**!!! Это один из способов как можно выполнить задание демоэкзамена. Лучше понять самому, чем копировать.**

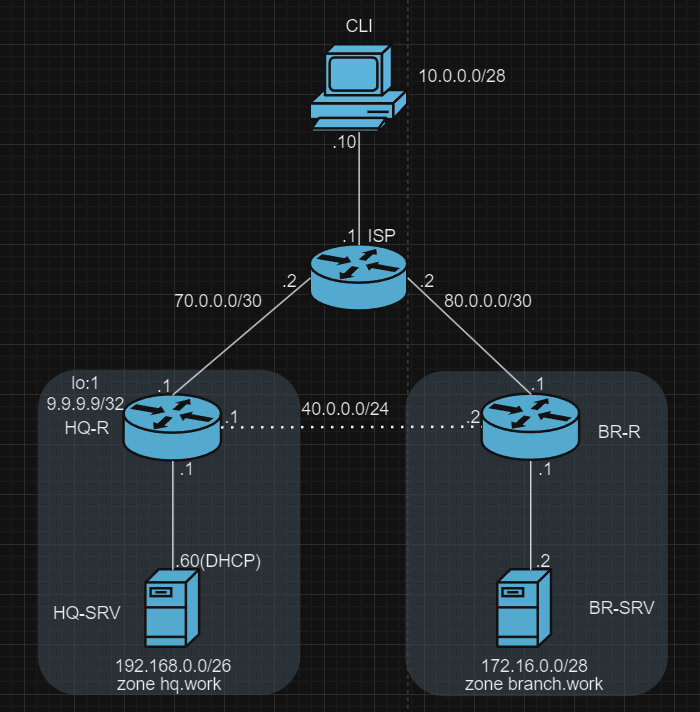
****

Рисунок 1 - Схема сети

# 

# Базовая настройка

1. Установка имен устройствам. На устройствах hq-r, hq-srv, br-r, br-srv устанавливается FQDN имя. Имена хостов задаются в соответствии со схемой. Ниже показаны имена для каждого устройства и файл, в котором его нужно задать.

**root@all:~#** nano /etc/hostname

hq-srv.hq.work

br-srv.branch.work

cli

isp

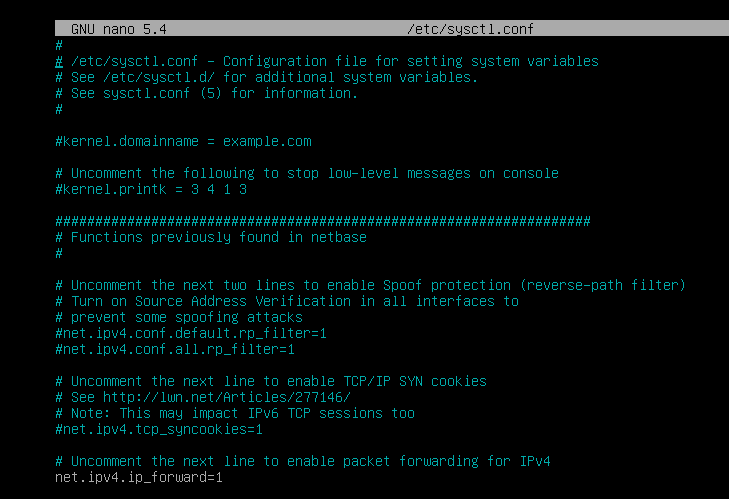
br-r.branch.work

hq-r.hq.work

1. На всех маршрутизаторах(isp, hq-r, br-r) необходимо включить ip\_forward.

**root@debian:~#** sysctl -w net.ipv4.ip\_forward=1 >> /etc/sysctl.conf

Либо зайти в файл /etc/sysctl.conf и привести его к такому виду:



После этого машины необходимо перезагрузить.

# IP-адресация

Необходимо выполнить установку ip-адресации как ipv4, так и ipv6. Задание IP-адресов производится в произвольном порядке. Схема дана для примера, см. рис 1. Также можно выполнить настройку адресации через nmtui.

**root@debian:~#** nano /etc/network/interfaces

auto ens\*

iface ens\* inet static

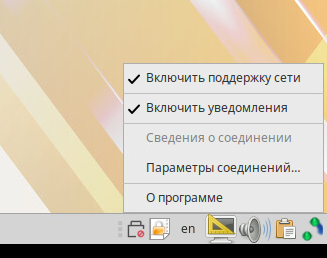
address \*/netmask\*

gateway (при необходимости)

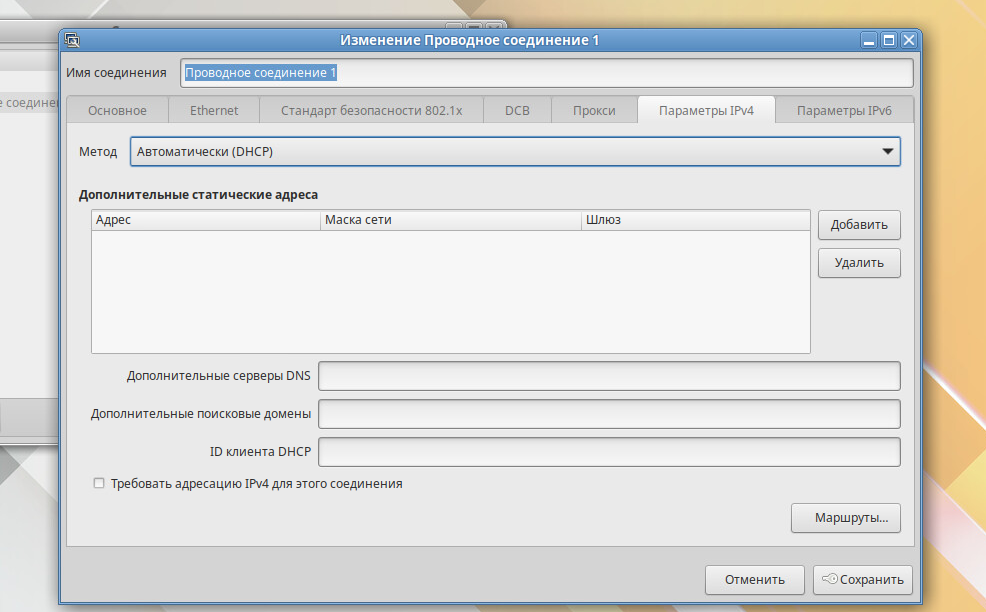
**root@debian:~#** systemctl restart networking

На устройствах OS Alt можно выполнить настройку адресации двумя способами:

1. Через графический интерфейс. Параметры соединений



Сменить метод с “Автоматически (DHCP)” на “Вручную” и нажать “Добавить”, после внесения изменений “Сохранить”.



Устанавливаем необходимый адрес

1. Через командную строку.

**root@alt:~#** nano /etc/net/ifaces/интерфейс/

Файл ipv4address содержит IP-адрес с указанием маски в префиксной форме

Файл ipv4route содержит адрес шлюза по умолчанию (default via x.x.x.x)

Файл resolv.conf содержит адрес DNS-сервера и домена (nameserver, search, domain)

Файл options содержит настройки конфигурации(пример ниже)

NM\_CONTROLLED=yes

DISABLED=no

TYPE=eth

CONFIG\_WIRELESS=no

BOOTPROTO=static

SYSTEMD\_BOOTPROTO=static

CONFIG\_IPV4=yes

SYSTEMD\_CONTROLLED=no

После внесения всех изменений необходимо перезапустить службу network

**root@alt:~#** systemctl restart network

На ISP необходимо прописать статические маршруты для CLI в сети BRANCH и HQ для этого:

**root@isp:~#** nano /etc/network/interfaces

up ip route add 192.168.0.0/26 via 70.0.0.1

up ip route add 172.16.0.0/28 via 80.0.0.1

# Туннель + IPSec

Настройка GRE туннеля выполняется между BR-R и HQ-R.

**root@hq-r:~#** nano /etc/network/interfaces

auto gre1

iface gre1 inet tunnel

address 40.0.0.1

netmask 255.255.255.0

pre-up modprobe ip\_gre

mode gre

local 70.0.0.1

endpoint 80.0.0.1

ttl 255

**root@br-r:~#** nano /etc/network/interfaces

auto gre1

iface gre1 inet tunnel

address 40.0.0.2

netmask 255.255.255.0

pre-up modprobe ip\_gre

mode gre

local 80.0.0.1

endpoint 70.0.0.1

ttl 255

Для настройки IPSec необходимо установить пакет libreswan на обоих машинах.

**root@hq-r&br-r:~#** apt install libreswan -y

**root@hq-r:~#** nano /etc/ipsec.conf

В конце дописываем

conn ipsec

auto=start

authby=secret

type=tunnel

ike=aes-sha1;modp2048

left=40.0.0.1

leftprotoport=gre

right=40.0.0.2

rightprotoport=gre

**root@hq-r:~#** nano /etc/ipsec.secrets

В конце дописываем

40.0.0.1 40.0.0.2 : PSK “pass”

**root@br-r:~#** nano /etc/ipsec.conf

В конце дописываем

conn ipsec

auto=start

authby=secret

type=tunnel

ike=aes-sha1;modp2048

left=40.0.0.1

leftprotoport=gre

right=40.0.0.2

rightprotoport=gre

**root@br-r:~#** nano /etc/ipsec.secrets

В конце дописываем

40.0.0.2 40.0.0.1 : PSK “pass”

**root@hq-r&&br-r:~#** systemctl restart ipsec

**root@all:~#** systemctl enable ipsec

# Динамическая маршрутизация

Необходимо осуществить настройку **внутренней** динамической маршрутизации, которая будет осуществляться между hq-r и br-r через gre туннель. Для этого требуется установить **пакет frr** на обоих машинах и далее включить возможность работы c ospf

**root@hq-r&br-r:~#** apt install frr -y

**root@hq-r&br-r:~#** nano /etc/frr/daemons

ospfd=yes

**root@br-r&hq-r:~#** systemctl restart frr

**root@br-r&hq-r:~#** systemctl enable frr

**root@hq-r:~#** vtysh

conf t

router ospf

network 40.0.0.0/24 area 0

network 192.168.0.0/26 area 0

network 9.9.9.9/32 area 0

do write

**root@br-r:~#** vtysh

conf t

router ospf

network 40.0.0.0/24 area 0

network 172.16.0.0/28 area 0

do write

После этого можно проверить связь между зонами hq.work и branch.work - должен быть ping.

Настройка DHCP

На роутере HQ-R необходимо настроить DHCP для выдачи зарезервированного адреса на сервер HQ-SRV. Для этого необходимо установить пакет isc-dhcp-server.

**root@hq-r:~#** apt install isc-dhcp-server

Далее внести изменения в конфигурационный файл, как показано ниже:

**root@hq-r:~#** nano /etc/dhcp/dhcpd.conf

subnet 192.168.0.0 netmask 255.255.255.192 {

range 192.168.0.10 192.168.0.20;

option routers 192.168.0.1;

}

host hq-srv {

hardware ethernet mac-address hq-srv;

fixed-address 192.168.0.60;

}

В файл /etc/default/isc-dhcp-server необходимо добавить интерфейс, который смотрит на hq-srv

**root@hq-r:~#** nano /etc/default/isc-dhcp-server

INTERFACESv4=”ens224”

Далее требуется перезагрузить службу isc-dhcp-server.

**root@hq-r:~#** systemctl restart isc-dhcp-server

**root@hq-r:~#** systemctl enable isc-dhcp-server

# Настройка учетных записей

Необходимо настроить локальные учетные записи в соответствии с таблицей. Вводим имена пользователей с большой буквы

**root@debian:~#** useradd Branch\_admin

**root@debian:~#** usermod -c “Branch admin” Branch\_admin

Далее вводится пароль P@ssw0rd.:

На устройствах ОС Альт создаем пользователей с маленькой буквы, далее необходимо добавить комментарий, где имя имеет верхний регистр.

**root@alt:~#** adduser branch\_admin -p P@ssw0rd

**root@alt:~#** usermod -c “Branch admin” branch\_admin

После необходимо изменить имя пользователя, чтобы оно отображалось с большой буквы.

# Измерение пропускной способности сети

На устройствах HQ-R и ISP устанавливаем пакет iperf3

**root@isp&hq-r:~#** apt install iperf3

**root@isp:~#** iperf3 -s

**root@hq-r:~#** iperf3 -c 70.0.0.2

# 

# Настройка DNS

Можно реализовать двумя способами. Первый - это установить пакет bind и выполнить традиционную настройку. Второй - это при настройке freeipa настроить DNS.

1.

**root@hq-srv:~#** apt-get install bind

**root@hq-srv:~#** cp /etc/bind/bind/zone/empty /etc/bind/bind/zone/hq

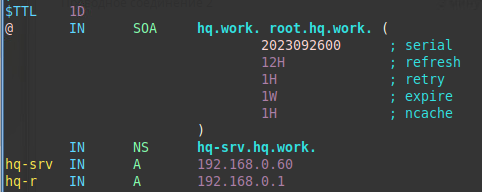
**root@hq-srv:~#** cp /etc/bind/bind/zone/empty /etc/bind/bind/zone/branch

**root@hq-srv:~#** cp /etc/bind/bind/zone/empty /etc/bind/bind/zone/hq\_obr

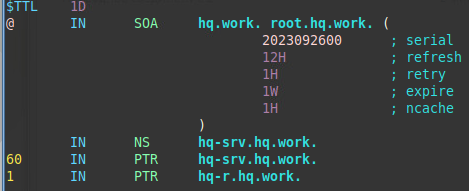
**root@hq-srv:~#** cp /etc/bind/bind/zone/empty /etc/bind/bind/zone/branch\_obr

**root@hq-srv:~#** chmod 777 /etc/bind/bind/zone/hq\*

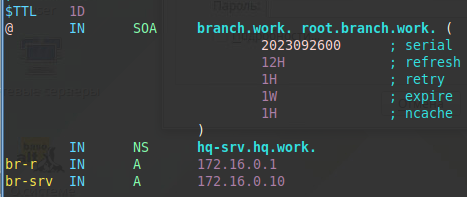
**root@hq-srv:~#** chmod 777 /etc/bind/bind/zone/branch\*



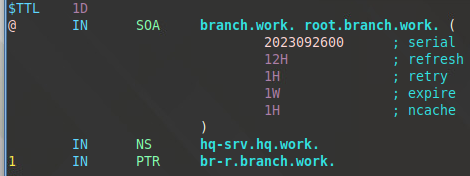
Зона hq.work - файл /etc/bind/bind/zone/hq.work



Зона 0.168.192.in-addr.arpa файл /etc/bind/bind/zone/hq.obr

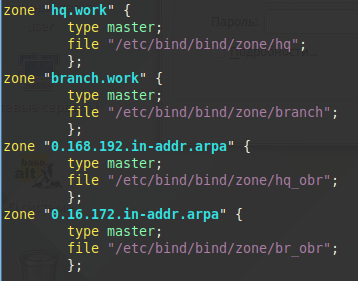


Зона branch.work файл /etc/bind/bind/zone/branch.work



Зона 0.16.172.in-addr.arpa файл /etc/bind/bind/zone/branch.obr

**root@hq-srv:~#** nano /etc/bind/local.conf



**root@hq-srv:~#** systemctl restart bind

**root@hq-srv:~#** systemctl enable bind

2. Настройка DNS в Freeipa находится [тут](#_xibxnbt05o3s)

# Настройка сервера времени

Для этого необходимо установить пакет chrony на машине HQ-R.

Клиенты должны подключаться к loopback адресу HQ-R, настройка приведена ниже.

**root@hq-r:~#** nano /etc/network/interfaces

auto lo:1

iface lo:1 inet static

address 9.9.9.9/32

Конфигурационный файл показан ниже.

**root@hq-r:~#** nano /etc/chrony/chrony.conf

server 127.127.0.1 iburst

allow all

local stratum 5

**root@hq-r:~#** systemctl restart chronyd

Для настройки клиентов необходимо установить пакет chrony на все машины. Конфигурационный файл показан ниже.

**root@all:~#** nano /etc/chrony/chrony.conf

server 9.9.9.9

# Настройка RAID 5

**root@br-srv:~#** mdadm —-create —-verbose /dev/md0 -l 5 —-raid-devices=3 /dev/sd{b,c,d}

# Настройка iptables

**root@br-r:~#** iptables -A INPUT -m state —-state RELATED,ESTABLISHED -j ACCEPT

**root@br-r:~#** iptables -A INPUT -p icmp -j ACCEPT

**root@br-r:~#** iptables -A INPUT -p gre -j ACCEPT

**root@br-r:~#** iptables -A INPUT -p tcp -m multiport —-dports 53,80,443,2222 -j ACCEPT

**root@br-r:~#** iptables -A INPUT -p udp -m multiport —-dports 53,500,4500 -j ACCEPT

**root@br-r:~#** iptables -A INPUT ! -i ens192 -j ACCEPT

**root@br-r:~#** iptables -A INPUT -m state —-state INVALID -j DROP

**root@br-r:~#** iptables -A FORWARD -m state —-state RELATED,ESTABLISHED -j ACCEPT

**root@br-r:~#** iptables -A FORWARD ! -i ens192 -j ACCEPT

**root@br-r:~#** iptables -A FORWARD -m state —-state INVALID -j DROP

**root@br-r:~#** iptables -P INPUT DROP

**root@br-r:~#** iptables -P FORWARD DROP

# Настройка SSH

На устройствах где не установлен ssh, необходимо установить пакет openssh-server.

Добавляем в конфигурационный файл необходимые параметры:

**root@debian:~#** nano /etc/ssh/sshd\_config

Port 2222

PasswordAuthentication no

PermitEmptyPassowrds no

PermitRootLogin no

MaxAuthTries 4

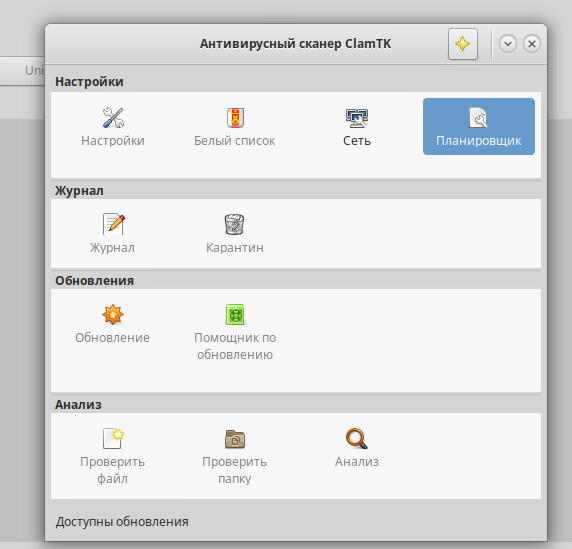
LoginGraceTime 5m

Banner (path to file banner)

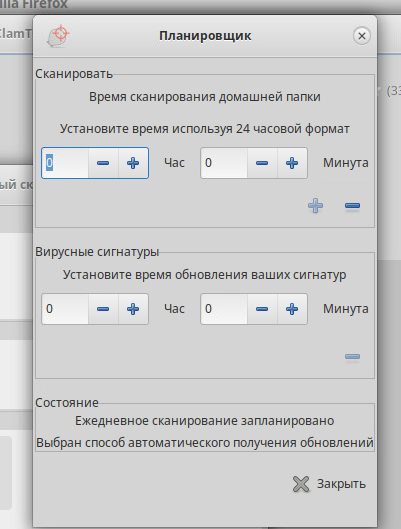
# Антивирусная защита ClamAV

Антивирус устанавливается и настраивается на устройствах HQ-SRV и BR-SRV.

Для этого необходимо открыть приложение “Менеджер Пакетов” и найти программу ClamTK. Далее зайти в планировщик:



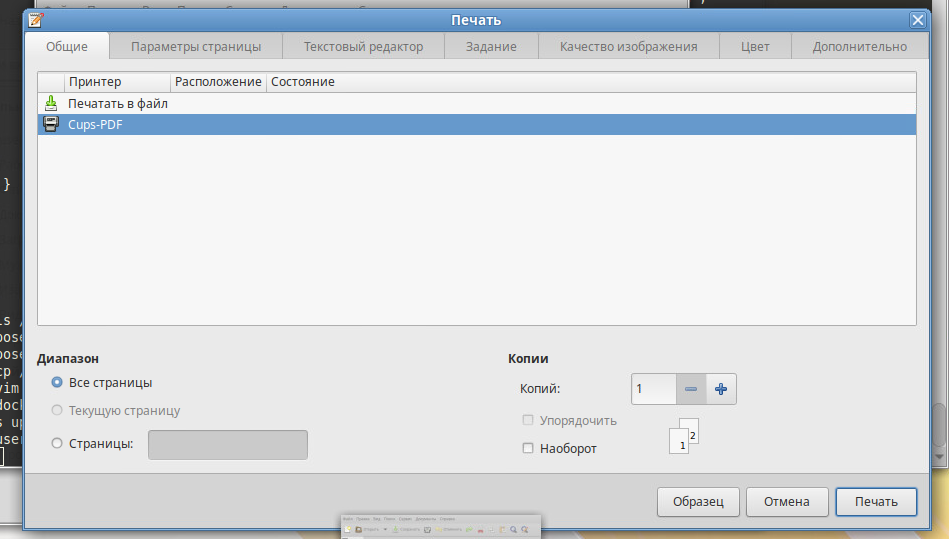
И установить любое ночное время для сканирования



# Настройка виртуального принтера CUPS

Необходимо на BR-SRV на рабочем столе создать обычный пустой файл

Открываем этот файл и жмем на печать



Выбираем параметр Cups-PDF и жмем печать. На рабочий стол сохранится файл в PDF. Задание выполнено.

# Docker

<https://hub.docker.com/_/mediawiki> - почти готовый конфиг.

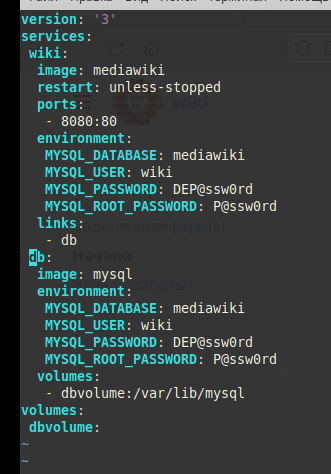
1. Установка. На hq-srv необходимо установить пакеты docker-ce, docker-compose.

**root@hq-srv:~#** apt-get install docker-ce docker-compose -y

1. Включить службу docker и добавить в автозагрузку

**root@hq-srv:~#** systemctl enable —-now docker

1. В домашней директории пользователя создать файл wiki.yml и скопировать туда конфиг из docker-hub и поправить его. Готовый yml файл показан ниже:



Запускаем compose:

**root@hq-srv:~#** docker-compose -f wiki.yml up -d

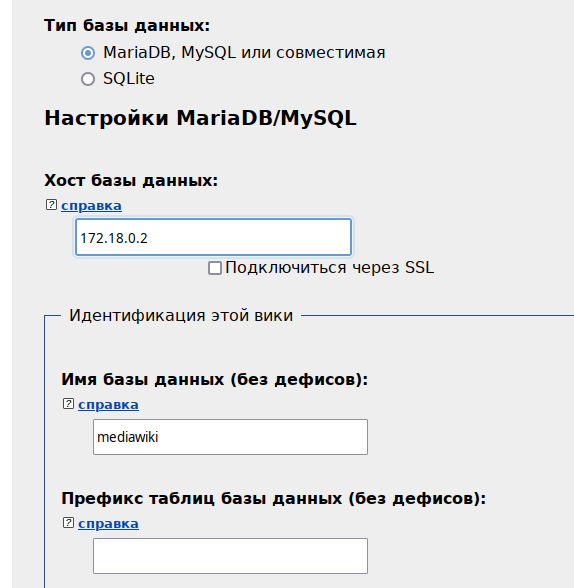
Далее в браузере открываем mediawiki:



Set up the wiki

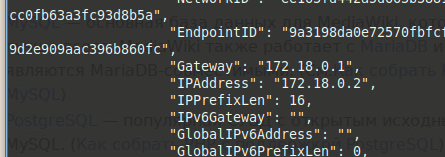
Далее выбирается язык, проверка окружения.

Настраиваем подключение к базе:

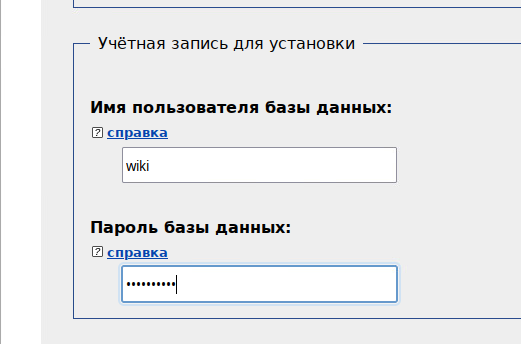


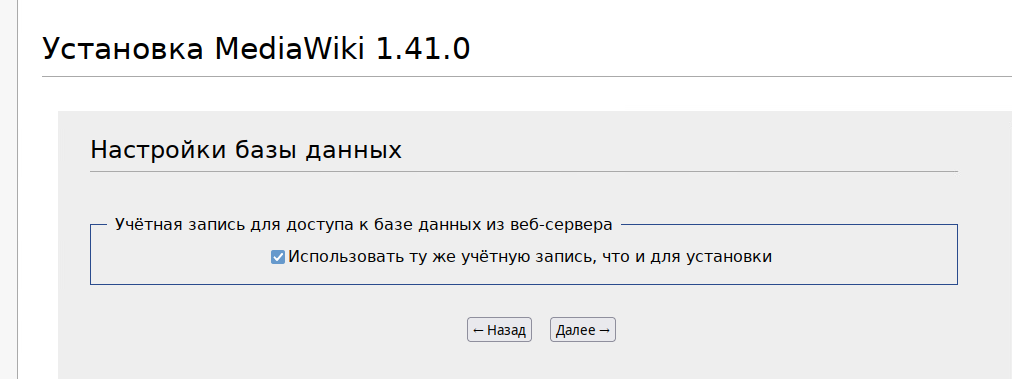
Для того, чтобы узнать адрес базы данных необходимо выполнить следующую команду:

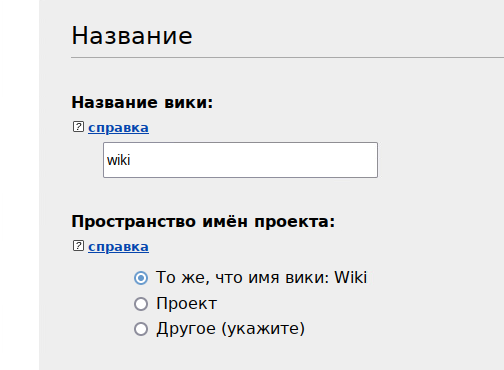
**root@hq-srv:~#** docker inspect user\_db\_1

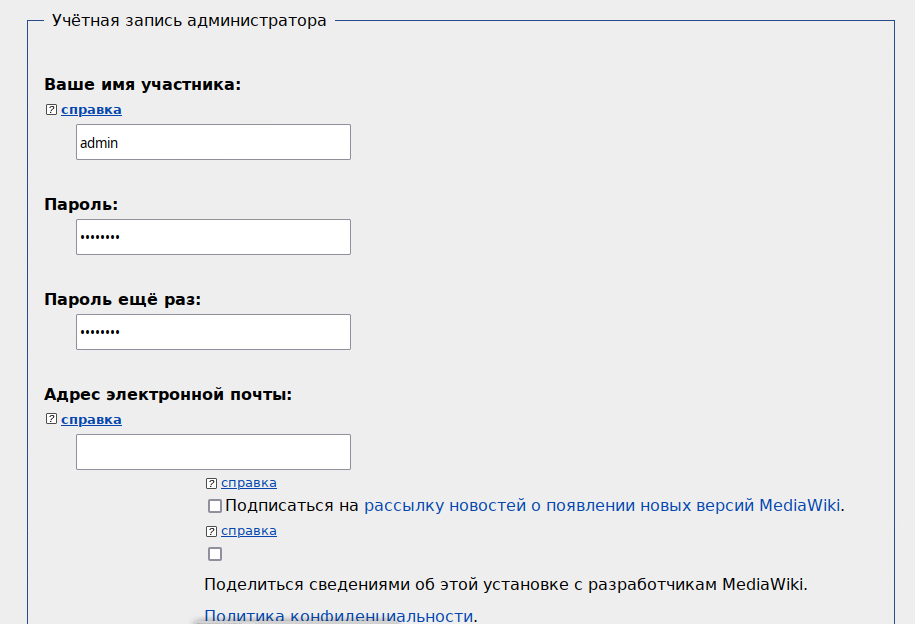


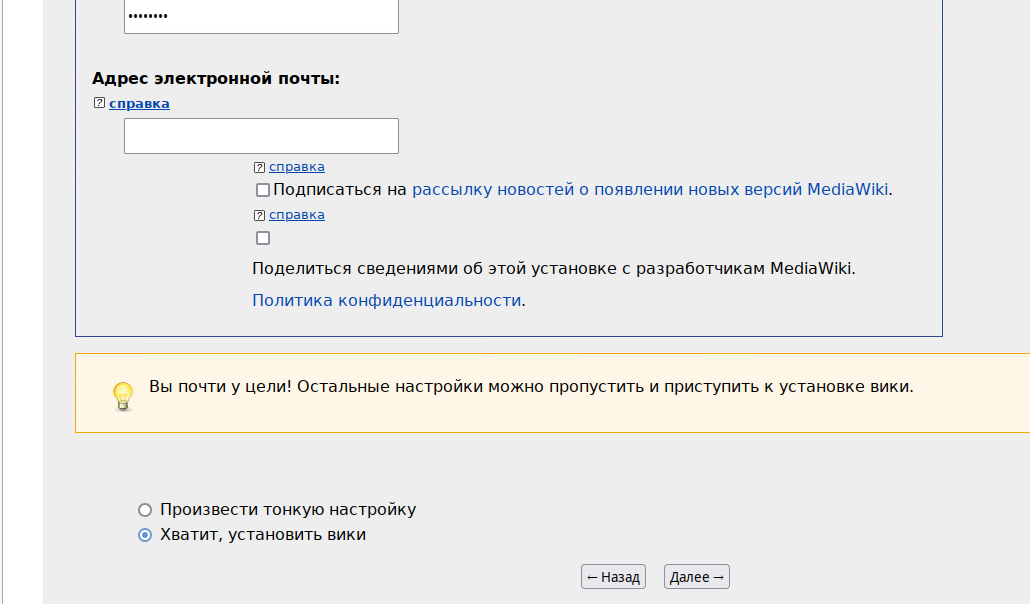
В строке IPAddress смотри IP, обычно это 172.18.0.2



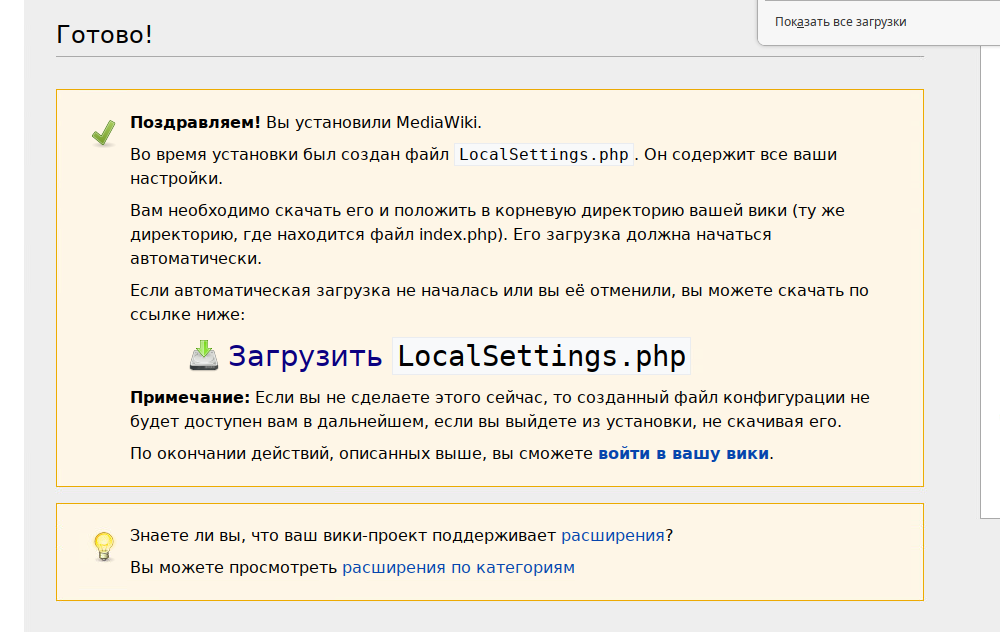








Далее загружаем файл LocalSettings.php

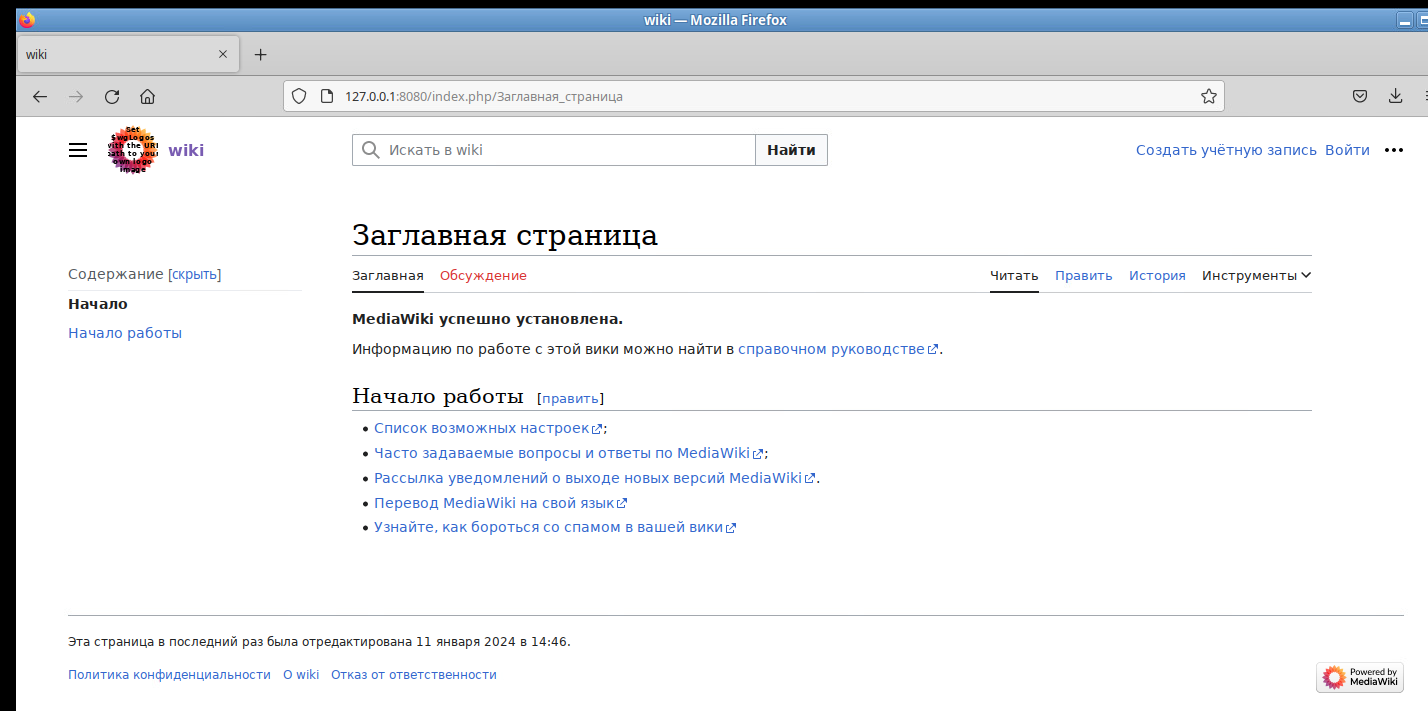


Открываем файл wiki.yml и создаем volume в контейнере wiki с LocalSettings.php:



После этого вновь прописываем:

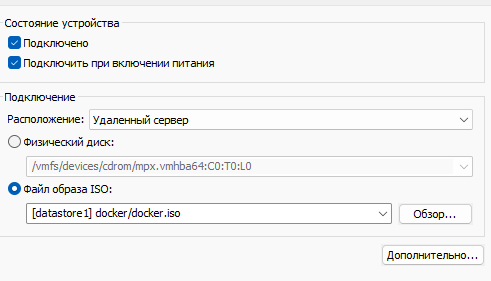
**root@hq-srv:~#** docker-compose -f wiki.yml up -d



Открываем wiki и видим, что всё работает.

!!!!! НА ДЕМОЭКЗАМЕНЕ, образы mysql и mediawiki будут лежать на диске, ниже показано как их оттуда достать

Первым делом подключаем сам диск



Монтируем его

mount /dev/sr0 /mnt

И прописываем

docker load -i /mnt/docker.tar

Далее производим те же процедуры написания docker-compose и его запуска

# Веб-сервер LMS Apache Moodle

Он настраивается на машине BR-SRV, советую использовать способ 2

### Способ 1:

Необходимо установить следующие пакеты:

**root@br-srv:~#** apt-get install httpd2 mariadb php8.0 php8.0-mysqli apache2-mod\_php8.0 php8.0-curl php8.0-zip php8.0-mbstring php8.0-openssl php8.0-gd php8.0-xmlreader php8.0-fileinfo php8.0-sodium php8.0-soap php8.0-exif

**root@br-srv:~#** systemctl enable —-now httpd2 mariadb

База данных

**root@br-srv:~#** mysql -uroot

CREATE DATABASE moodledb;

CREATE USER ‘moodle\_user’@’localhost’ IDENTIFIED BY ‘P@ssw0rd’;

GRANT ALL ON moodledb.\* TO ‘moodle\_user’@’localhost’;

FLUSH PRIVILEGES;

\q

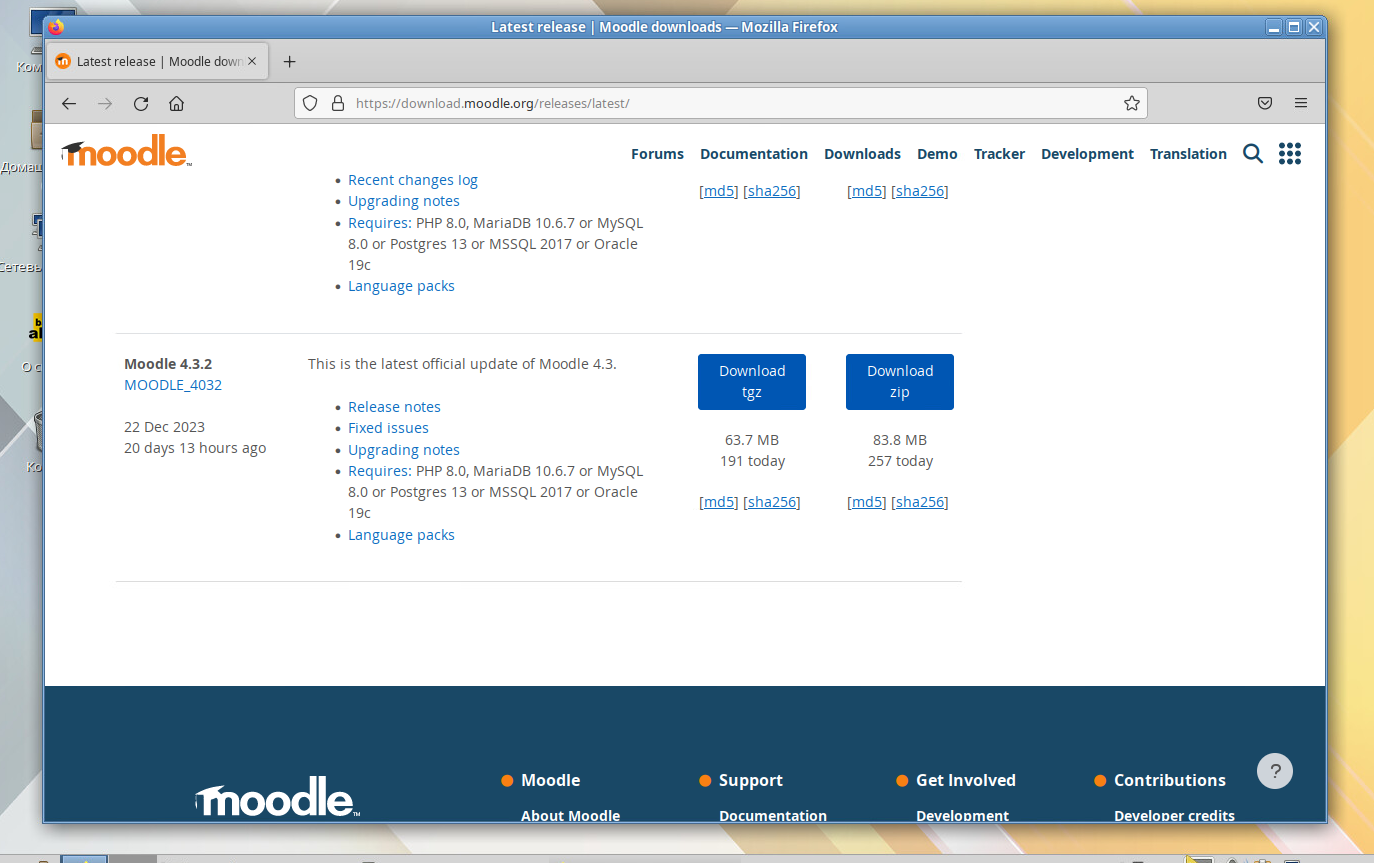
### Параметр php

Также необходимо отредактировать параметр max\_input\_vars поставив значение 6000 в файле:

**root@br-srv:~#** nano /etc/php/8.0/apache2-mod\_php/php.ini

max\_input\_vars 6000

Далее необходимо скачать сам moodle



После этого распаковать архив.

Далее создаем директории для moodle:

**root@br-srv:~#** mkdir /var/www/moodledata

**root@br-srv:~#** chown -R apache2:apache2 /var/www/moodledata

**root@br-srv:~#** chmod -R 755 /var/www/moodledata

**root@br-srv:~#** cp -r /home/user/moodle /var/www/html/

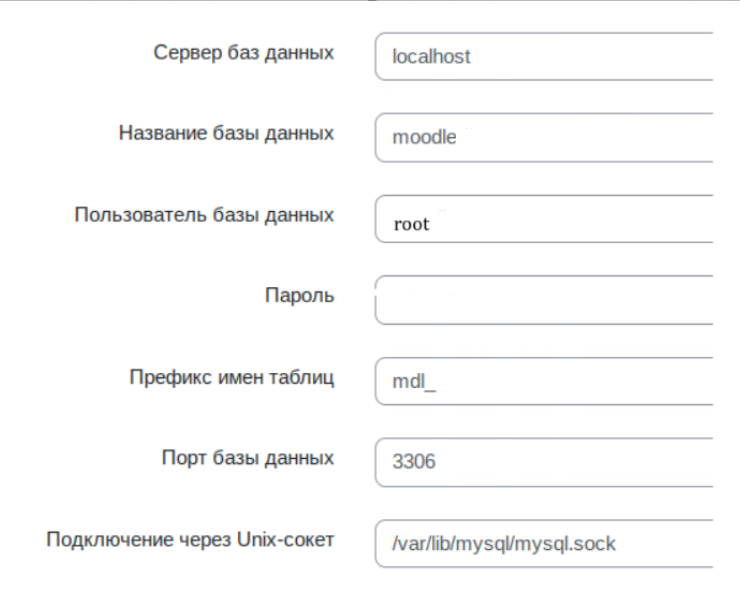
### Развертка moodle

После этого открываем сайт:

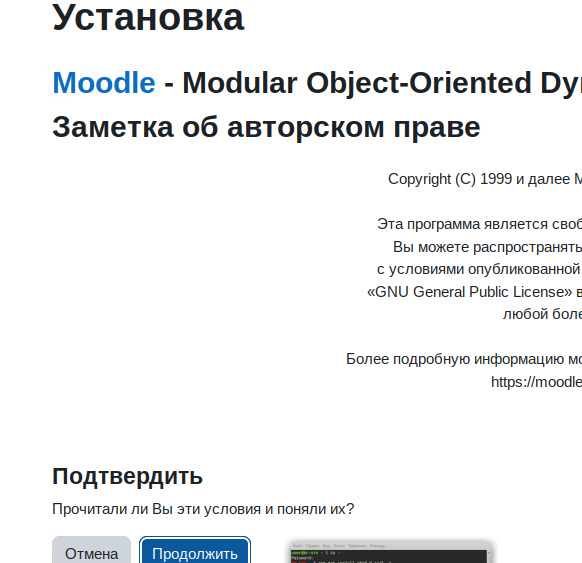
Выбираем язык

Проверяем, чтобы верно были указаны каталоги

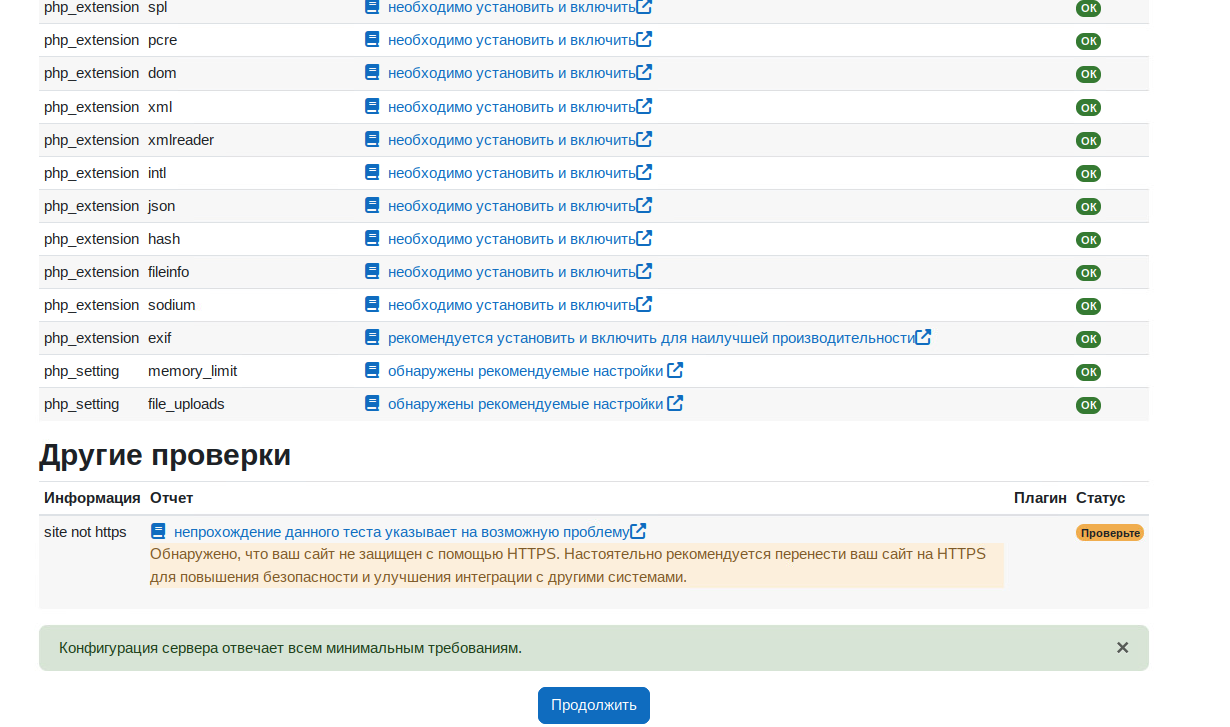
Выбираем базу данных MariaDB и указываем параметры подключения к ней:



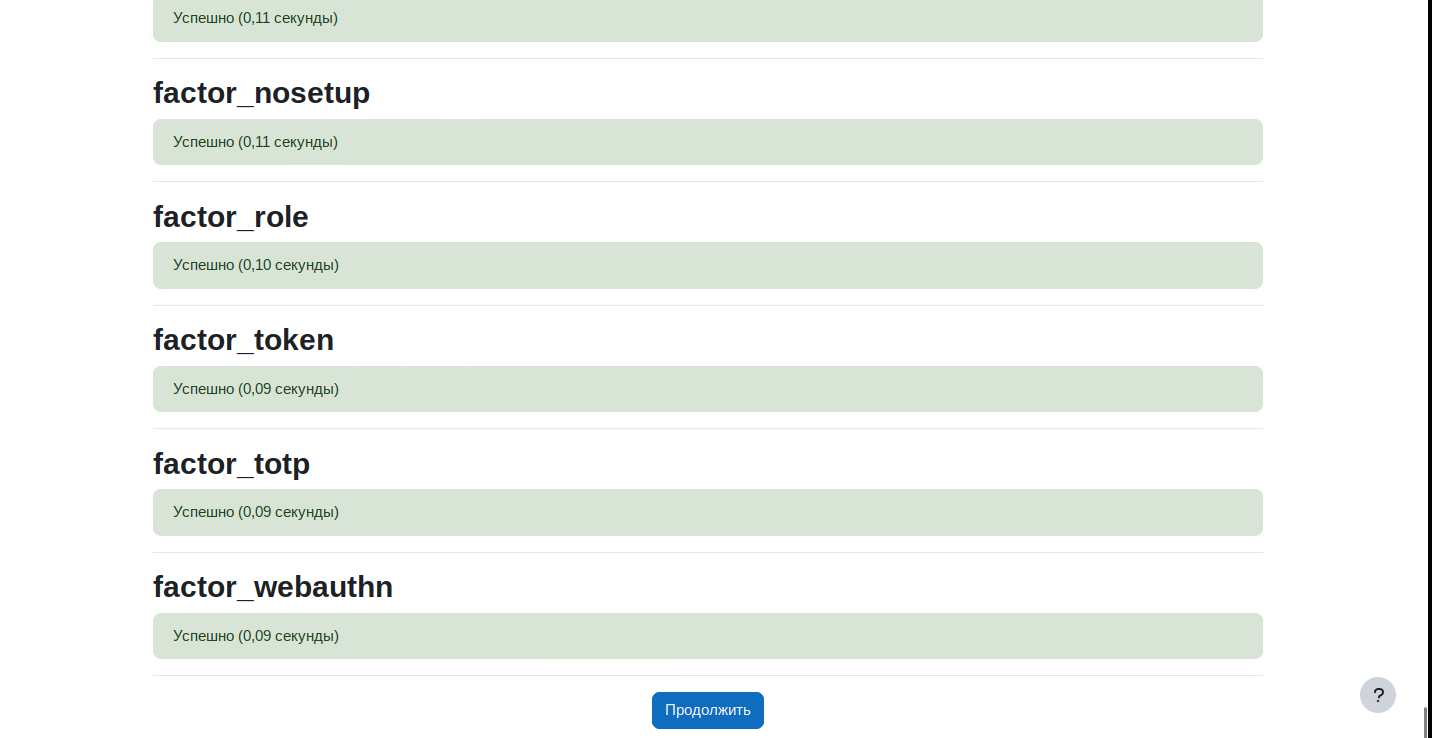
Принимаем условия



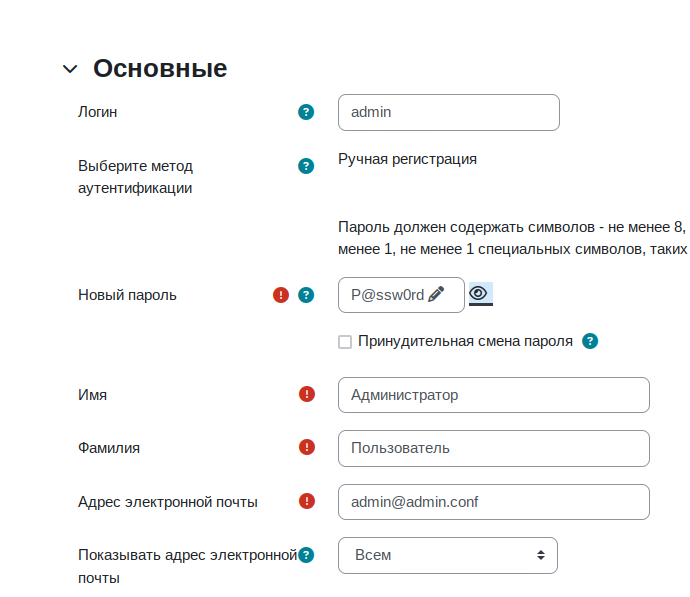
Проверяем, что конфигурация сервера отвечает минимальным требованиям , если нет, то устраняем проблемы

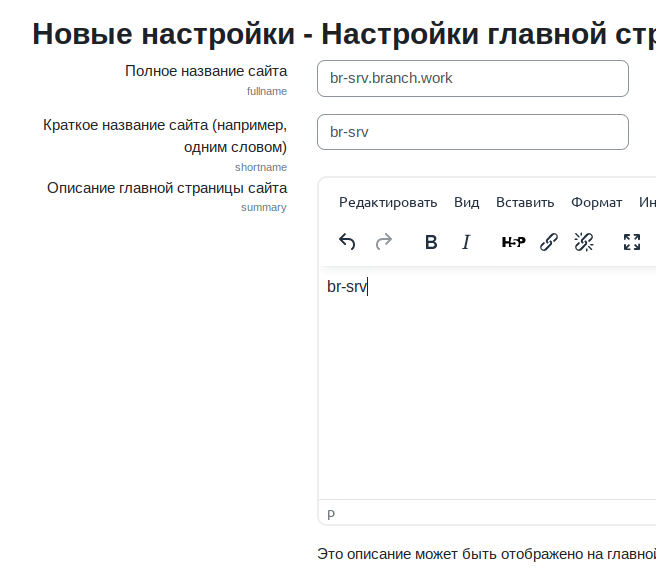


Жмем продолжить

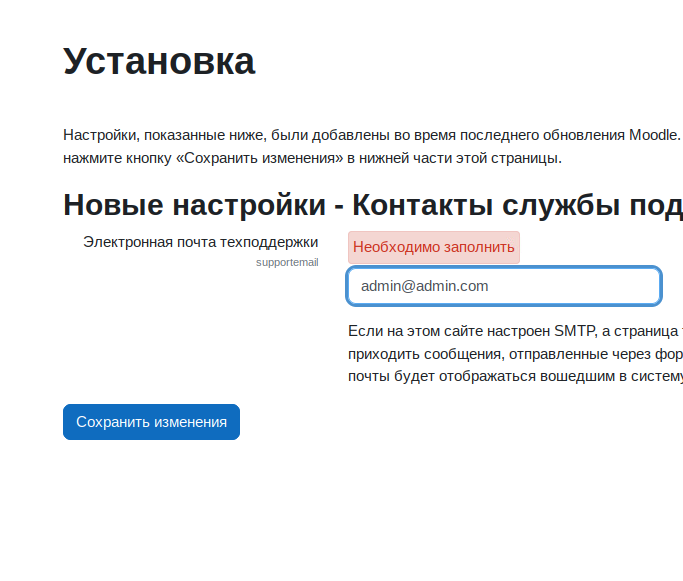


Указываем обязательные данные

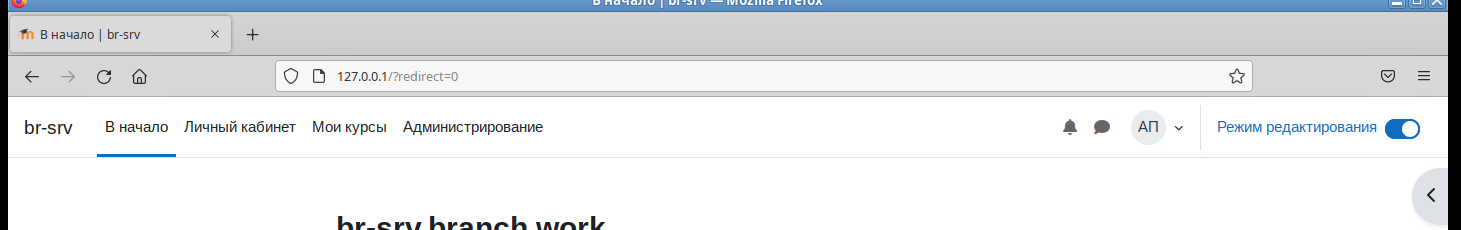


Прописываем параметры главной страницы(абсолютно любые)

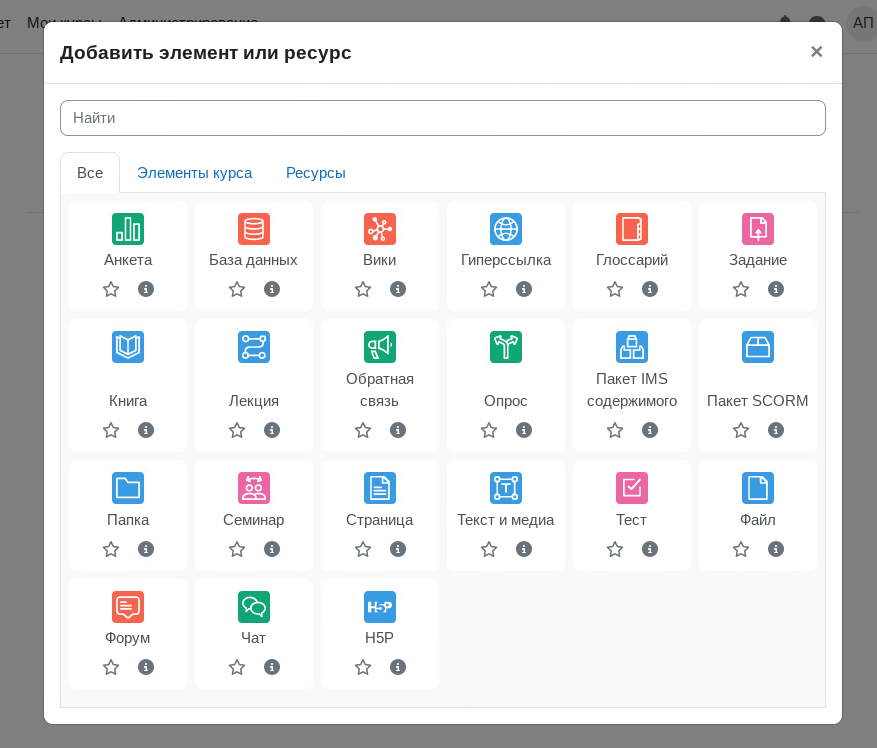
Любые контакты



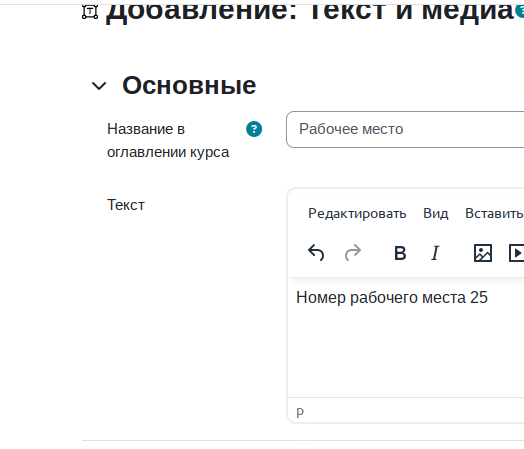
Перейти во вкладку “В начало” и включить режим редактирования



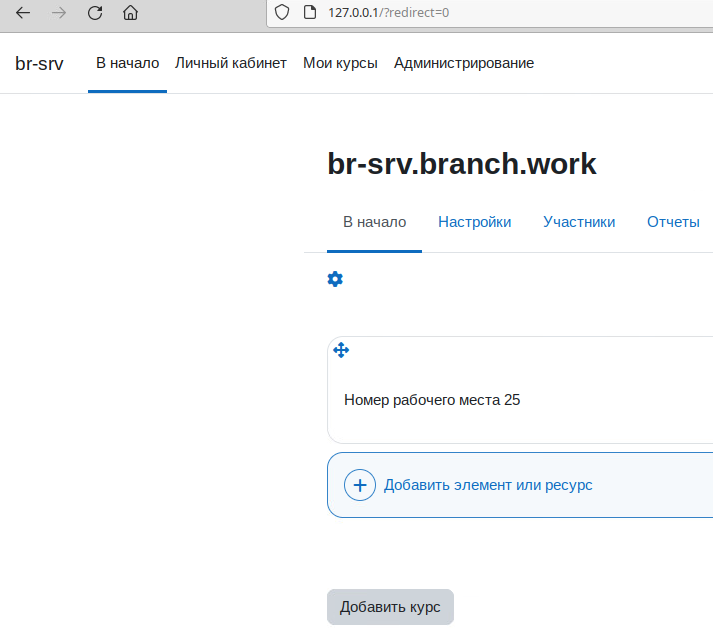
Добавляем элемент или ресурс “Текст и медиа”



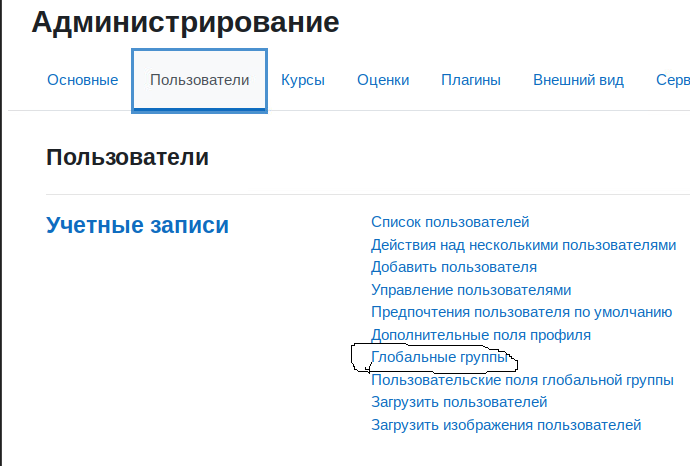
И указываем в поле текст номер рабочего места



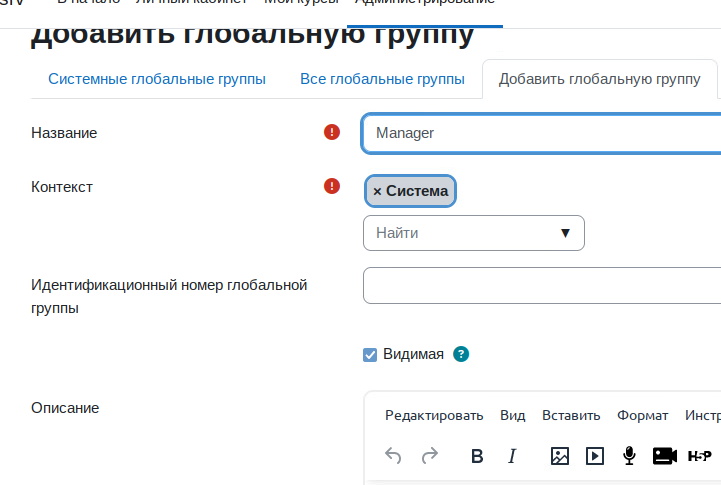
Теперь на главной странице отображается номер рабочего места



Далее необходимо создать группы и пользователей в соответствии с таблицей. Для этого переходим в раздел “Администрирование”, “Пользователи”, “Учетные записи”, “Глобальные группы”

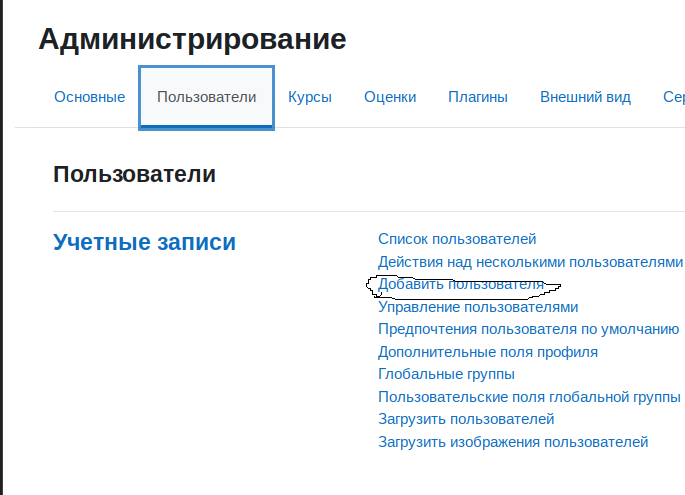


Жмем “Добавить глобальную группу” и создаем необходимые группы

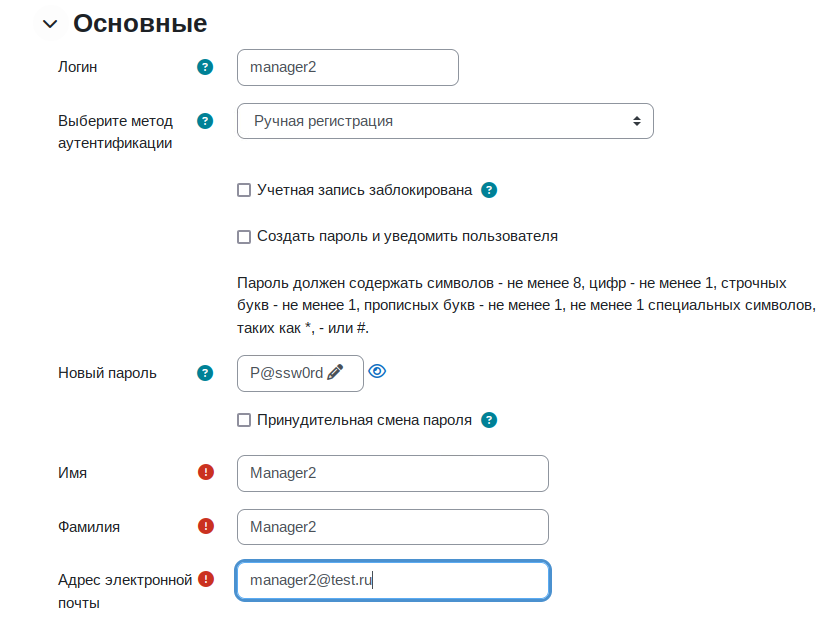


Далее необходимо создать пользователей и присоединить его к соответствующей группе.

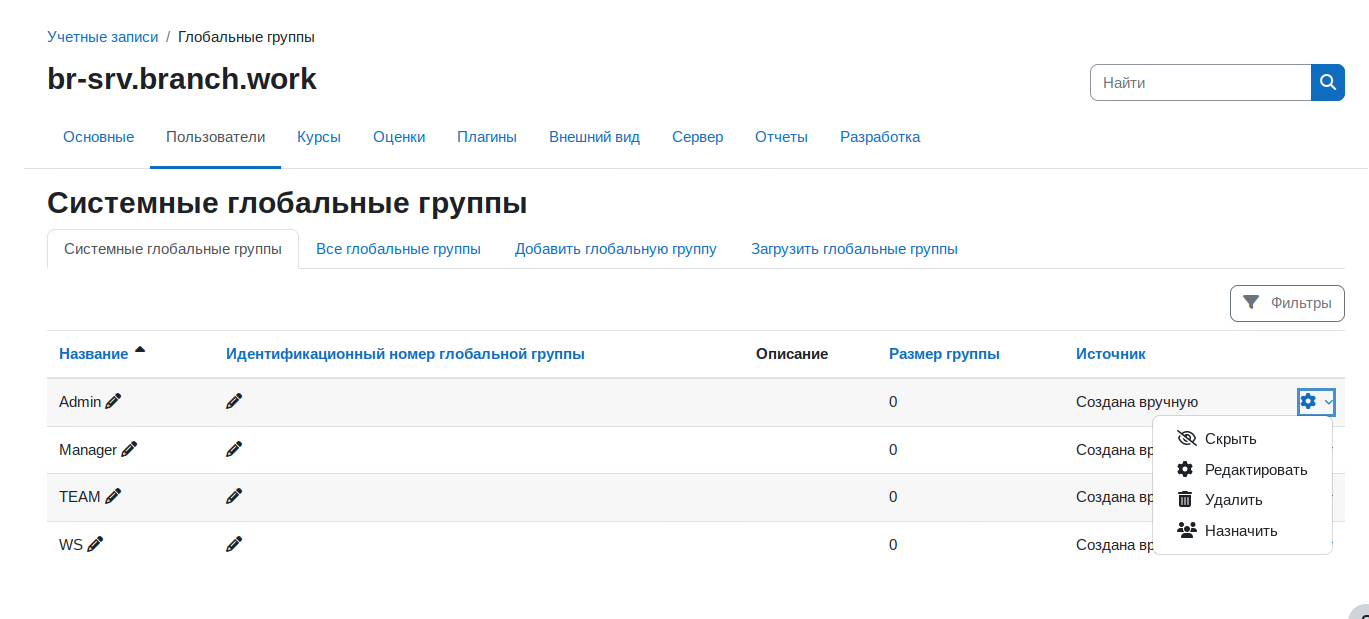
Для этого переходим в “Администрирование”, “Пользователи”, “Учетные записи”, “Добавить пользователя”:



Создаем пользователей:



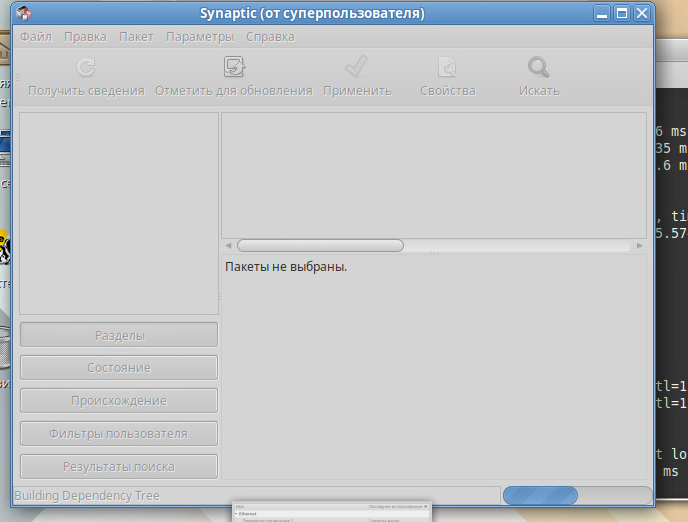
Далее необходимо добавить пользователей в соответствующие группы, для этого необходимо перейти снова к “Глобальные группы”, выбрать группу и нажать “Назначить”



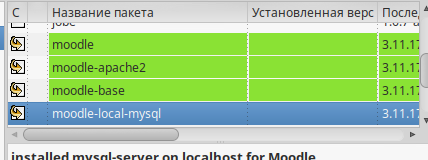
И выбираем пользователей

### Способ 2:

Открываем данную программу



Ставим пакеты:



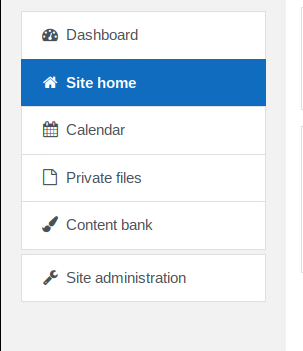
После запускаем apache и mysql:

**root@br-srv:~#** systemctl enable —-now httpd2 mariadb

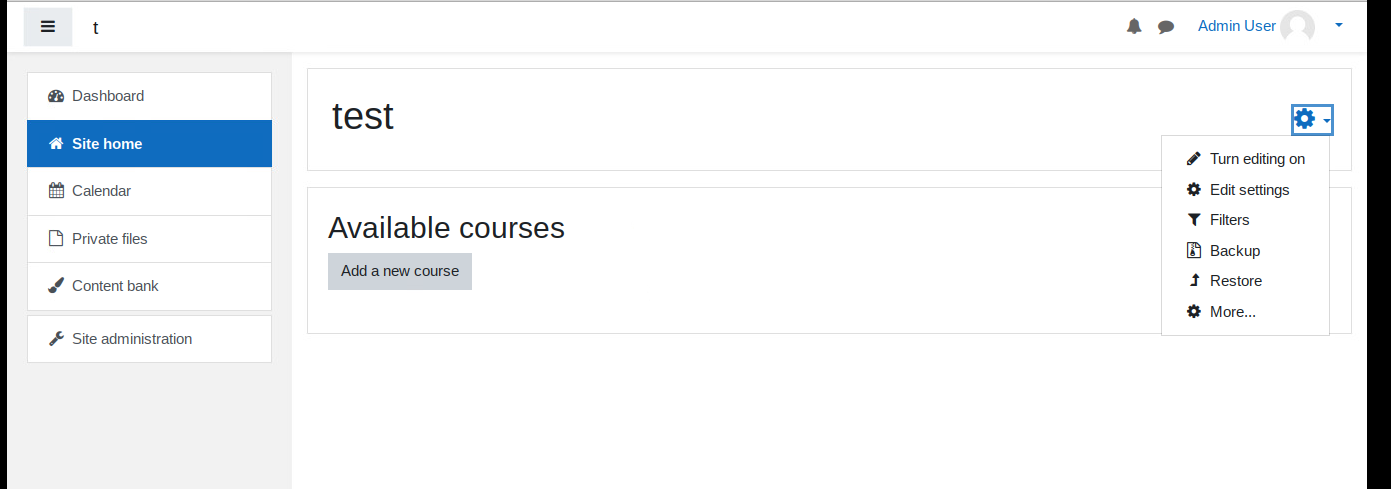
и далее всё также, как в первом способе, заходим на <http://localhost>/moodle и выполняем установку как написано [тут](#_onlqpxpngdp0) и не забываем [отредактировать параметр php](#_k5ctsifb8jef).

### Настройка подписи способ 2

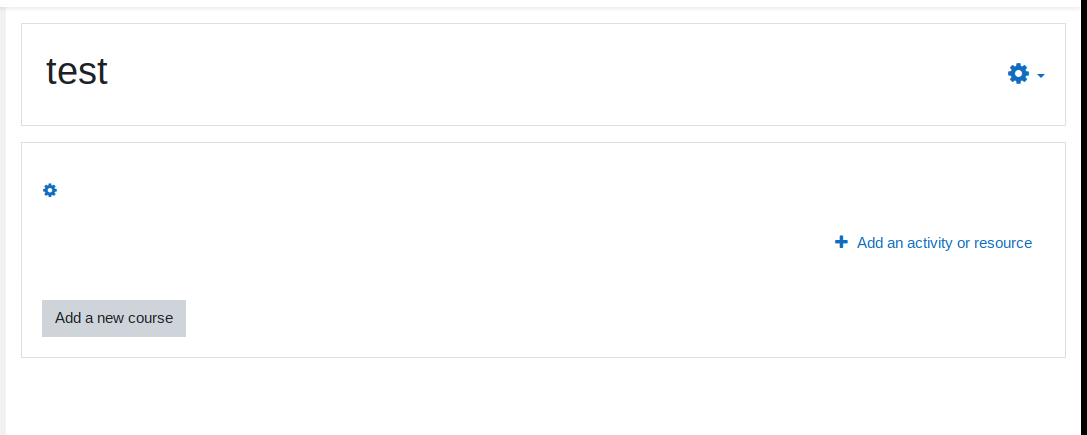
Настройка подписи рабочего места в данном случае выполняется следующим способом. Переходим на домашнюю страницу сайта:



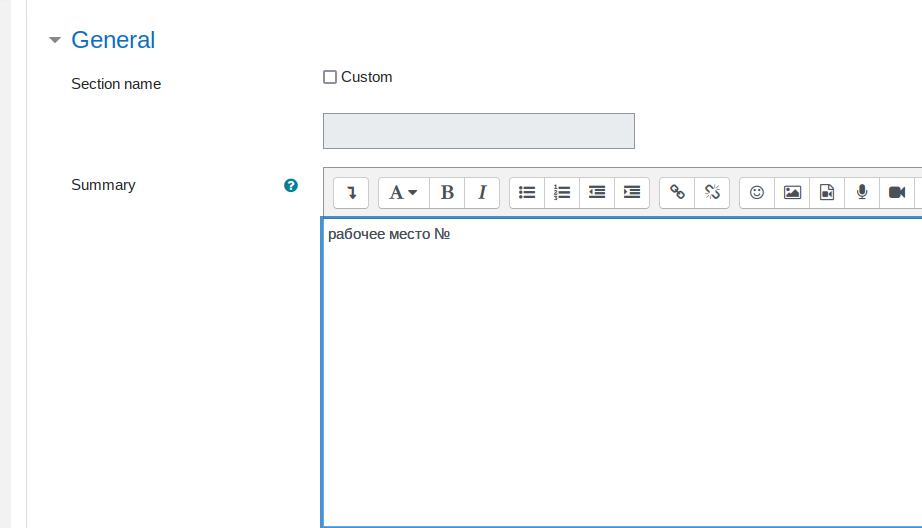
Далее Turn editing on



Жмем на шестереночку, которая под надписью “test”



В поле Summary пишем номер рабочего места



Сохраняем

Создание пользователей выполняется похожим с первым способом, для этого переходим в раздел Site administration и далее всё тоже самое.

На этом настройка LMS Moodle окончена.

# Домен Freeipa

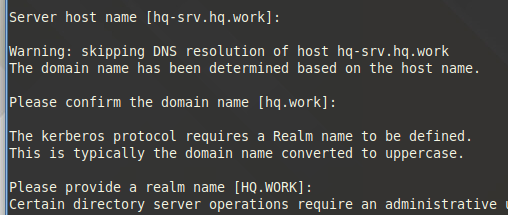
Настраивается на устройстве HQ-SRV. Для этого необходимо установить следующие пакеты:

**root@hq-srv:~#** apt-get install freeipa-server freeipa-server-dns -y

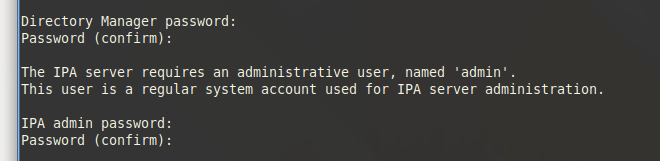
Далее прописываем команду для установки freeipa:

**root@hq-srv:~#** ipa-server-install —-setup-dns —-allow-zone-overlap

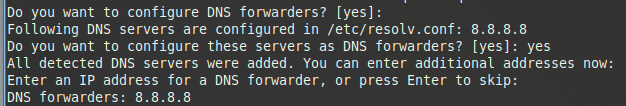
Подтверждаем имя сервера, доменное имя и real name:



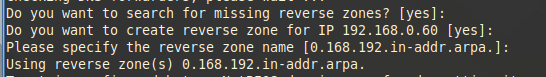
Далее вводим пароль для менеджера каталогов(например, P@ssw0rd) и пароль учетной записи админа(P@ssw0rd)



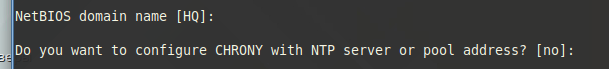
Далее будет предложено указать сервер пересылки. Соглашаемся с предложением и далее либо выбираем предложенный сервер, который был взят из /etc/resolv.conf или же указываем другой/добавляем еще.



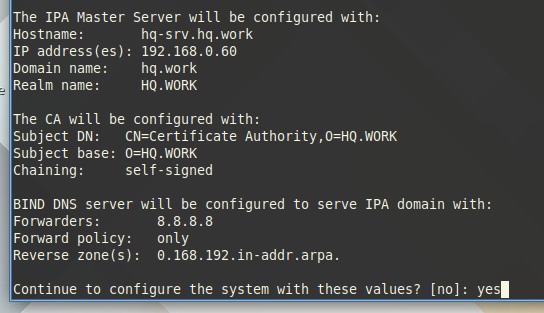
Соглашаемся с созданием обратной зоны DNS



Подтверждаем NetBios имя и отказываемся от настройки ntp сервера:

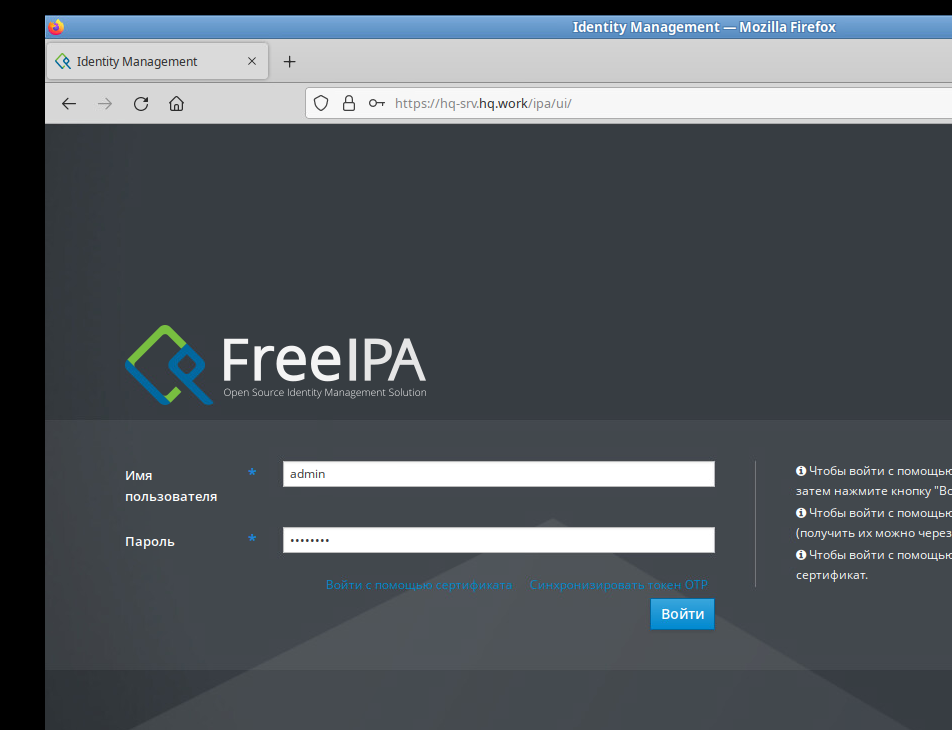


Подтверждаем выбранную нами конфигурацию

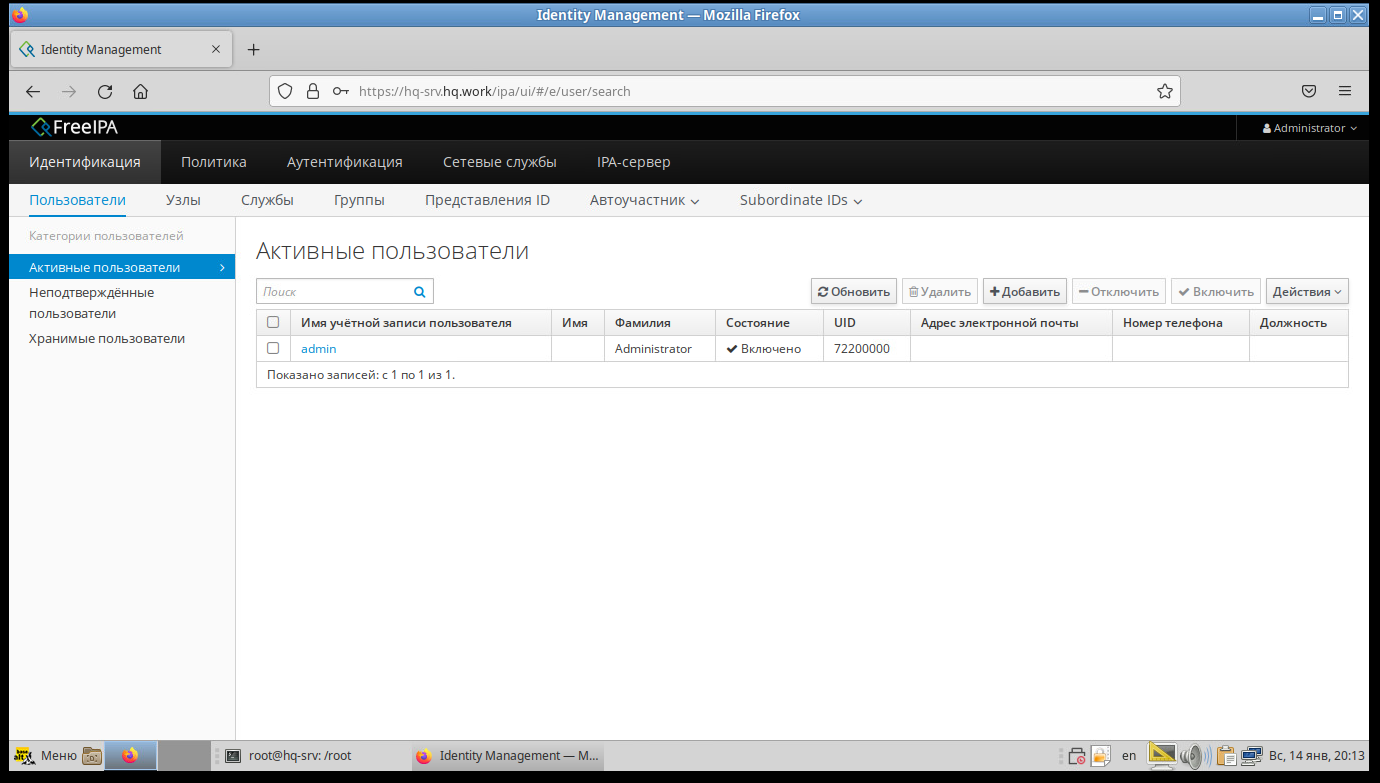


!!!Учитывайте, что установка контроллера домена Freeipa по времени занимает ~10 минут, чтобы не сидеть и не ждать просто так, можно делать другие пункты задания.

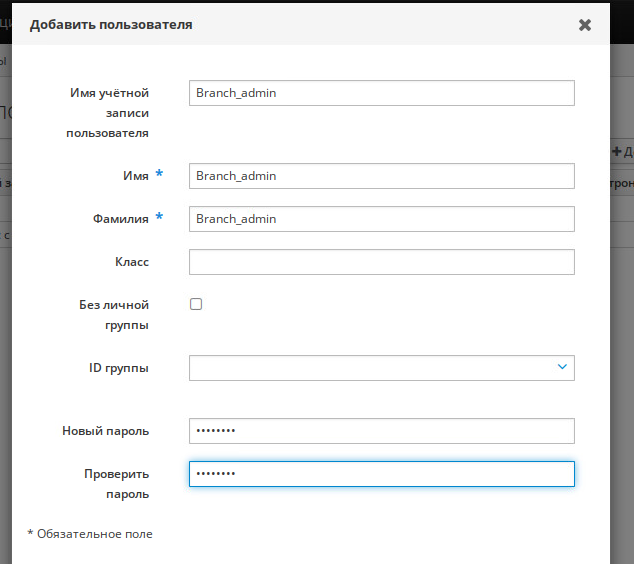
Далее переходим в браузер по адресу <https://hq-srv.hq.work/>. Откроется окно авторизации в котором надо ввести имя пользователя admin и пароль P@ssw0rd



По заданию требуется создать пользователей, которые прописаны в таблице 2 задания. Для этого переходим во вкладку “Пользователи” и добавляем необходимых пользователей

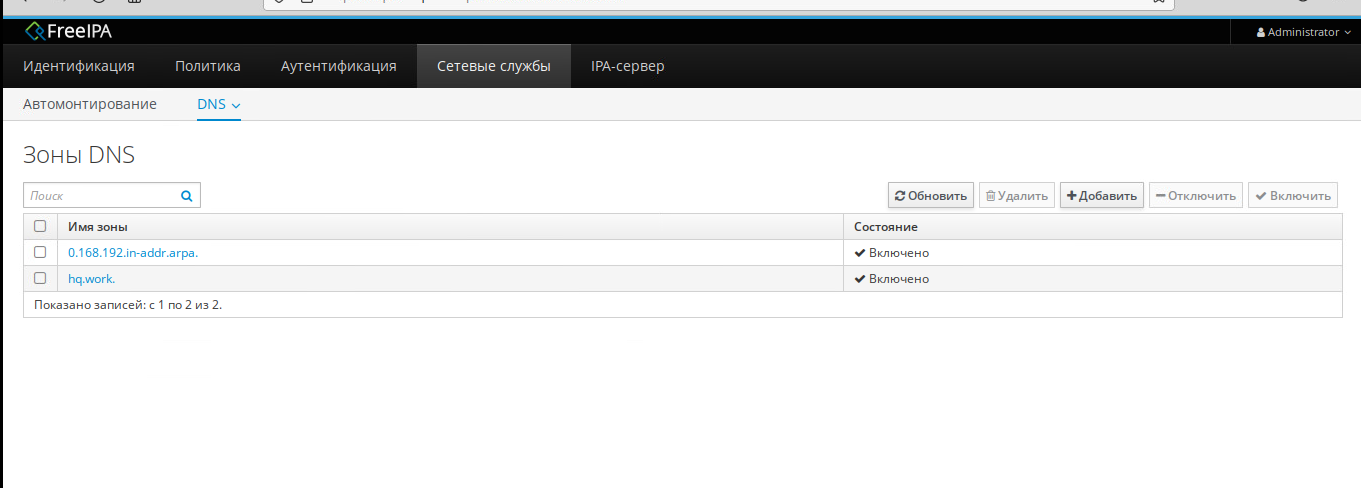


И создаем пользователя



## Настройка DNS

Настройка DNS в Freeipa. При установке домена мы уже создали автоматически и прямую и обратную зоны. Они находятся по следующему пути:



Необходимо просто добавить записи необходимых устройств, согласно заданию(см. задание 1 модуля 2).

## Ввод устройств в домен

Ввод BR-SRV и CLI в домен. Для начала необходимо установить следующие пакеты:

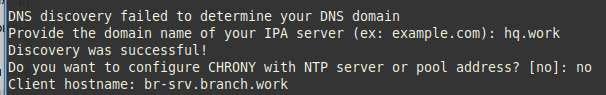
**root@br-srv&&cli:~#** apt-get install freeipa-client task-auth-freeipa -y

Перед вводом в домен проверяем, что контроллер домена доступен с устройства (ping hq-srv.hq.work).

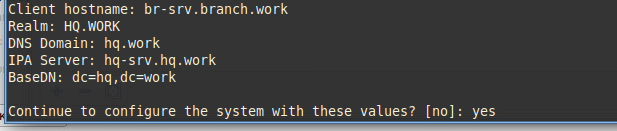
После подготовки вводим в домен

**root@br-srv&&cli:~#** ipa-client-install

Указываем имя домена и отказываемся от настройки ntp:



Подтверждаем параметры:



Указываем пользоватея admin для присоединения к домену и вводим пароль



После ввода в домен необходимо перезагрузить устройство и можно выполнять авторизацию доменных пользователей.

# Backup-скрипт

Для его работы необходимо настроить подключение ssh для рута(если делали подключение по сертификатам для пользователей, то рута не включаем)

Необходимо продемонстрировать его работу, путем занесения в отчет, доказывающих работоспособность. Для начала создадим директории, куда будут сохранятся настройки сетевых настроек

**root@hq-srv:~#** mkdir -p /backup/hq-r

**root@hq-srv:~#** mkdir /backup/br-r

После пишем сам скрипт, для этого на hq-srv создаем любой файл и заносим туда следующее:

**root@hq-srv:~#** vim backup

#!/bin/bash

scp -r root@192.168.0.1:/etc/network/ /backup/hq-r

scp -r root@172.16.0.1:/etc/network/ /backup/br-r

Запускаем скрипт:

**root@hq-srv:~#** bash script

Заносим в отчет сам скрипт и показываем, что в /backup/hq-r и /backup/br-r появились файлы.

!!! Для тех, кто настраивает интерфейсы через nmtui скрипт будет выглядеть следующим образом:

**root@hq-srv:~#** vim backup

#!/bin/bash

scp -r root@192.168.0.1:/etc/Network-Manager/system-connection /backup/hq-r

scp -r root@172.16.0.1:/etc/Network-Manager/system-connection/ /backup/br-r

# Проброс порта для SSH

Осуществляется на HQ-R, путем написания следующей команды:

**root@hq-r:~#** iptables -t nat -A PREROUTING -p tcp —-dport 22 -j DNAT —-to-destination 192.168.0.60:2222

# Контроль доступа по SSH

Необходимо на HQ-SRV открываем файл и в конце пишем:

**root@hq-srv:~#** vim /etc/hosts.deny

sshd:10.0.0.10

# Сохранение правил iptables

Проверяйте, что после перезагрузки hq-r и br-r все правила iptables остаются включенными, для этого:

iptables-persistent

**root@hq-r&&br-r:~#** apt install iptables-persistent -y

В всплывающих окнах жмем “yes”

После внесения изменений в iptables не забываем прописать следующее:

**root@hq-r&&br-r:~#** iptables-save > /etc/iptables/rules.v4

# Файловый сервер NFS

Перед этим должен быть настроен и поднят домен freeipa, далее:

**root@hq-srv:~#** apt-get install nfs-server -y

Создаем папки на сервере, которые откроем в общий доступ:

**root@hq-srv:~#** mkdir /Branch\_Files /Network /Admin\_Files

И создаем папки для монтирования:

**root@hq-srv&&br-srv:~#** mkdir /mnt/branch /mnt/network /mnt/admin

Для автомонтирования необходимо на hq-srv и br-srv сказать следующие пакеты(названия этих пакетов и прочее есть в документации альта, которая лежит на рабочем столе(пункт 42.6.2))):

**root@hq-srv&&br-srv:~#** apt-get install pam\_mount cifs-utils systemd-settings-enable-kill-user-processes -y

Вносим изменения в конфиг, дописываем в самый конец)

**root@hq-srv&&br-srv:~#** vim /etc/pam.d/system-auth

session [success=1 default=ignore] pam\_succeed\_if.so service = systemd-user quiet

session optional pam\_mount.so disable\_interactive

Далее добавляем volume(перед тегом cifsmount) для монтирования в файл:

**root@hq-srv&&br-srv:~#** vim /etc/security/pam\_mount.conf.xml

<volume user=”admin” fstype=”nfs” server=”hq-srv.hq.work” path=”/Admin\_Files” mountpoint=”/mnt/admin” />

<volume user=”network-admin” fstype=”nfs” server=”hq-srv.hq.work” path=”/Network” mountpoint=”/mnt/network” />

<volume user=”branch-admin” fstype=”nfs” server=”hq-srv.hq.work” path=”/Branch\_Files” mountpoint=”/mnt/branch” />

Настройка nfs производится в следующем файле:

**root@hq-srv:~#** vim /etc/exports

/Branch\_Files 192.168.0.0/26 (rw,sync,all\_squash,no\_subtree\_check)

/Branch\_Files 172.16.0.0/28 (rw,sync,all\_squash,no\_subtree\_check)

/Network 172.16.0.0/28 (rw,sync,all\_squash,no\_subtree\_check)

/Network 192.168.0.0/26 (rw,sync,all\_squash,no\_subtree\_check)

/Admin\_Files 192.168.0.0/26 (rw,sync,all\_squash,no\_subtree\_check)

/Admin\_Files 172.16.0.0/28 (rw,sync,all\_squash,no\_subtree\_check)

Перезагружаем nfs

**root@hq-srv:~#** systemctl restart nfs-server

Готово!!!

# Bacula

Выполняется на hq-srv.

Данная статья может помочь дополнительно, все материалы показаны ниже, взяты оттуда (<https://www.altlinux.org/Bacula>)

**root@hq-srv:~#** apt-get install bacula13-common bacula13-console bacula13-director-common bacula13-director-mysql bacula13-storage mt-st mariadb-server -y

Запускам базу данных и создаем директорию для сохранения бекапов

**root@hq-srv:~#** systemctl enable —-now mariadb

**root@hq-srv:~#** mkdir -p /srv/backup

**root@hq-srv:~#** chown bacula -R /srv/backup

Задаем пароль для пользователя bacula в базе данных:

**root@hq-srv:~#** nano /usr/share/bacula/scripts/grant\_mysql\_privileges

. . .

db\_password=”P@ssw0rd”

. . .

Создаем скриптом базу данных, таблицы, пользователя и привилегии для пользователя:

**root@hq-srv:~#** /usr/share/bacula/scripts/create\_mysql\_database

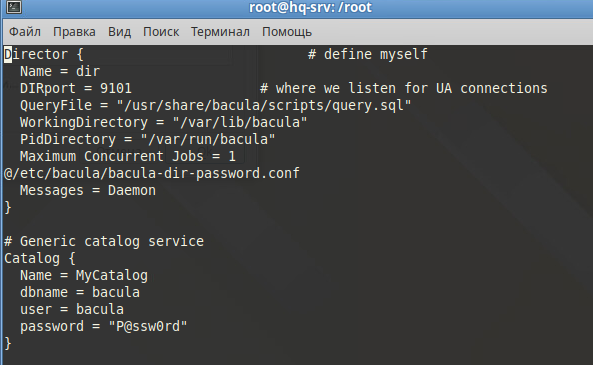
**root@hq-srv:~#** /usr/share/bacula/scripts/make\_mysql\_tables

**root@hq-srv:~#** /usr/share/bacula/scripts/grant\_mysql\_privileges

Далее переходим к настройке файлов, чтобы настроить бекап:

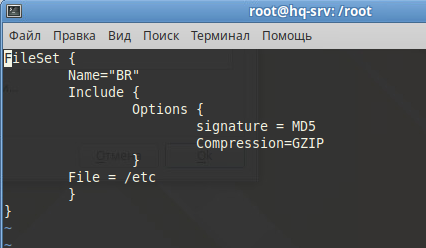
**root@hq-srv:~#** nano /etc/bacula/bacula-dir.conf

Приводим к такому виду:



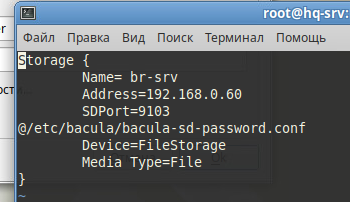
Создаем файл

**root@hq-srv:~#** nano /etc/bacula/fileste.d/brsrv.conf



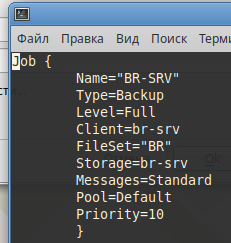
Создаем файл

**root@hq-srv:~#** nano /etc/bacula/storage.d/brsrv.conf



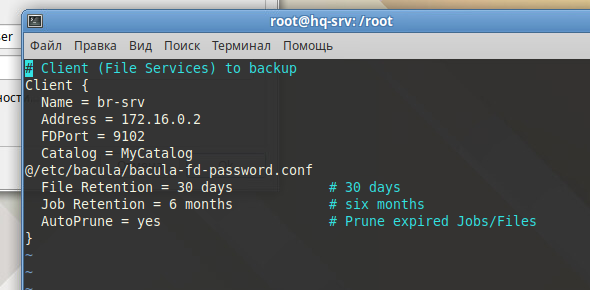
Создаем файл

**root@hq-srv:~#** nano /etc/bacula/jobs.d/brsrv.conf



Создаем файл

**root@hq-srv:~#** nano /etc/bacula/client.d/client2.conf



Также необходимо зайти в файлы ниже и прописать пароль “P@ssw0rd”

/etc/bacula/bacula-dir-password.conf

/etc/bacula/bacula-sd-password.conf

/etc/bacula/bacula-fd-password.conf

Перезапускаем bacula и добавляем в автозагрузку

**root@hq-srv:~#** systemctl restart bacula-dir bacula-fd bacula-sd

**root@hq-srv:~#** systemctl enable bacula-dir bacula-fd bacula-sd

Если на моменте рестарта возникают ошибки от bacula-dir и там написано “Нет доступа”, то необходимо выдать права 660 на вышесозданные файлы и дать пользователю bacula права доступа на эти файлы.

Настройка клиента

Переходим на br-srv, ставим пакет bacula13-client

**root@br-srv:~#** apt-get install bacula13-client

В файле bacula-fd-password.conf прописать пароль P@ssw0rd

**root@br-srv:~#** nano /etc/bacula/bacula-fd-password.conf

Перезапускаем клиента и добавляем в автозагруку

**root@br-srv:~#** systemctl restart bacula-fd

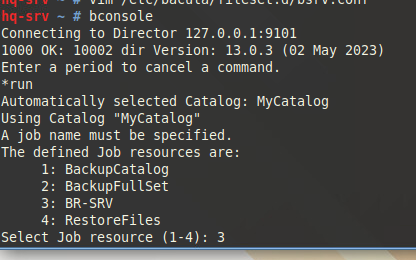
**root@br-srv:~#** systemctl enable bacula-fd

Пробуем выполнить бекап

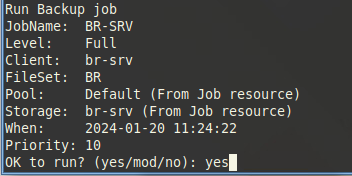
**root@br-srv:~#** bconsole

run

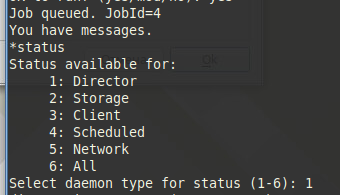
Выбираем созданное задание



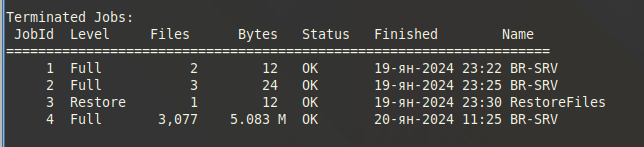
Подтверждаем



Прописываем status и смотрим произошел ли бекап



Видим, что status OK.



Если в директории /srv/backup появился файл и его содержание выглядит примерно так, то всё работает

