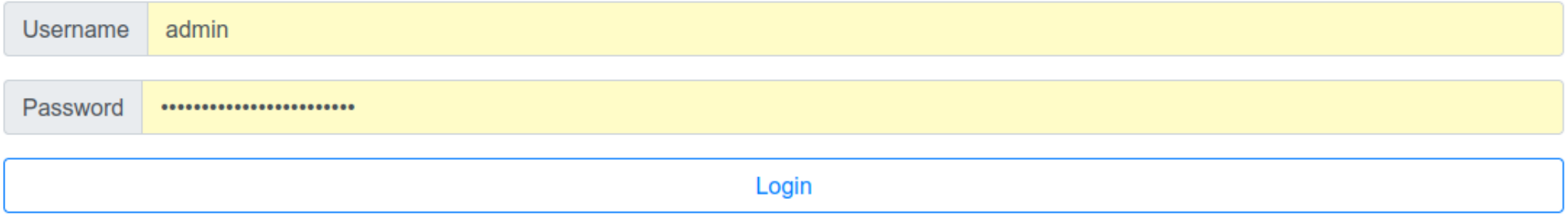
Начальная настройка сервера

Если все предыдущие шаги выполнены правильно, то вам становится доступной веб-панель администрирования сервером, в которой производятся все остальные настройки.

С помощью браузера зайдите на порт 8888 сервера (например, http://127.0.0.1:8888) и авторизуйтесь под администратором (логин admin) с паролем, указанным в конфиге в параметре adminPassword.

Для работы с https используйте порт 9999 (например, https://127.0.0.1:9999).

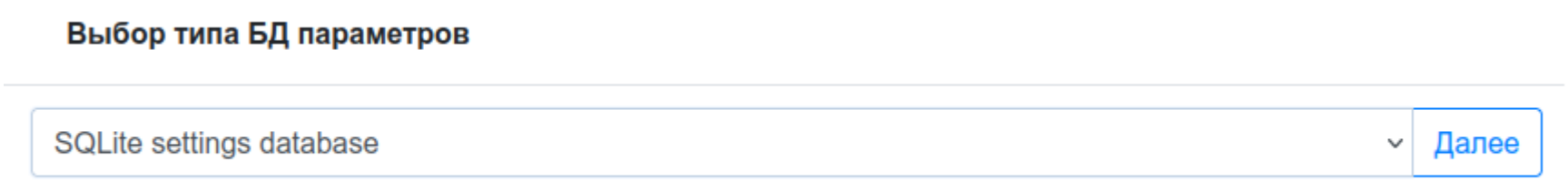
Содержание



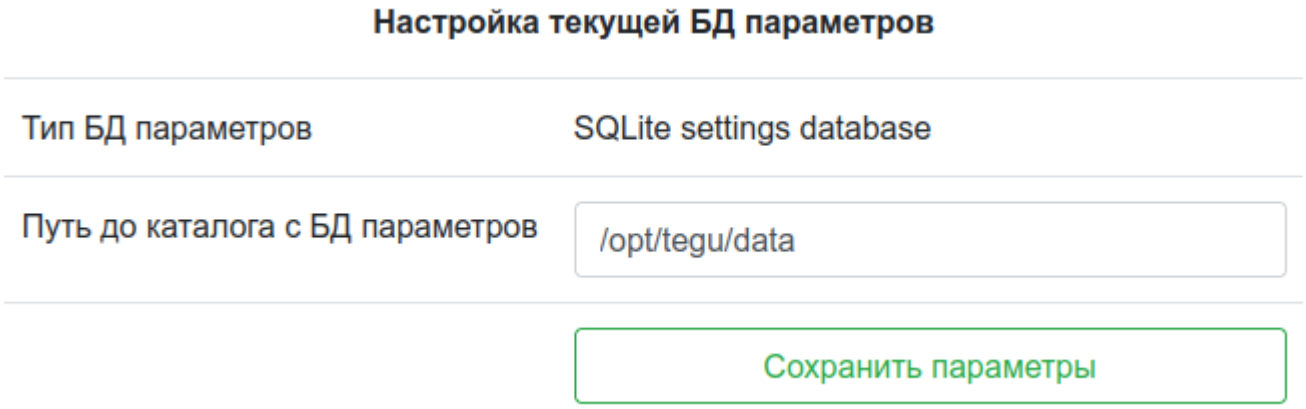
При первом запуске административного интерфейса вам будет предложено выбрать место хранения конфигурации:

- Вы можете выбрать SQLite setings database для версии FreeWare или Professional (локальная база);
- Либо PosgresSQL для версии Enterprise.

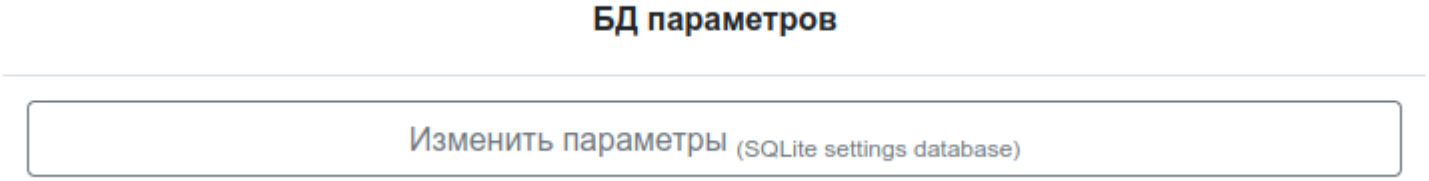
или



Сохраните введенные данные и сохраните параметры.

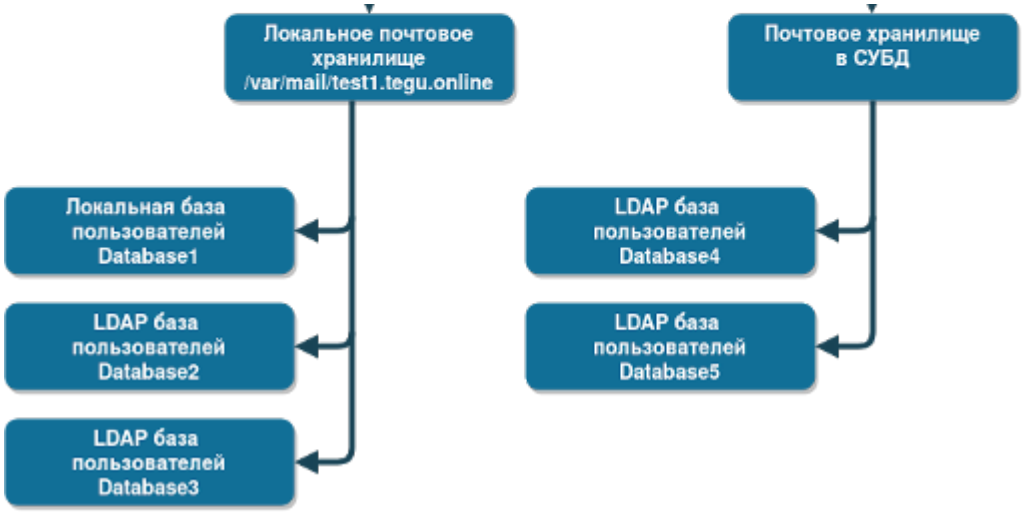


Сервер создаст файл конфигурации по указанному вами пути. Отредактируйте эти настройки или нажмите Назад для выхода в корневое меню.



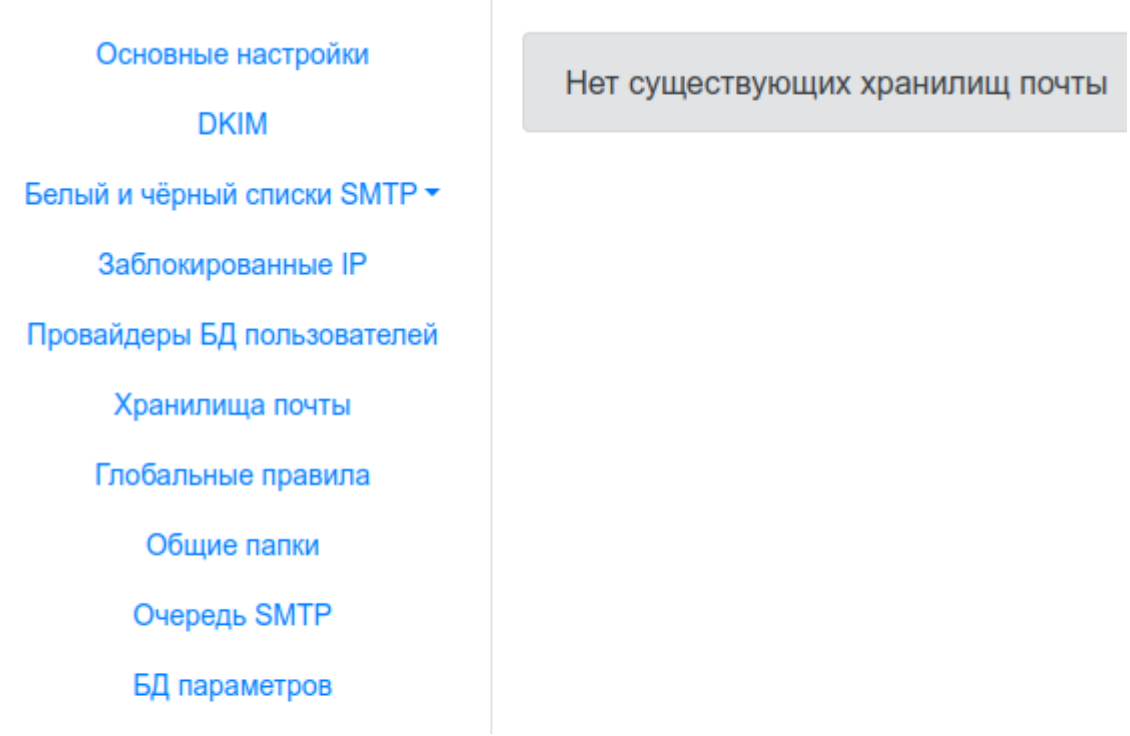
Вы вошли в корневое меню управления сервером.

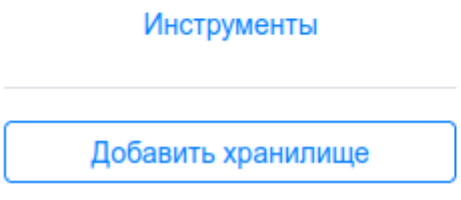
Взаимосвязь объектов сервера и последовательность настройки вам поможет понять следующая условная диаграмма.



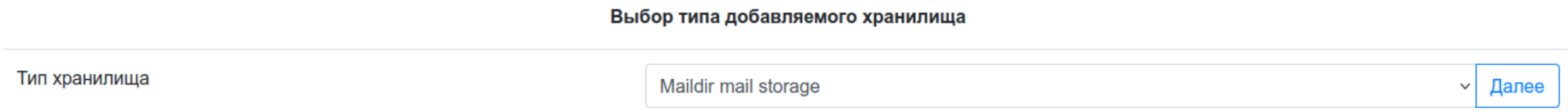
Создание почтового хранилища Maildir

Приступаем к созданию хранилищ почты. Для этого выбираем пункт меню **Хранилища почты**.

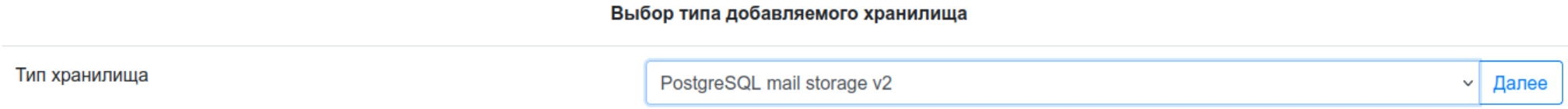




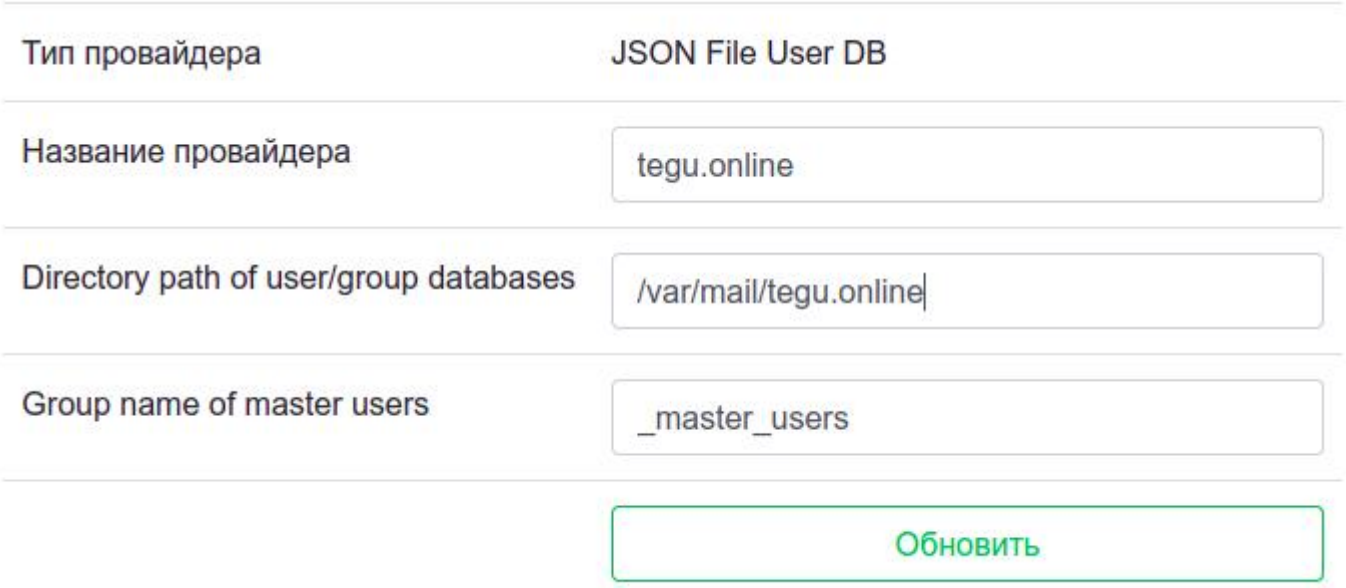
На данном этапе необходимо выбрать тип хранилища.



или



Выбрав "Maildir storage" вы можете создать локальное хранилище.



Обратите внимание, что при создании хранилища maildir соответствующий каталог должен быть предварительно создан с правами RW для пользователя mail.

Права на катологи должны быть такими:

```
drwxr-x---
```

Выполним это с помощью команд:

```
$ mkdir /var/mail/tegu.online
```

Права на файлы должны быть такими:

```
-rw-r-----
```

которые устанавливаются командой:

```
find /var/mail/tegu.online -type f -exec chmod 640 {} \;
```

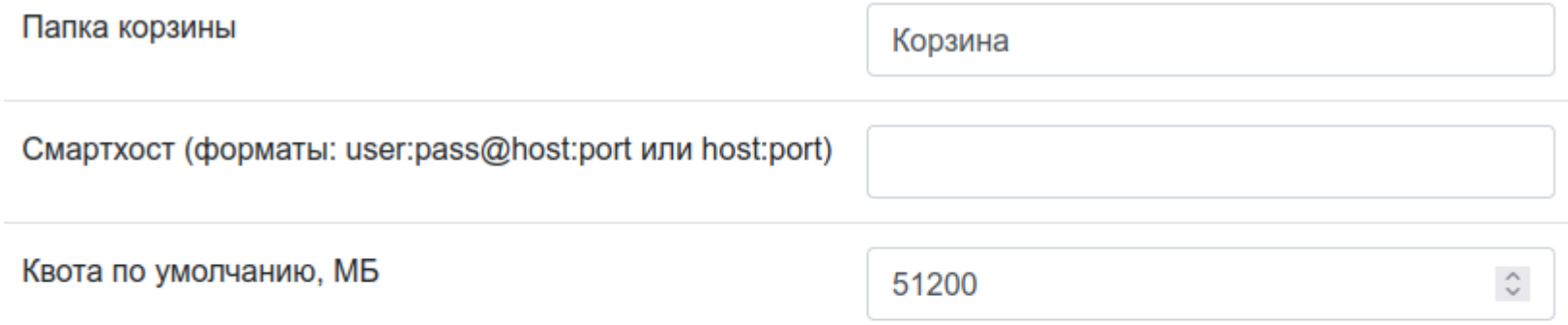
Владелец и группа должны быть те, от которых запускается сервис tegu.
Например, mail.mail, которые устанавливаются командой:

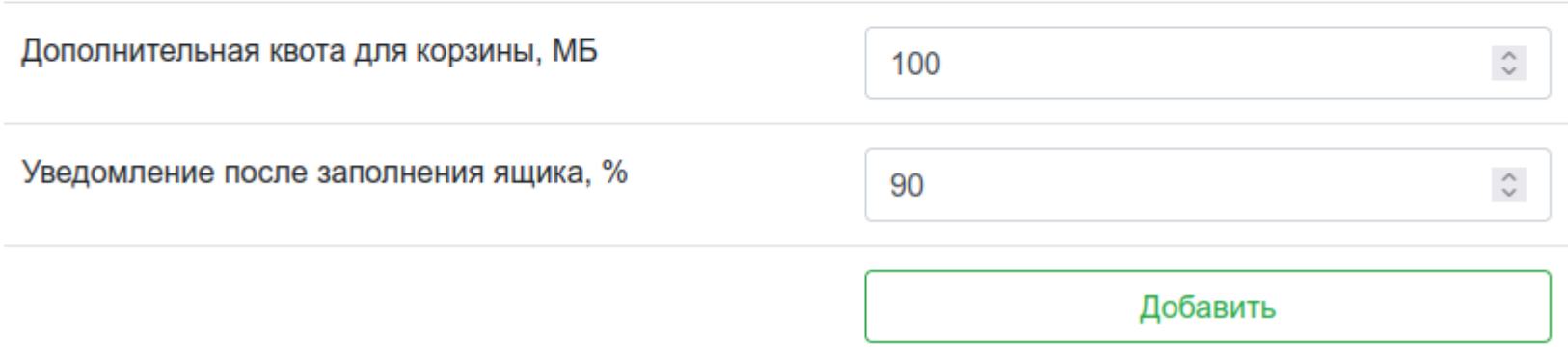
```
chown -R mail.mail /var/mail/tegu.online
```

Для создания хранилища укажите:

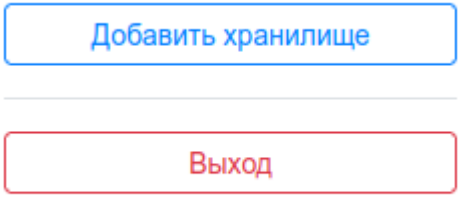
- Local mail domain name - интернет-домен, для которого создается хранилище;
- Root directory path of mail - каталог для хранения почты выбранного домена.

Завершив настройку, нажмите кнопку **Добавить**.





Хранилище будет создано и вы попадете в диалог добавления нового хранилища.



Создание почтового хранилища СУБД

Как было сказано выше, если вы используете редакцию Tegu Enterprise, то вы можете создать хранилище почты в СУБД. С Tegu совместима любая версия от отечественного вендора PosgresPro , либо свободная версия от PostgeSQL . (версия - не ниже 13)

Создаем пользователя:

```
createuser -d -S -E -P postgres
```

Создаем 3 базы данных

- tegu_queue - база данных очередей;
- tegu_mailboxes - база данных почтового хранилища;
- tegu_settings - база данных настроек почтового сервера.

```
createdb -E UTF-8 -O postgres tegu_queue
```

```
createdb -E UTF-8 -O postgres tegu_mailboxes
```

```
createdb -E UTF-8 -O postgres tegu_settings
```

Прописываем доступы с подсетей

```
nano /var/lib/pgsql/data/pg_hba.conf
```

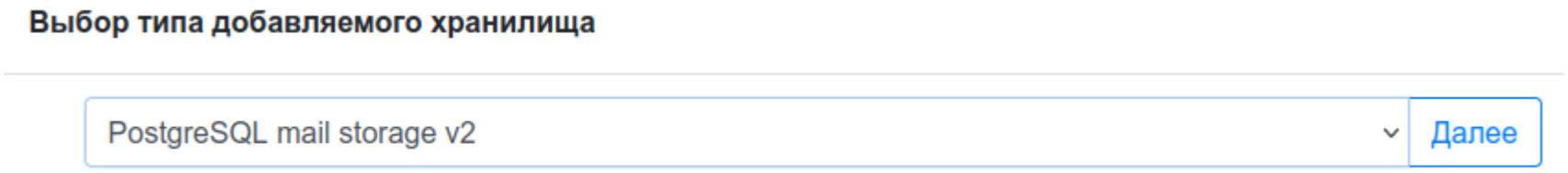
Смотрим какие базы данных у нас есть

```
psql -U postgres -c "\l+"
```

Удалить базы данных

```
psql
DROP DATABASE tegu_mailboxes;
```

Для создания хранилища в корневом меню выбираем **Хранилища почты**.



Очевидно, что целесообразно разместить почтовый сервер Tegu и СУБД на различных вычислительных нодах (виртуальных или физических).
Установка сервера БД производится согласно официальной документации Postgre . По окончании установки вам необходимо создать пользователя с правами создания баз, которым будет пользоваться сервер Tegu, а также

- необходимо создать две базы:
  - для хранения почты;
  - для хранения конфигурации.
- и, если необходимо:
  - для очереди сообщений SMTP.

Для всех БД пользователь этих БД должен иметь в них право CREATE.

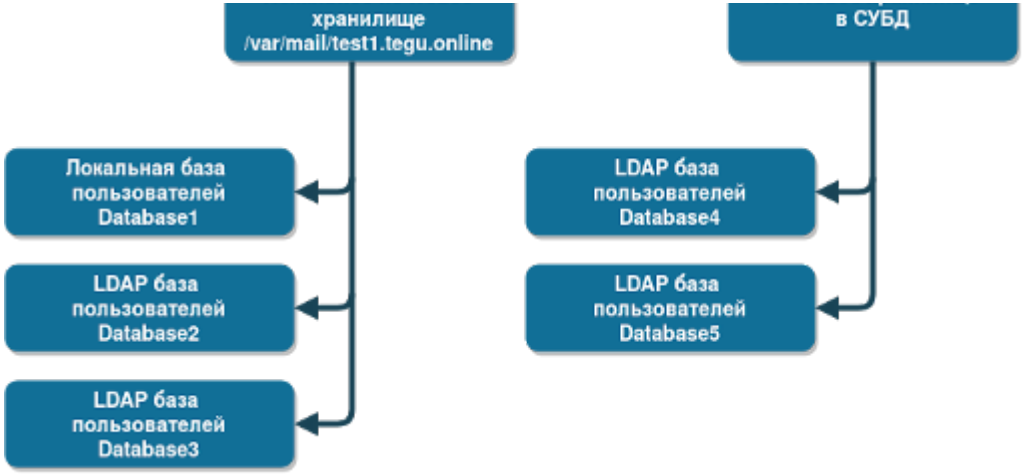
Параметры хранилища почты домена tegu.online

Тип хранилища	PostgreSQL mail storage v2
Адрес сервера	10.44.44.15
Порт сервера	5432
Имя базы данных	tegu_mailboxes
Имя пользователя	tegu
Пароль	••••••

Оптимизация БД, а также сборка отказоустойчивого решения БД, выходит за рамки установки почтового сервера и рассматривается в каждом конкретном случае по запросу. Интерес также представляет создание отказоустойчивой конфигурации базы данных, "рассмотренной в данной статье Построение отказоустойчивого кластера СУБД Postgres.

Создание/подключение баз данных пользователей

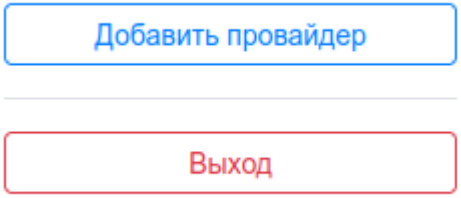
Итак, для понимания структуры давайте еще раз взглянем на картинку архитектуры объектов сервера.



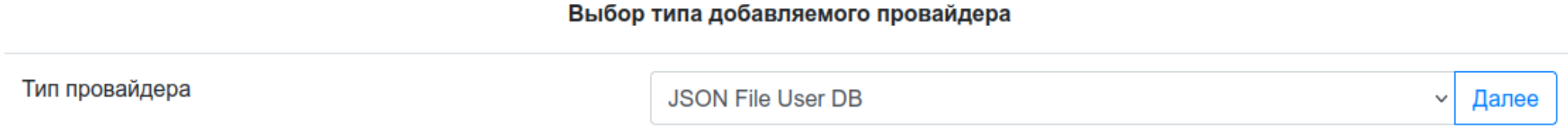
Как видно, каждый интернет-домен обслуживается одним хранилищем почты (которое может быть любого из двух типов: maildir или СУБД). Количество интернет-доменов не ограничено.

При этом каждый интернет-домен может обслуживать пользователей из различных баз данных. Базы данных могут быть локальными, либо LDAP3 (куда входит в т.ч. и Windows Active Directory).
Можно предположить, что найдутся более одной базы, которые будут содержать данные одного и того же пользователя. Эту коллизию, необходимо разрешить организационными мероприятиями, но сервер разрешит ее следующим образом: обслужен будет пользователь, описанный в конфигурации первым, все остальные будут проигнорированы.

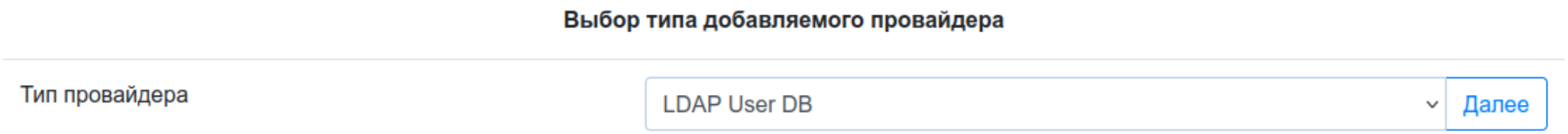
Для создания базы пользователей в корневом меню выберем пункт **Провайдеры БД пользователей**.
Добавим базу данных кнопкой **Добавить провайдер БД пользователей**.



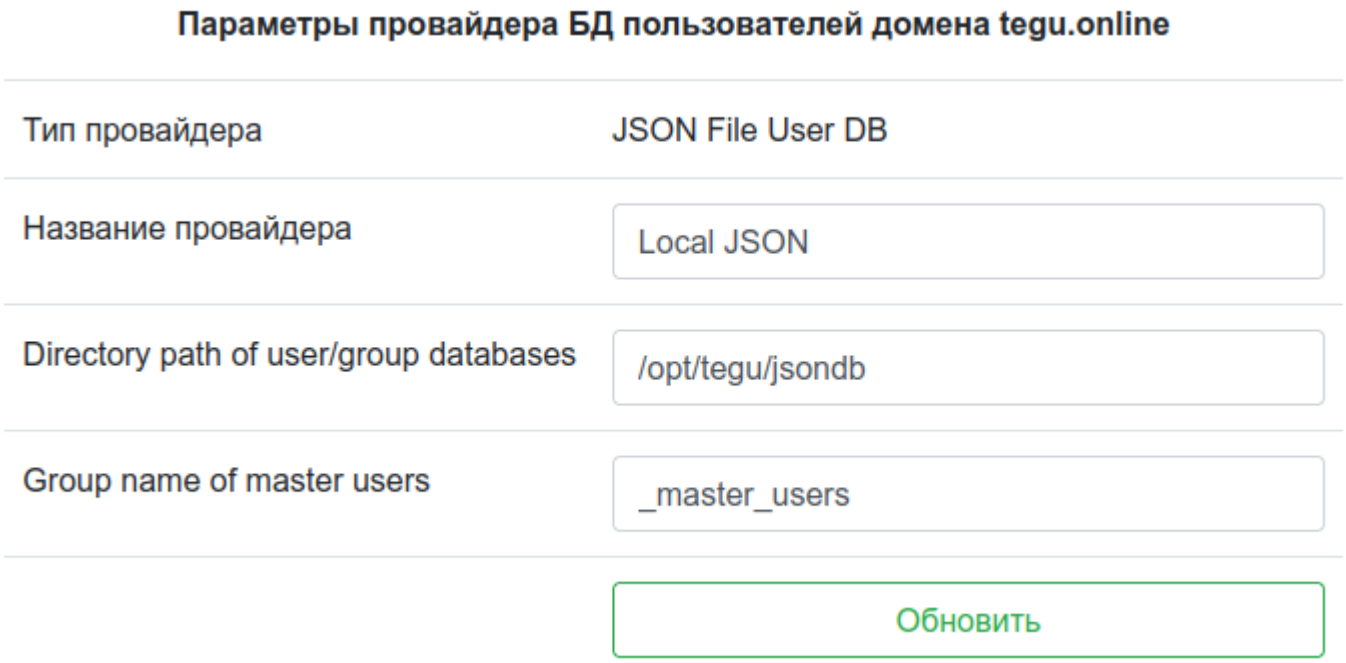
В данном диалоге мы можем выбрать локальную базу пользователей пунктом **JSON File User DB**, либо подключиться к одному из серверов каталогов **LDAP User DB**



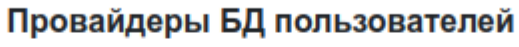
или

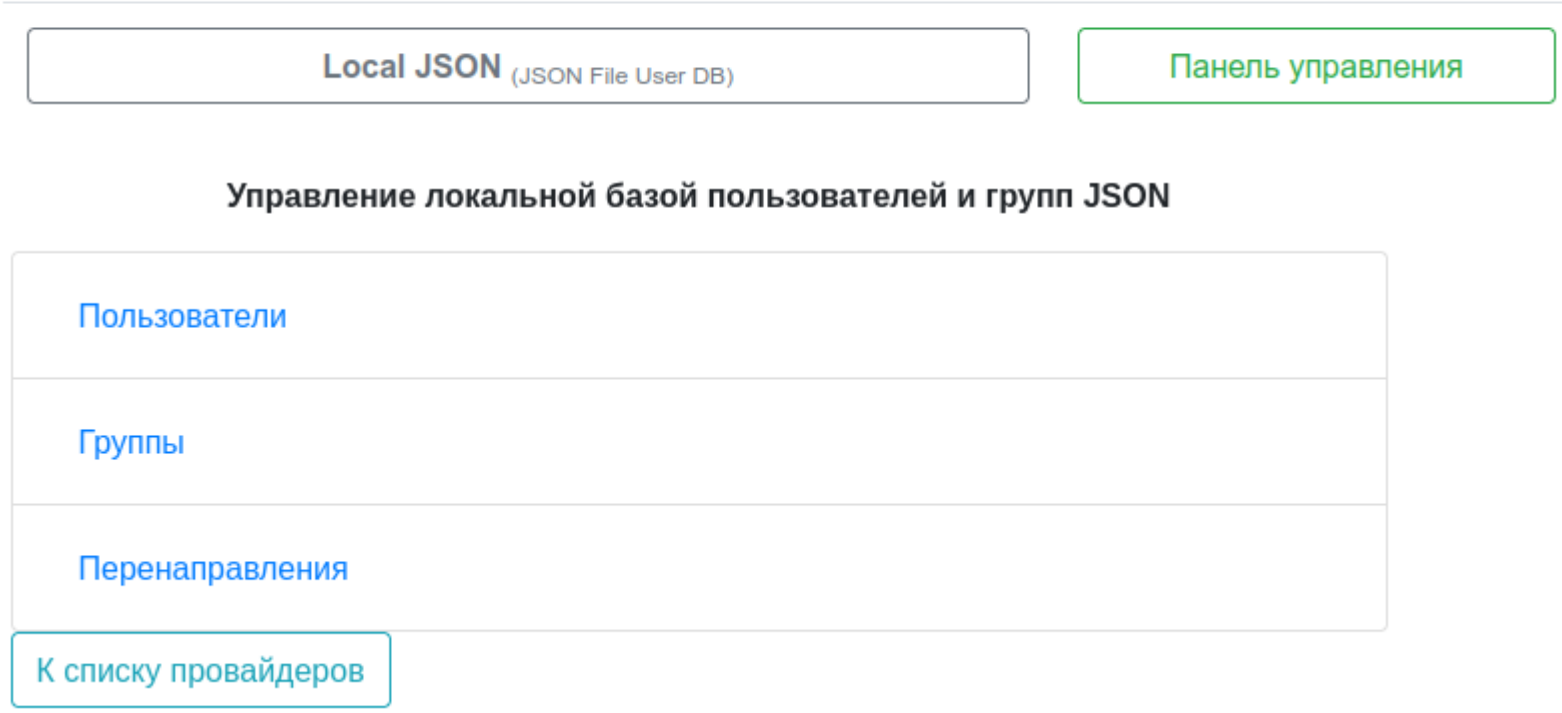


Далее заполняем либо имя и каталог размещения локальной базы данных, которая будет создана в формате JSON.

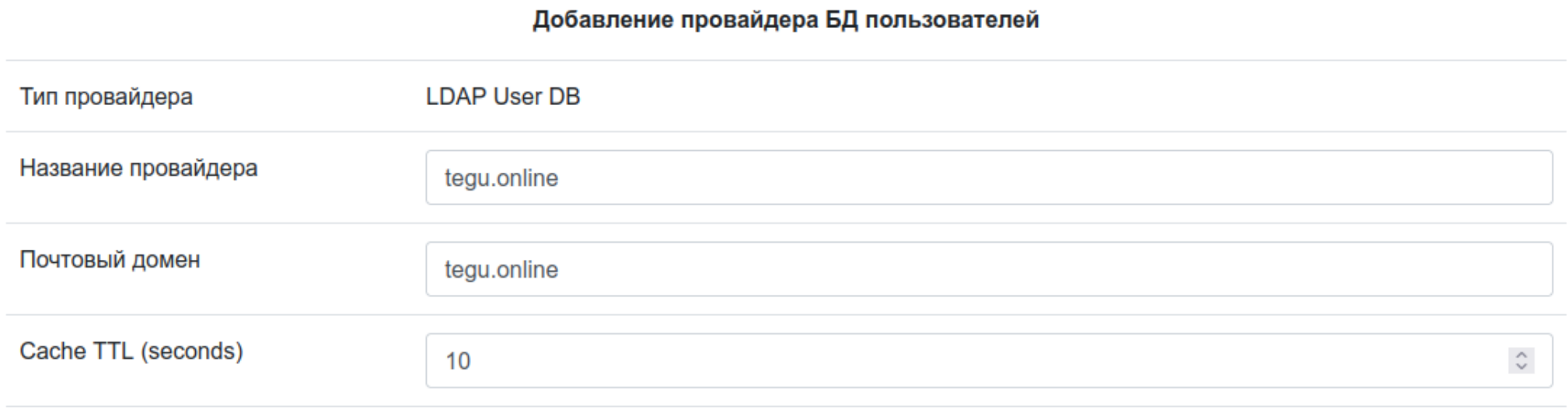


После создания локальной базы пользователей в интерфейсе рядом с созданной базой появится кнопка "Панель управления", нажав на которую вы попадаете в интерфейс создания групп, пользователей и правил данной локальной базы.





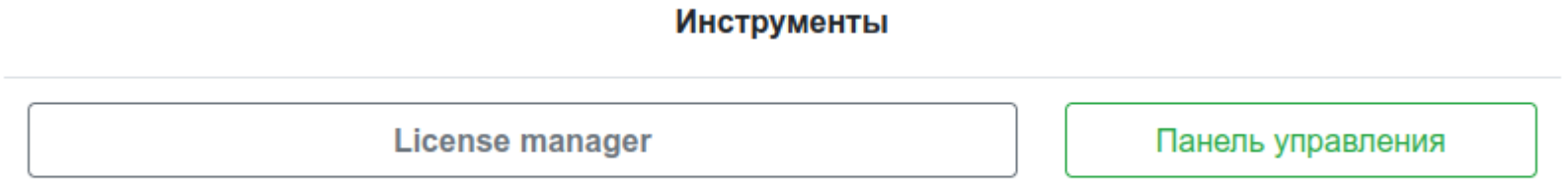
Второй вариант базы пользователей - подключение к LDAP-серверу каталогов.



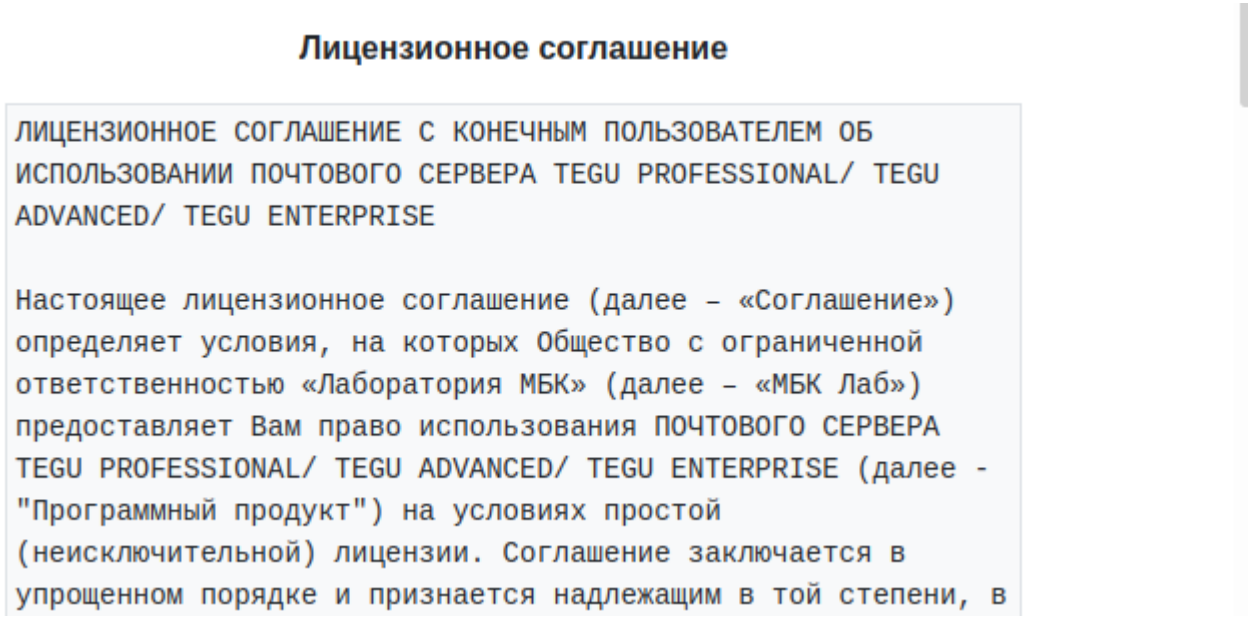
Обратите внимание! Почтовый сервер Tegu не синхронизирует данные ваших серверов каталогов. Это сделано специально для того, чтобы ни в каком случае не иметь возможности скомпрометировать учетные данные ваших пользователей. В момент, когда необходимо выполнить аутентификацию, сервер выполняет запрос к серверу каталогов в отношение одного пользователя, а выполнив аутентификацию очищает эти данные в памяти. По этой причине, осуществив подключение Tegu к LDAP-серверу, не ждите от него активности, ее не будет. Сервер обратится к LDAP только в момент аутентификации.

Загрузка лицензии

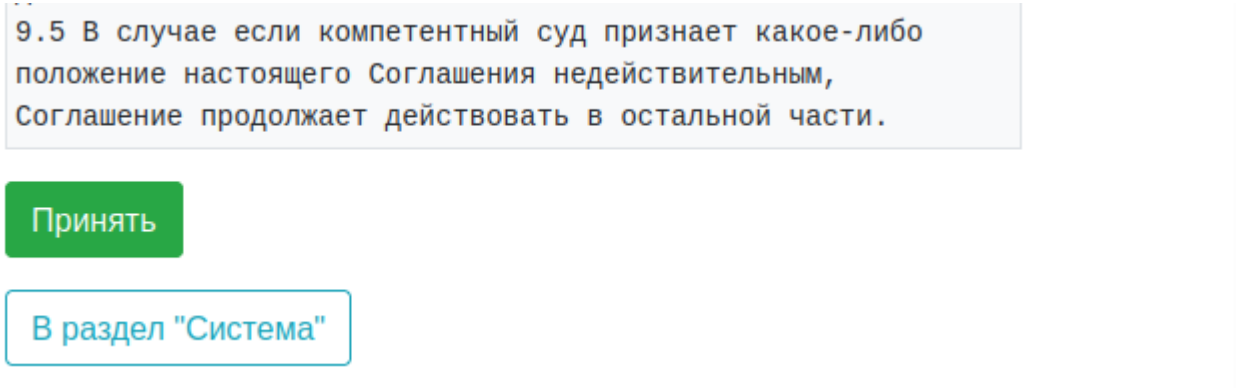
Для работы коммерческой редакции сервера вам потребуется загрузить файл лицензии. Это выполняется в пункте меню **Система**.
Выберите кнопку **Панель управления**.



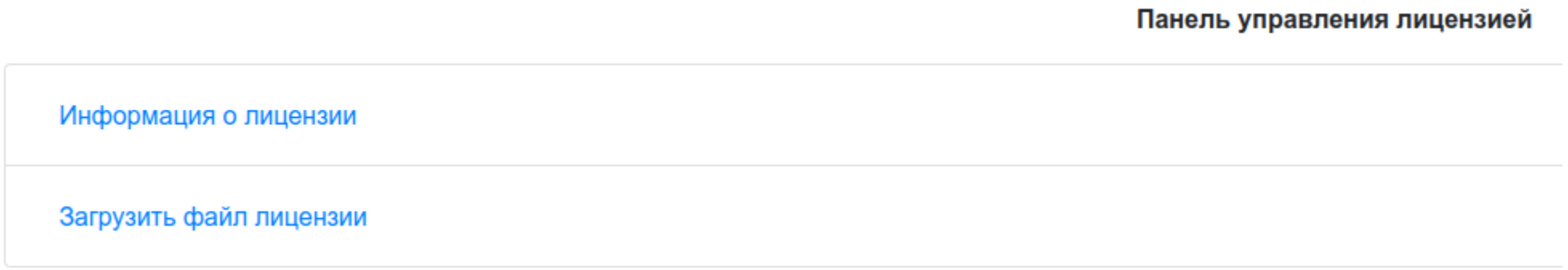
Прочтите лицензионное соглашение.



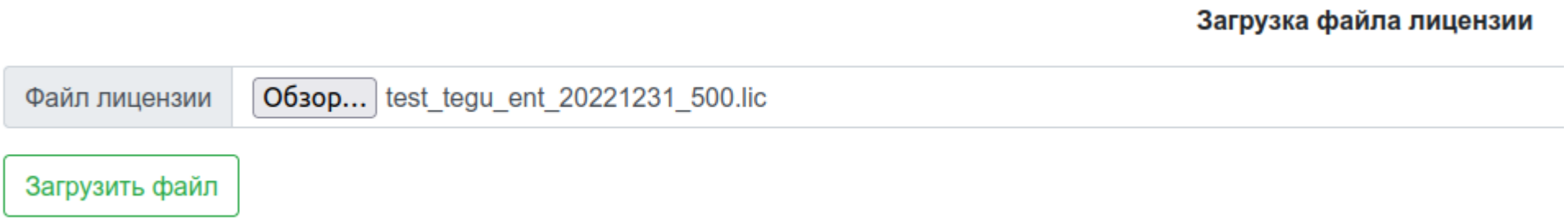
И нажмите кнопку **Принять**. Если вы не принимаете соглашение, загрузка лицензии невозможна и работа сервера будет остановлена.
В любой момент вы также можете прочесть Лицензионное соглашение к конечным пользователем на сайте компании.



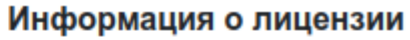
Выберите опцию **Загрузить файл лицензии**.



Выберите файл лицензии и нажмите **Загрузить файл**.



Загрузка лицензии завершена.



Идентификатор лицензии: **053c3ca02f204111a52bf6b60792f7d1**

Редакция Tegu: **Enterprise**

Дата окончания действия лицензии: **01.08.2022**

Максимальное количество почтовых ящиков: **500**

Наименование покупателя: **Тестовая лицензия Tegu Enterprise**

Тип покупателя: **Юр. лицо**

Данные покупателя:

Проверка настроек сервера

Проверить все выполненные настройки сервера можно с помощью утилиты teguctl (идущие в комплекте дистрибутива).

Команда:

```
# /opt/tegu/bin/teguctl dump
```

выведет всю конфигурацию сервера в тестовом формате.

> *Утилита teguctl поставляется с дистрибутивом (вы найдете ее в каталоге bin).*

Установка и генерация сертификатов Letsencrypt.

Центр сертификации, предоставляющий бесплатные криптографические сертификаты X.509 для шифрования передаваемых через интернет данных HTTPS и других протоколов, используемых серверами в Интернете.
Процесс выдачи сертификатов полностью автоматизирован.

Центр сертификации Let’s Encrypt выдаёт сертификаты со сроком действия в 90 дней.
Для получения сертификата должны быть проброшены порты: 80, 443.

Для Debian дистрибутивов.

Проверяем обновления пакетов:

```
apt update
```

Устанавливаем Letsencrypt:

```
apt install certbot
```

Получаем сертификат на свой почтовый домен:

```
certbot certonly --standalone -m ваша_почта@yandex.ru -d mail.вашдомен.рф
```

Проверяем, что сертификаты получены:

```
cd /etc/letsencrypt/live/mail.вашдомен.рф/

ls
```

Должны увидеть следующие файлы:

```
cert.pem  chain.pem  fullchain.pem  privkey.pem  README
```

Нас интересуют fullchain.pem privkey.pem .

Для RED OS 7.3

Для того что бы получить и установить сертификат, нам необходимо установить пакет certbot, но в репозитории РЕД ОС данного пакета нет, поэтому будем устанавливать его с помощью python.
Python у нас уже установлен, установим недостающий нам пакет.

```
dnf install  python-virtualenv
```

Создаем каталог:

```
mkdir -p /web/install/python/
```

Переходим в этот каталог:

```
cd /web/install/python/
```

Далее нам необходимо создать виртуальную среду для приложения. Саму среду мы назовём python-red :

```
python3 -m venv python-red
```

Далее, активируем среду приложения python-red :

```
source python-red/bin/activate
```

Если всё сделано правильно, мы увидим что перешли в среду разработки python.

Далее, нам необходимо обновить:

```
pip install --upgrade pip
```

Теперь устанавливаем пакет certbot:

```
pip install certbot
```

После установки пакета, запускаем процедуру получения ssl сертификатов:

```
certbot certonly --standalone -m ваша_почта@yandex.ru -d mail.вашдомен.рф
```

Проверяем что сертификаты получены:

```
cd /etc/letsencrypt/live/mail.вашдомен.рф/

ls
```

Должны увидеть следующие файлы:

```
cert.pem  chain.pem  fullchain.pem  privkey.pem  README
```

Нас интересуют fullchain.pem privkey.pem .

Автоматизируем обновление сертификатов скриптами:

Создаем папку work в папке root, она нам чуть позже пригодится:

```
mkdir work
```

Создаем в папке Letsencrypt hook со следующим содержанием:

nano /etc/letsencrypt/renewal-hooks/deploy/hook01

```
#!/bin/sh
do
        if [ "$domain" = mail.вашдомен.рф ]
        then
                /root/work/tegu_certs
                /bin/systemctl restart tegu
        fi
done
```

Делаем его исполняемым:

```
chmod +x /etc/letsencrypt/renewal-hooks/deploy/hook01
```

Далее создаем еще один скрипт:

```
nano /root/work/tegu_certs
```

И прописываем в нем следующие строки:

```
#!/bin/bash
cat /etc/letsencrypt/live/mail.вашдомен.рф/fullchain.pem > /opt/tegu/certs/cert.pem
cat /etc/letsencrypt/live/mail.вашдомен.рф/privkey.pem > /opt/tegu/certs/key.pem
chgrp mail /opt/tegu/certs/*
chmod 640 /opt/tegu/certs/*
```

Делаем скрипт исполняемым:

```
chmod +x /root/work/tegu_certs
```

Меняем группу владельцев:

```
chgrp root /etc/letsencrypt/archive/mail.вашдомен.рф/*
```

Запускаем скрипт:

```
/root/work/tegu_certs
```

Проверяем результат отрабатывания скрипта:

```
ls -lh /opt/tegu/certs/
```

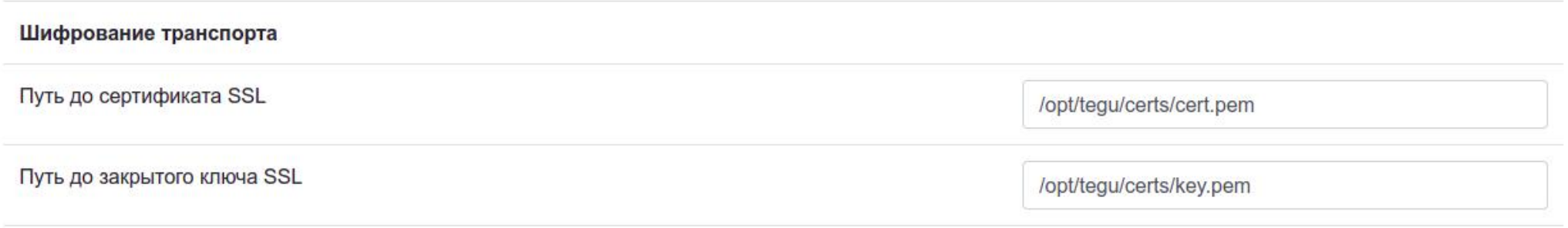
В этой папке должны появится сертификаты:

```
cert.pem key.pem
```

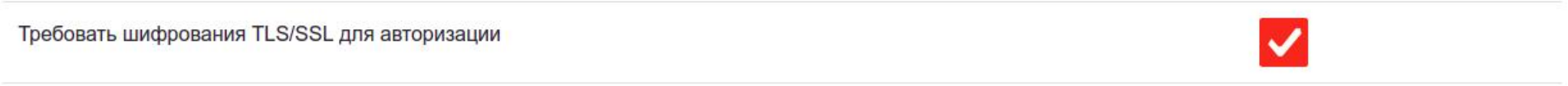
Соответственно в основных настройках почтового сервера мы указываем следующие пути к сертификатам:

```
/opt/tegu/certs/cert.pem
/opt/tegu/certs/key.pem
```

Должно получиться так.



После того как сертификаты сгенерированы и прописаны на почтовом сервере, в основных настройках необходимо включить опцию "Требовать шифрования TLS/SSL для авторизации".



Перезапустим почтовый сервер:

```
systemctl restart tegu
```

После того как все настройки выполнены только теперь можно проверять какие порты слушает почтовый сервер:

```
netstat -lnp
```

Интеграция с Active Directory и OpenLDAP

Пример настроек для подключения к Active Directory

Параметры провайдера БД пользователей домена test.tegu.online

Тип провайдера	LDAP User DB
Название провайдера	LDAP
Cache TTL (seconds)	10
LDAP connection URIs (one per line)	ldaps://tegu-ds.mbk.lan:636
BindDN	administrator@test.tegu.online
Password	••••••••••••••••••••••••
Base DN	dc=test,dc=tegu,dc=online
objectClass for user	user
Attr for mailbox e-mail	mail
Attr for mailbox quota (value in MB)	facsimileTelephoneNumber
User memberOf attr	memberOf

Use groups

objectClass for group: group

Attr for group name: cn

Attr for group email: mail

Attr for group members: member

Group member attr contains DN

Attr for user RDN:

Use mailbox alias (redirect list)

objectClass for alias: nisMailAlias

Attr for alias email: name

Attr for email redirect to: rfc822MailMember

Use mailbox alternative email	☑
Attr for mailbox alternative email	otherMailbox
Attr for group name of master-users	cn
Group name of master-users	_master_users

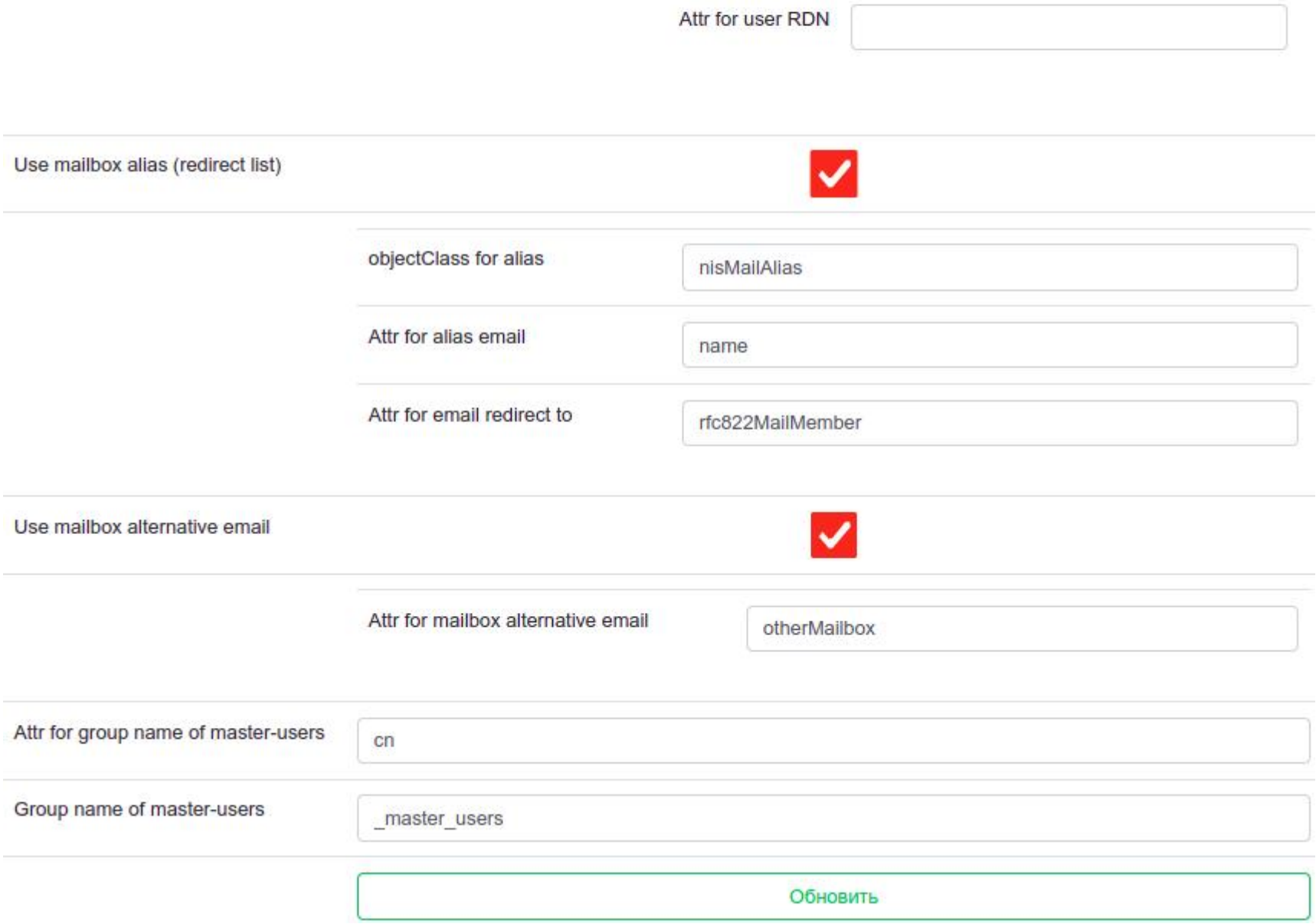
Обновить

Пример настроек для подключения к OpenLDAP

Параметры провайдера БД пользователей домена tegu.online

Тип провайдера	LDAP User DB
Название провайдера	LDAP
Cache TTL (seconds)	10
LDAP connection URIs (one per line)	ldap://10.44.44.16:389
BindDN	adminnistrator@tegu.online

Password	•••••••••••••
Base DN	dc=tegu,dc=online
objectClass for user	inetOrgPerson
Attr for mailbox e-mail	mail
Attr for mailbox quota (value in MB)	pager
User memberOf attr	
Use groups	☑
objectClass for group	groupOfNames
Attr for group name	cn
Attr for group name	cn
Attr for group email	mail
Attr for group members	member
Group member attr contains DN	☑



См. также:

- Администрирование сервера