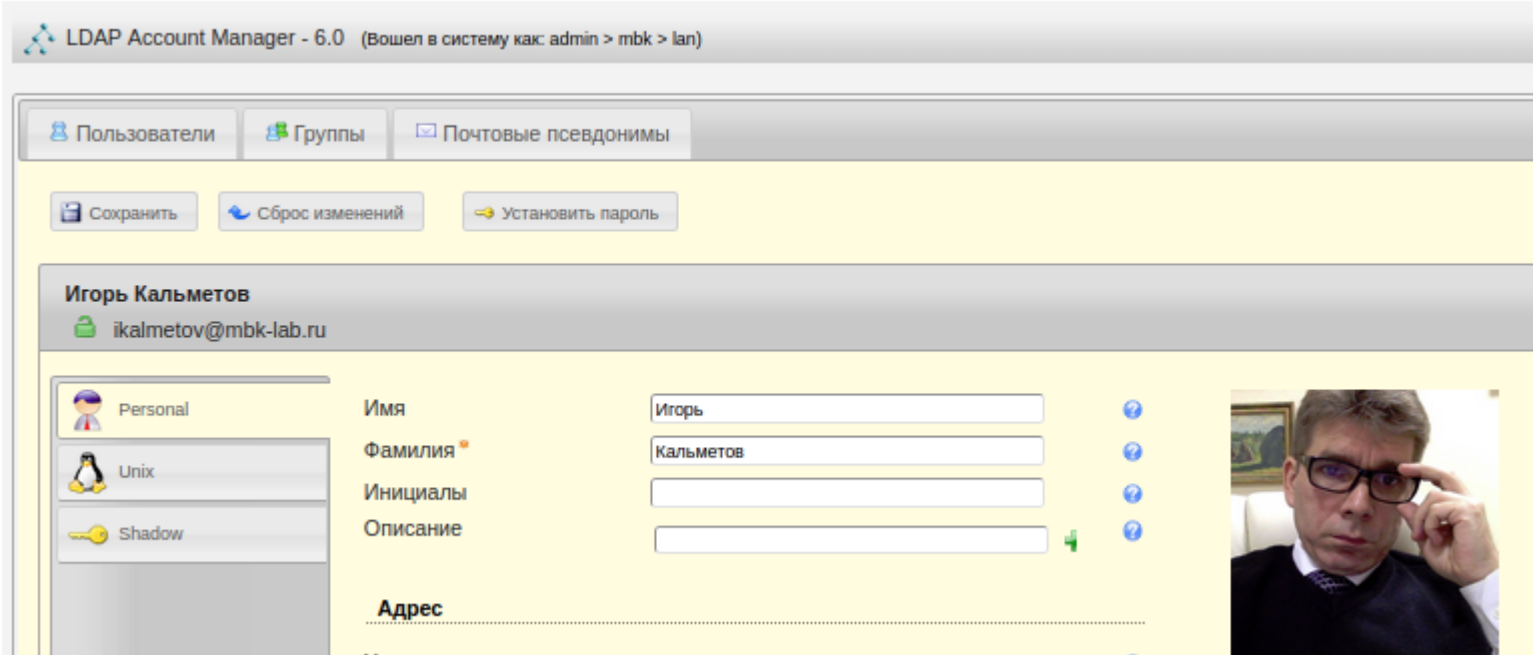
Перед настройкой **Провайдера БД пользователей** проверьте, что вы создали **Хранилище почты** для целевого домена. В противном случае серверу негде создавать почтовй ящики. Конфигурация без хранилища может быть использована только для настройки релея.

Почтовый сервер Tegu, начиная с редакции Professional и выше поддерживает любое количество подключений к серверам каталогов LDAP версии 3 (в эту же категорию попадает и популярный Windows Active Directory).

На что надо обратить внимание. Унификация подключений неизбежно влечет к некоторой кажущейся сложности.
К примеру, для работы сервера необходимо задать не только дефолтный, но и персональный размер почтового ящика. Но в стандартной LDAP-схеме такого поля нет. Конечно, мы можем это поле создать, но тогда наша схема будет отличаться от стандартной и неизвестно что именно повлечет за собой такое изменение.
Мы предлагаем компромиссное решение - например, использовать уже существующее, но заведомо неиспользуемое поле, к примеру "Номер факса".

Другими словами, мы оставляем за вами выбор механизма: создать или использовать существующее, важно понимать, что почтовому серверу необходимо явно объяснить какое поле как именно трактовать.

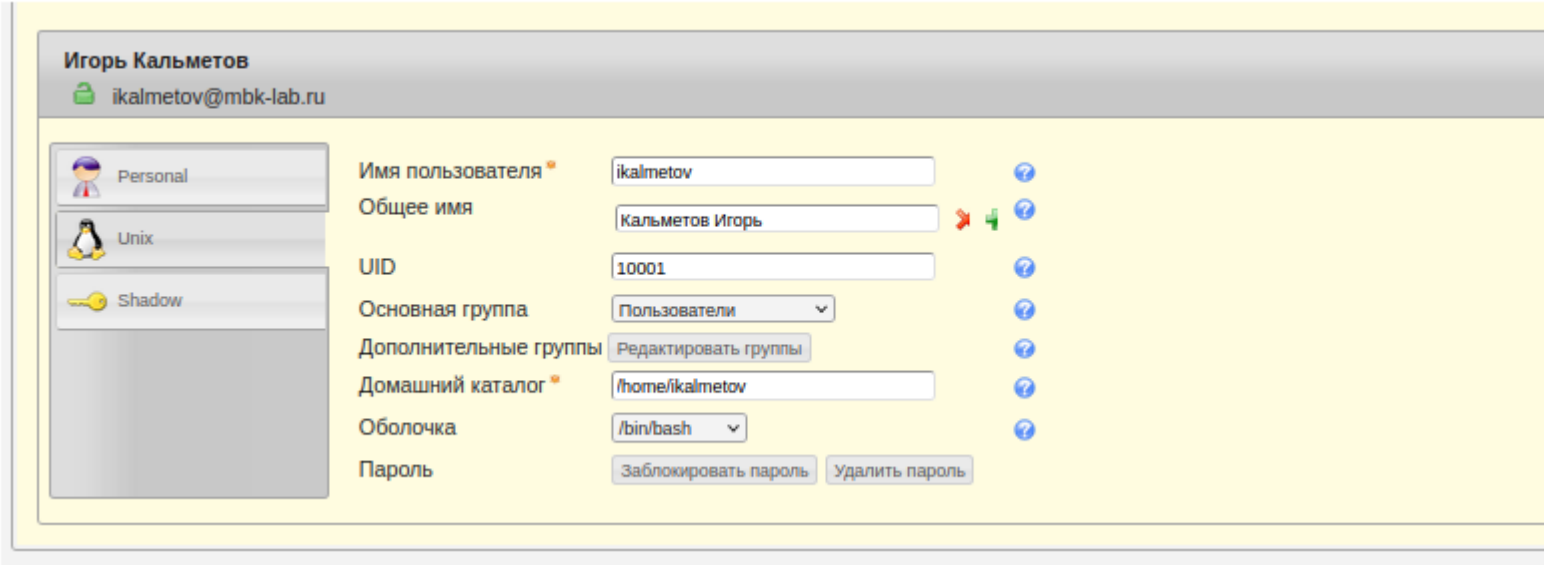
Рассмотрим учетную запись на картинке:



Обратите внимание:

- В поле **Адрес электронной почты** внесен email-адрес пользователя (это ключевое поле);
- В поле **Номер факса** внесена квота почтового ящика в Mb.

На следующей картинке мы видим логин указанного пользователя:



Далее перейдем на консоль почтового сервера и в командной строке проверим правильность будущего подключения.
Для этого нам потребуется утилита **ldapsearch** .
Если у вас нет утилиты, то установите пакет **ldap-utils** примерно такой командой:

```
sudo apt install ldap-utils
```

Синопсис команды:

```
ldapsearch -x -b <search_base> -H <ldap_host> -D <bind_dn> -W
```

В моем случае для подключения к LDAP получается следующая команда:

```
ldapsearch -x -b "DC=mbk,DC=lan" -H ldap://ldap.mbk-lab.ru:389
```

Вывод команды весьма интересен и многое говорит сам за себя.
Но мы с вами запросим информацию о конкретном пользователей **uid=ikalmetov** :

```
$ ldapsearch -x -b "uid=ikalmetov,ou=People,DC=mbk,DC=lan" -H ldap://ldap.mbk-lab.ru:389
# extended LDIF
#
# LDAPv3
# base <uid=ikalmetov,ou=People,DC=mbk,DC=lan> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ikalmetov, People, mbk.lan
dn: uid=ikalmetov,ou=People,dc=mbk,dc=lan
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
homeDirectory: /home/ikalmetov
loginShell: /bin/bash
uid: ikalmetov
uidNumber: 10001
gidNumber: 10000
title:: 0JjQvdC20LXQvdC10YA=
o:: 0JzQkdCaLdCb0LDQsQ==
mail: ikalmetov@mbk-lab.ru
sn:: 0JrQsNC70YzQvNC10YLQvtCy
givenName:: 0JjQs9C+0YDRjA==
cn:: 0JrQsNC70YzQvNC10YLQvtCyINCY0LPQvtGA0Yw=
jpegPhoto:: /9j/4AAQSkZJRgABAQAASABIAAD/7QByUGhvdG9zaG9wIDMuMAA4QklNBAQAAAAAAD
 ocAVoAAxslRxwCAAACAAIcAigAFm0zTXV6VDhMVHNHQ0JLWCUwc0t4MEEcAhkAC1Bob3RvIEJvb3R
 Bh479yI1rrF7bn/9k=
facsimileTelephoneNumber: 10000

# search result
search: 2
```

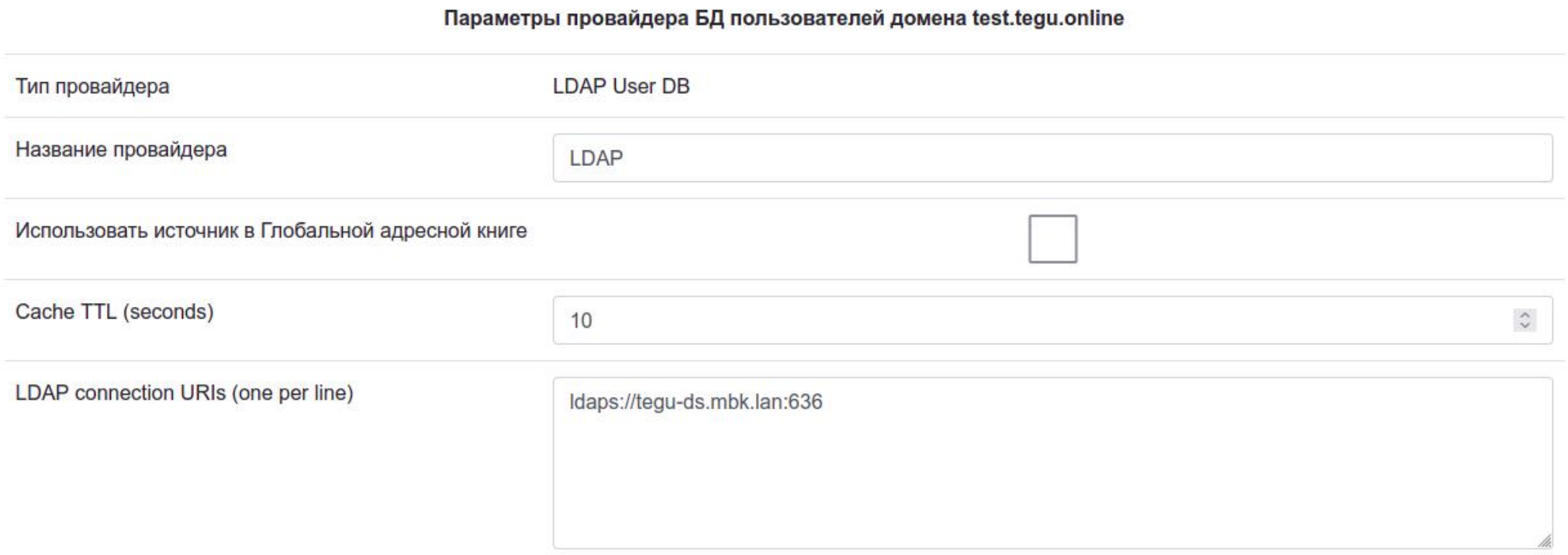
```
result: 0 Success

# numResponses: 2
# numEntries: 1
```

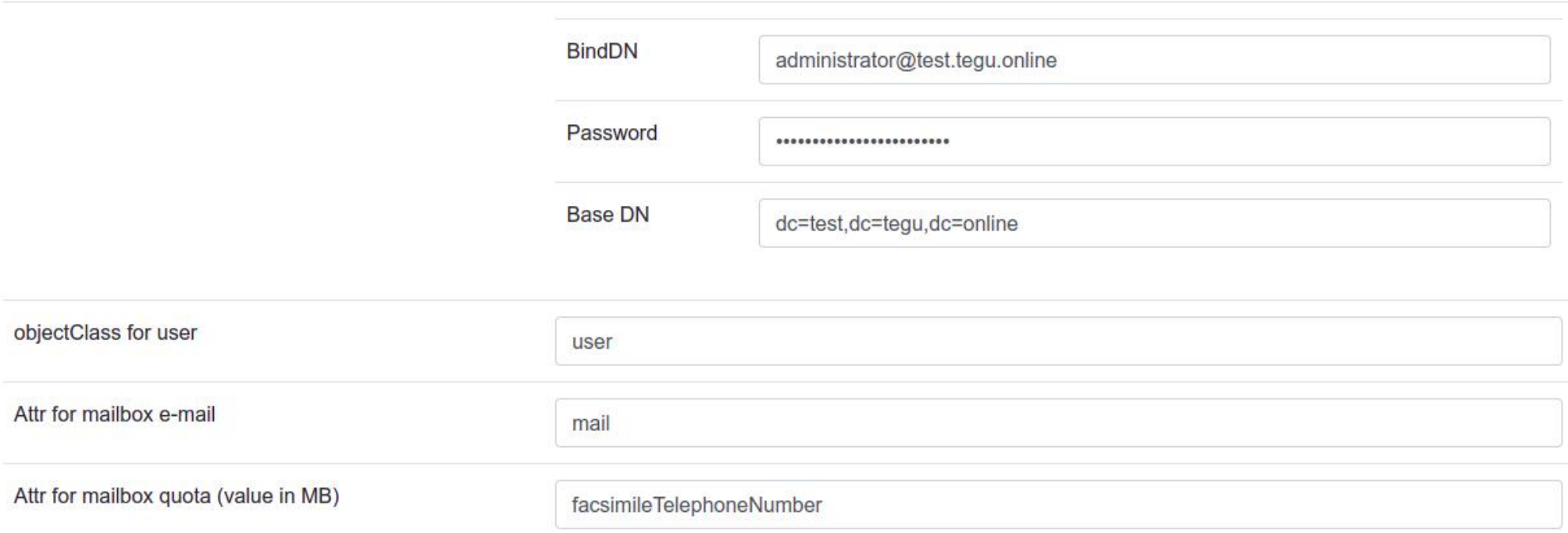
Как трактовать этот вывод?

- Почтовый сервер может обратиться к LDAP серверу **ldap://ldap.mbk-lab.ru:389** с логином **BindDN: cn=admin,dc=mbk,dc=lan** и вашим паролем;
- Определена область поиска **BaseDNdc=mbk,dc=lan** ;
- Определено поле **Attr for mailbox e-mail** = mail ;
- Определено поле **Attr for mailbox quota (value in MB)** = facsimileTelephoneNumber .

Теперь переходим к настройке Провайдера БД пользователей в административном интерфейсе Tegu.

- Поле **Provider Name** - любой текст, означающий имя подключения;
- **Local Domain Name** - имя домена (а не сервера т.е. то, что в email-адресе следует после @);
- **LDAP server connection URI** - найденный и проверенный выше пусть к серверу;
- **BindDN** - логин;
- **Password** - пароль;
- **BaseDN** - найденный выше фильтр поиска.;
- **Atr for mailbox e-mail** - название поля, которое в LDAP заполнено email-адресом пользователя (важно! с доменным суффиксом);
- **Atr for mailbox quota** - название поля, которое в LDAP используется для определения квоты.





На этом настройка интеграции с серверов каталогов завершена.

Проверка подключения

Вы можете проверить правильность сделанных настроек в диалоге настройки.
Для этого введите в поле "Email пользователя LDAP для проверки подключения" адрес любого из созданных на сервере каталогов пользователей и нажмите кнопку "Проверить подключение".
Вы получите статус:

- Проверка пройдена на зеленом фоне в случае правильных настроек;
- Сообщение "no user with this email" на краном фоне - в случаях если подключение настроено неправильно, либо такого пользователя на сервере каталогов нет.