

# Локальная база пользователей и интеграция с серверами каталогов

## Локальная база пользователей

## Интеграция с серверами каталогов

Перед настройкой **Провайдера БД пользователей** проверьте, что вы создали **Хранилище почты** для целевого домена. В противном случае серверу негде создавать почтовый 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:

The screenshot shows the LDAP Account Manager 6.0 web interface. At the top, it says "LDAP Account Manager - 6.0 (Вошел в систему как: admin > mbk > lan)". Below this is a navigation bar with tabs for "Пользователи", "Группы", and "Почтовые псевдонимы". Under the "Пользователи" tab, there are buttons for "Сохранить", "Сброс изменений", and "Установить пароль". The main content area displays the profile for "Игорь Кальметов" with the email "ikalmetov@mbk-lab.ru". On the left, there are tabs for "Personal", "Unix", and "Shadow". The "Personal" tab is active, showing fields for "Имя" (Igor), "Фамилия" (Kalyetov), "Инициалы", and "Описание". There are also fields for "Адрес" and a small photo of a man with glasses.

### Содержание

Локальная база пользователей и интеграция с серверами каталогов  
Локальная база пользователей  
Интеграция с серверами каталогов  
Проверка подключения

Улица	<input type="text"/>	✚	?	Удалить фото
<b>Контактные данные</b>				
Телефонный номер	<input type="text"/>	✚	?	
Домашний телефон	<input type="text"/>	✚	?	
Мобильный телефон	<input type="text"/>	✚	?	
Номер факса	10000	✖	✚	?
Адрес электронной почты	ikalmetov@mbk-lab.ru	✖	✚	?
Веб сайт	<input type="text"/>	✚	?	

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:

**Игорь Кальметов**  
ikalmetov@mbk-lab.ru

Personal	Имя пользователя *	ikalmetov	?
Unix	Общее имя	Кальметов Игорь	✖ ✚ ?
Shadow	UID	10001	?
	Основная группа	Пользователи	?
	Дополнительные группы	Редактировать группы	?
	Домашний каталог *	/home/ikalmetov	?
	Оболочка	/bin/bash	?
	Пароль	Заблокировать пароль Удалить пароль	

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
```

Синописис 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 пользователе **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/4AAQSkZJRgABAQASABIAAD/7QByUGhvdG9zaG9wIDMuMAA4Qk1NBAQAAAAAAD
ocAVoAAxs1RxwCAAACAAIcAigAFm0zTXV6VDhMVHNHQ0JLWCUwc0t4MEEcAhkAC1Bob3RvIEJvb3R
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.

#### Параметры провайдера БД пользователей домена test.tegu.online

Тип провайдера

LDAP User DB

Название провайдера

LDAP

Использовать источник в Глобальной адресной книге

☐

Cache TTL (seconds)

10

LDAP connection URIs (one per line)

ldaps://tegu-ds.mbk.lan:636

BindDN	<input type="text" value="administrator@test.tegu.online"/>
Password	<input type="password" value="....."/>
Base DN	<input type="text" value="dc=test,dc=tegu,dc=online"/>
objectClass for user	<input type="text" value="user"/>
Attr for mailbox e-mail	<input type="text" value="mail"/>
Attr for mailbox quota (value in MB)	<input type="text" value="facsimileTelephoneNumber"/>

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 красном фоне - в случаях если подключение настроено неправильно, либо такого пользователя на сервере каталогов нет.

Email для проверки подключения	<input type="text" value="monica@tegu.online"/>
	<input type="button" value="Проверить подключение"/>
	<input type="button" value="Обновить"/>

