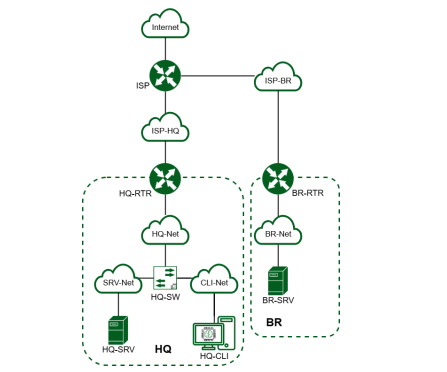
**Обновлено 09.04.2024 V1.3**



**Преднастройка**

Если в задании не будут использоваться встроенные репозитории, а будет возможность скачивать все пакеты из интернета, необходимо отключить проверку пакетов через cdrom зайдя по пути

**Nano /etc/apt/sources.list**

и закомментировать находящуюся там строку.

**Для коректной работы сети используй NMTUI только на машине ISP. На остальных машинах настройку IP-адресации производите через файл конфигурации /etc/network/interfaces**

**Задание 1 модуля 1**

1. Произведите базовую настройку устройств

● Настройте имена устройств согласно топологии. Используйте полное доменное имя

***Примечание:*** для выполнения данного задания необходимо постоянное изменение имени каждого устройства, указанного на топологии (временно изменение, действует только до перезагрузки системы и не является верным выполнением задания)

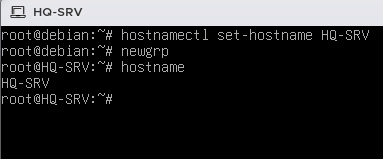
***Решение:***

Для фиксированного изменения имени компьютера, необходимо использовать команду:

**hostnamectl set-hostname Имя устройства**

Для изменения имени компьютера в текущем сеансе без перезагрузки можно воспользоваться командой:

**newgrp**

Рисунок 1 — Пример изменения имени устройства

● Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов

● Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов

● Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов ● Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов

● Сведения об адресах занесите в отчёт, в качестве примера

|  |  |
| --- | --- |
| Имя устройства | IP |
| HQ-CLI | 192.168.200.2 255.255.255.240 — к HQ-RTR |
| ISP | 172.16.4.1 255.255.255.240 — к HQ-R  172.16.5.1 255.255.255.240 — к BR-R |
| HQ-RTR | 192.168.100.1 255.255.255.192 — к HQ-SRV  172.16.4.2 255.255.255.240 — к ISP  192.168.200.1 255.255.255.240 — к HQ-CLI |
| HQ-SRV | 192.168.100.2 255.255.255.192 — к HQ-RTR |
| BR-RTR | 192.168.0.1 255.255.255.224 — к BR-SRV  172.16.5.2 255.255.255.240— к ISP |
| BR-SRV | 192.168.0.2 255.255.255.224— к BR-RTR |
| Сеть управления (VLAN 999) | 192.168.999.0 255.255.255.248 |

Следующим шагом необходимо установить выбранные IP адреса на соответствующие машины, для этого существуют 2 способа.

**Первый способ: через network-manager**

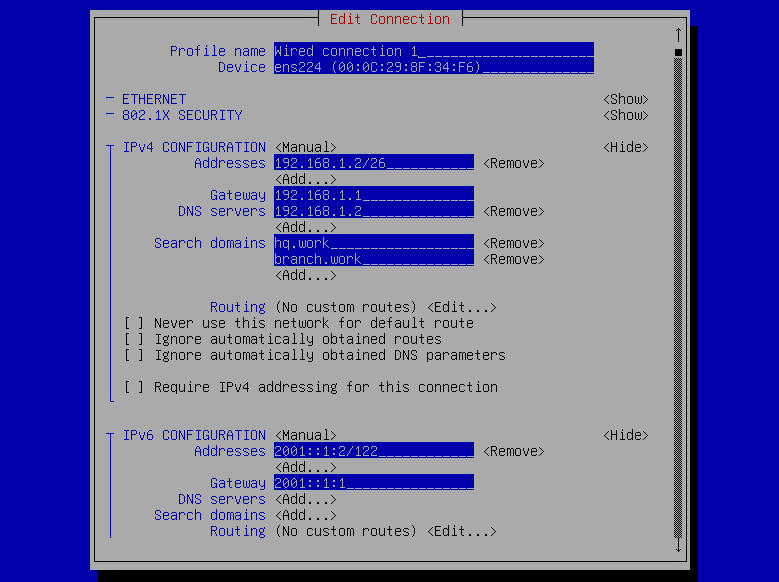
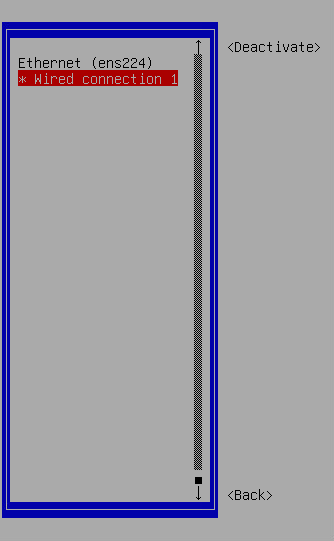


Рисунок 3 — Пример настройки IPv4 и IPv6 на HQ-SRV

После настройки необходимо зайти в activate a connection и перезагрузить все интерфейсы (нажать deactivate и activate на каждом интерфейсе)

Рисунок 4 — перезагрузка интерфейсов

**Примечание:** на интерфейсах, находящихся между маршрутизаторами, не нужно указывать dns, достаточно это сделать на внутренних локальных интерфейсах маршрутизаторов.

**Второй способ: через редактирования конфига интерфейсов**

Вариант ручной настройки без использования любых программ (в случае если не будет возможности установки nmtui или она будет запрещена). Перед установкой интерфейсов необходимо воспользоваться командой IP A для определения имён 7интерфейсов, находим незаполненный интерфейс, в примере ниже незаполненным интерфейсов является ens256

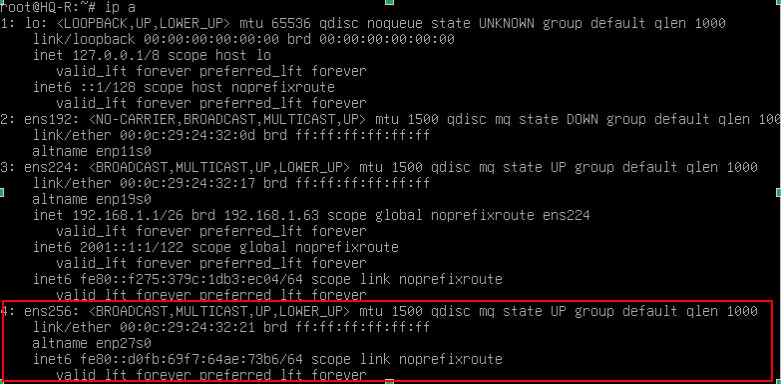


Рисунок 5— Поиск имён интерфейсов для настройки

Определив интерфейс, необходимо воспользоваться командой для просмотра и изменения конфигураций интерфейсов

**nano /etc/network/interfaces**

***или***

**vi /etc/network/interfaces**

И затем сконфигурировать настройки интерфейсов в соответствии с таблицей адресации по примеру, представленному на скриншоте ниже

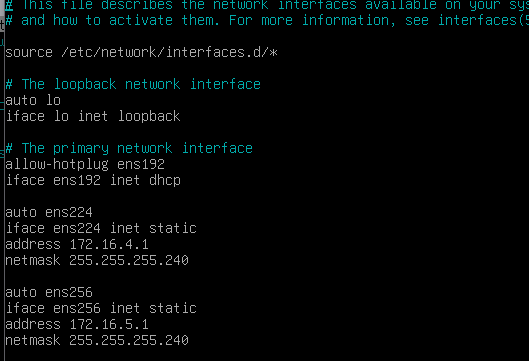


Рисунок 6 — Пример настройки интерфейсов ISP

Для настройки VLAN на роутере HQ-RTR нужно скачать утилиту VLAN:

apt install vlan. Также нужно установить модуль 8021:

modprobe 8021q

и добавить его в автозапуск echo 8021q >> /etc/modules

Теперь можно преступить к настройке файла конфигурации /etc/network/interface. Он должен выглядеть следующим образом:

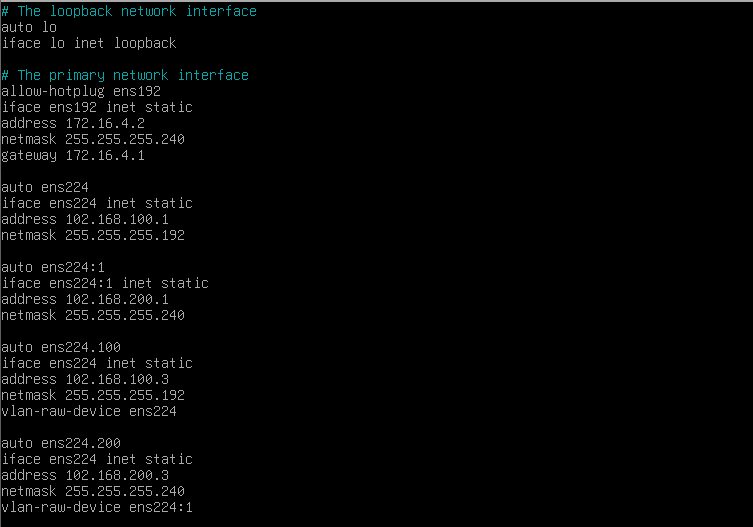


Рисунок 7 — Настройка интерфейсов HQ-RTR

2) Настройка ISP

iptables:

**apt-get install iptables iptables-persistent**

Затем нужно создать правила iptables

iptables –t nat –A POSTROUTING –s 172.16.4.0/28 –o ens192 –j MASQUERADE

iptables –t nat –A POSTROUTING –s 172.16.5.0/28 –o ens192 –j MASQUERADE

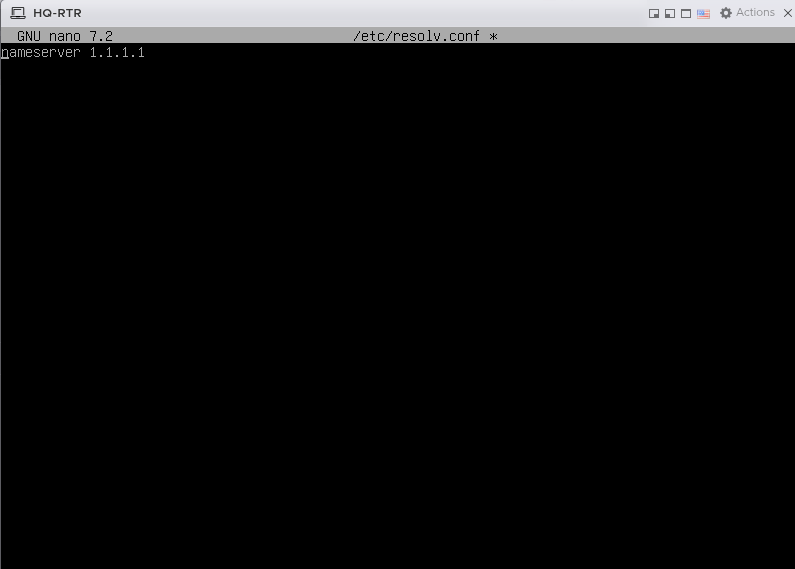
iptables-save > /etc/iptables/rules.v4

Перезапускаем iptables: systemctl restart iptables

Для проверки вводим команду **iptables –L –t nat**

После настройки на интерфейсах ISP может слететь Ip. Также на роутерах и ISP нужно зайти в файл /etc/sysctl.conf и раскомментировать строку «**net.ipv4.ip\_forward=0» и привести её к виду «net.ipv4.ip\_forward=1». Также для работы nat и доступа в интернет на роутерах в качестве gateway указать адрес ISP.**

**На HQ-RTR и BR-RTR Нужно зайти в файл /etc/resolv.conf и оставить там только одну строку: nameserver 1.1.1.1**

Рисунок 8 — Пример настройки интерфейсов ISP

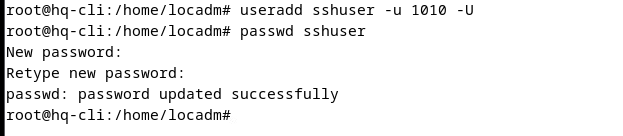
**Правила для HQ-RTR**

iptables –t nat –A POSTROUTING –s 192.168.100.0/26 –o ens192 –j MASQUERADE

**3. Создание локальных учётных записей**

**adduser sshuser**

Затем появится поле ввода пароля как показано на рисунке 9

Рисунок 9 — окно ввода пароля при создании пользователя

**Для смены id используется команда usermode -u 1010 sshuser**

Так же возможно понадобится выдать Root права для данных клиентов это можно выполнить посредством команды **visudo**

в открывшемся окне необходимо вписать изменения для каждой новой созданной учётной записи как показано на рисунке 10



**Рисунок 10 — выдача Root прав пользователям**

**5. Настройка безопасного удалённого доступа**

Первым делом необходимо перейти по пути **nano /etc/ssh/sshd\_config** где в окне конфигурации нам необходимо на HQ-SRV найти строки и изменить значения как указанно на рисунке 10

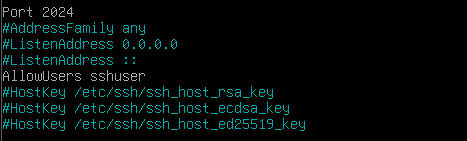
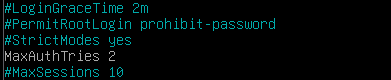


Рисунок 10— смена порта доступа по ssh и права подключения только определённого пользователя



**Рисунок 11— Ограничение попыток авторизации**



**Рисунок 12— Указание файла баннера**

Для настройки баннера нужно зайти в файл /etc/ssh-banner и написать следующее: Authorized acces only



**Рисунок 13— баннера**

**Для применения конфигурации необходимо перезагрузить службу командой systemctl restart ssh**

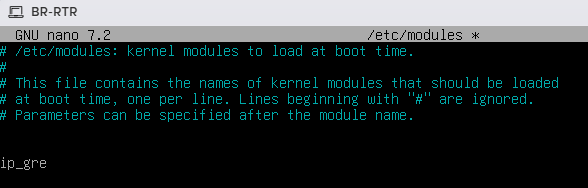
Для проверки доступа нужно написать команду: ssh sshuser@192.168.100.2 -p 2024

Где -p — указание порта. Без указания порта подключится не получится

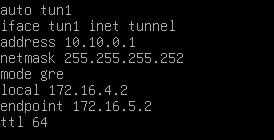
Также, при неправильном вводе пароля должно вывестись сообщение баннера

**6) Реализация GRE-туннеля между офисами**

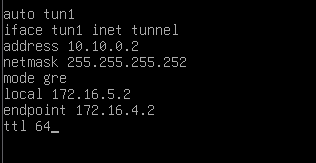
Нужно зайти в файл /etc/modules и добавить там строку ip\_gre:



Вся последующая настройка проводится в файле /etc/network/interfaces

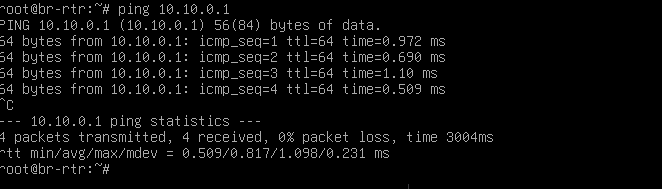


**Рисунок 14 - Настройка GRE на HQ-RTR**



**Рисунок 15 - Настройка GRE на BR-RTR**

Ping 10.10.0.1 и ping 10.10.0.2 для проверки работоспособности туннеля с обеих сторон:

**Рисунок 16 – Проверка работоспособности**

**8. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.**

**Решение:** Первым делом необходимо установить пакеты FRR, для этого необходимо воспользоваться командой:

**apt install frr**

Следующим шагом необходимо произвести изменения конфигурационных файлов

**nano /etc/frr/daemons**

и изменить параметры на YES для протокола OSPF

Рисунок 17 — настройка конфигурации FRR

После сохранения конфига, следующим шагом необходимо, перезапустить frr.service командой

**systemctl restart frr**

Далее, после перезагрузки, посредством команды **vtysh** перейти в режим конфигурирования (Настройки идентичны Cisco IOS).

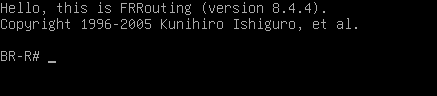


Рисунок 18 — пример конфигурационного окна

Посредством команд:

**Conf t**

**router ospf**

перейти к конфигурированию протокола ospf

Настройка производится посредством объявления

ospf router-id x.x.x.x

и прилегающих к маршрутизатору сетей

network x.x.x.x/x area x

как показано на рисунке 9

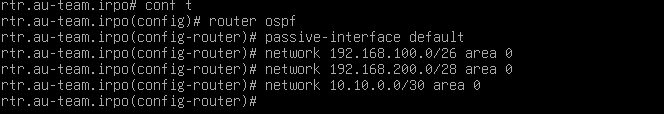


Рисунок 19 — пример настройки OSPF на HQ-RTR



Рисунок 20— Включение авторизации и последующая настройка интерфейса

**После завершения конфигурации в frr, необходимо записать конфигурацию в память устройства, командой write, иначе при перезагрузке frr или устройства, все настройки вернутся к дефолтным**

Для этого необходимо

Для завершения настройки сети необходимо сконфигурировать настройку для передачи пакетов между сетями в файле **nano /etc/sysctl.conf**

переменную **net.ipv4.ip\_forward=1 необходимо раскоментить** и сохранить изменения в файле, и применить изменения командой **sysctl -p**

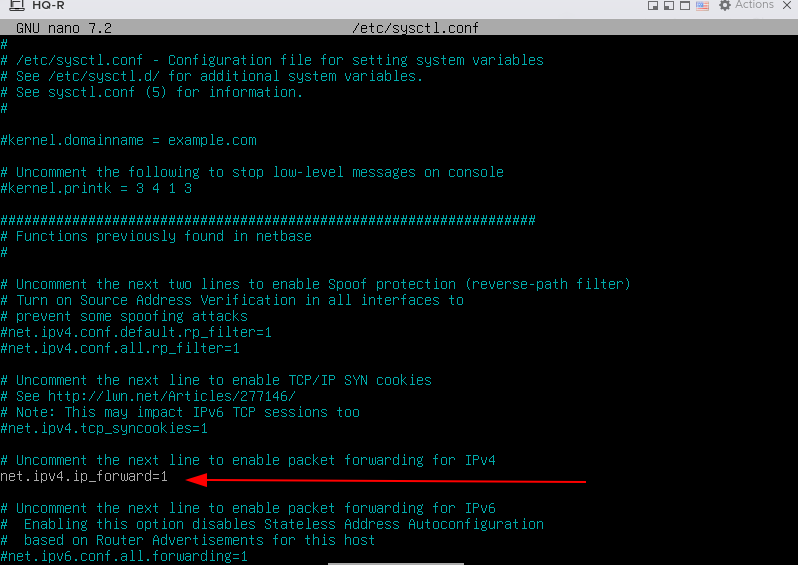


Рисунок 21 — настройка пересылки пакетов в режиме маршрутизатора

**Примечание: при каждой перезагрузке устройства, данная настройка будет изменятся обратно, что связано с загрузкой операционной системы на виртуальной машине для того, чтобы снова включить пересылку пакетов необходимо прописать sysctl -p**

**Идентичная настройка проводится на BR-RTR, только указывается другая подсеть(192.168.0.0/27). Указание сети туннеля и настройки авторизации абсолютно идентичны**

8) Настройка динамической трансляции адресов

Точно также как и для ISP устанавливаем пакеты iptables:

apt install iptables iptables-persistent

**iptables –t nat –A POSTROUTING –s 192.168.100.0/26 –o ens192 –j MASQUERADE**

**iptables –t nat –A POSTROUTING –s 192.168.200.0/28 –o ens192 –j MASQUERADE**

**Правило для BR-RTR**

**iptables –t nat –A POSTROUTING –s 192.168.0.0/27 –o ens192 –j MASQUERADE**

**Затем эти правила нужно сохранить: iptables-save > /etc/iptables/rules.v4**

**После этого перезапускаем службу**

**9.Настройте автоматическое распределение IP-адресов на роутере HQ-R.**

**a. Учтите, что у сервера должен быть зарезервирован адрес.**

Первым шагом необходимо на машине HQ-R установить dhcp server командой

**apt install isc-dhcp-server**

После установки пакета следующим шагом необходимо сконфигурировать файл для указания интерфейсов прослушивания DHCP сервера зайти можно с помощью команды

**nano /etc/default/isc-dhcp-server**

и настроить интерфейс, направленный в сторону клиента, если в сети подразумевается DHCP-relay, то 2 интерфейса в сторону клиента, и в сторону сети откуда исходит запрос. Строка v6 закоментирована, чтобы DHCP даже не думал пробовать его раздавать

Рисунок 22 — Указание интерфейса для передачи адреса

Далее необходимо настроить 2 конфигурационных файла для IPv4 для IPv6

Которые можно найти по путям **nano /etc/dhcp/dhcpd.conf** и **nano /etc/dhcp/dhcpd6.conf** соответственно

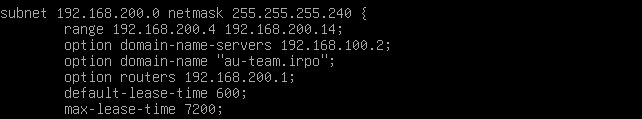


Рисунок 23— Пример настройки DHCP для ipv4 без Relay

**ddns-update-style interim** — способ автообновления базы dns

**authoritative** — делает сервер доверенным

**subnet** — указание сети

**range** — пул адресов

**option routers** — шлюз по умолчанию

***Перезапускаем службу DHCP: systemctl restart isc-dhcp-server***

Для проверки на HQ-CLI нужно указать получение адреса по DHCP

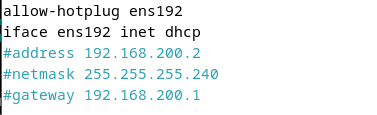
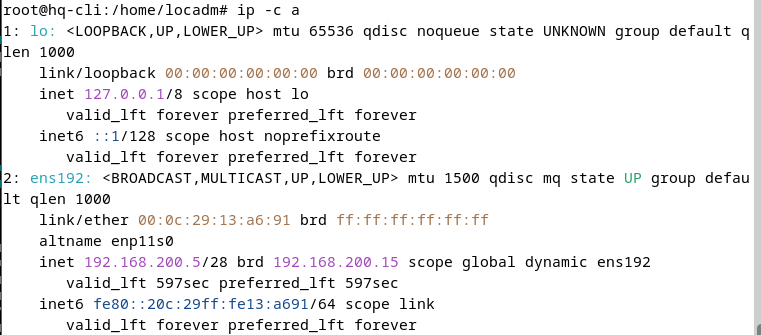


Рисунок 24 — Настройка интерфейса

Прописываем systemctl restart networking для применения и проверяем выданный ip-адрес командой ip -c a

Рисунок 25 — Проверка выдачи ip-адреса

**10. Настройте DNS-сервер на сервере HQ-SRV:**

Вся настройка будет происходить на сервере HQ-SRV

Первым делом необходимо установить пакеты для dns командой

**apt install bind9 dnsutils**

**где:**

**bind9** — пакеты для создания dns сервера

**dnsutils** — дополнительные пакеты, которые помогут проверить работоспособность (команда host)

Следующим шагом необходимо создать зоны для прямого и обратного просмотра dns

Для этого переходим по пути **nano /etc/bind/named.conf.default-zones** и создаём зоны как показано на скриншотах ниже

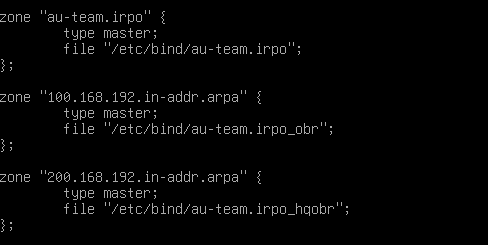


Рисунок 26 — зоны для hq.work(На скриншоте указаны 2 обратные зоны, т. к. у HQ-CLI и HQ-SRV IP-адреса заканчиваются на одинаковые октеты и из-за этого DNS может не работать)

**где:**

**zone —** создаваемая зона

**type —** выбор между первичным и вторичным dns. (Master и Slave)

**file —** расположение конфигурационного файла зоны

**allow-update —** разрешение динамических обновлений

**где zone:**

**hq.work —** зона прямого просмотра

**in-addr.arpa —** зона обратного просмотра ipv4

Следующим шагом необходимо создать конфигурационные вайлы для наших зон. Это можно сделать, скопировав стандартные шаблоны командой **cp**

Пример:

**cp /etc/bind/db.local /etc/bind/au-team.irpo** — создание файла для прямой зоны

**cp /etc/bind/db.127 /etc/bind/ au-team.irpo\_obr** — создание обратной зоны ipv4

Первым шагом сконфигурируем зону прямого просмотра, переходим по пути

**nano /etc/bind/au-team.irpo** и конфигурируем файл как показано на скриншоте ниже

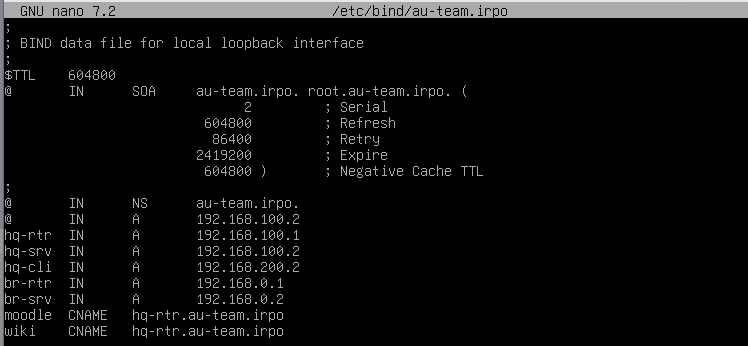


Рисунок 27 — зона прямого просмотра

**Где:**

**NS запись** — обозначение сервера отвественного за разрешение запросов к dns

**A запись** — основная запись для зоны прямого просмотра по протоколу ipv4

**CNAME** — необязательный параметр, для указания альтернативного имени записи

Вторым шагом настроим зону обратного просмотра как указано на скриншоте ниже

Зона находится по пути

**nano /etc/bind/au-team.irpo\_obr**

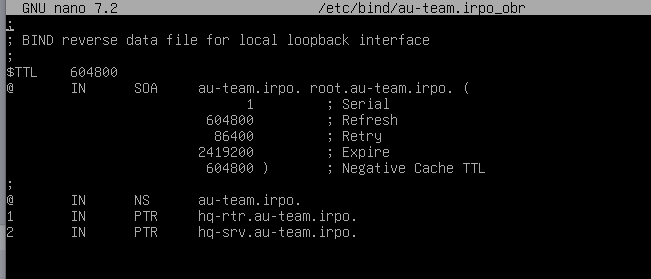
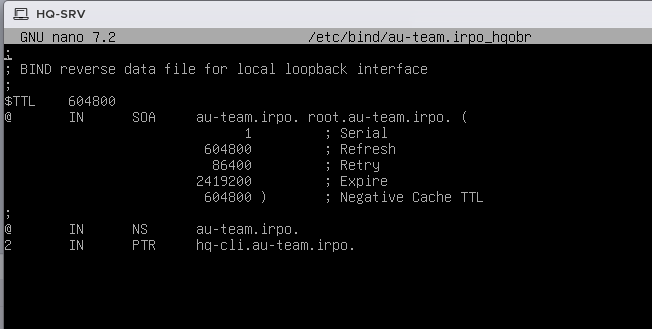


Рисунок 28— настройка зоны обратного просмотра hq.work для ipv4

Рисунок 29— настройка второй зоны обратного просмотра hq.work для ipv4

Где:

**PTR запись** — основная запись для зоны обратного просмотра

**Проверка выполняется посредством команд**

**host IP-адрес**

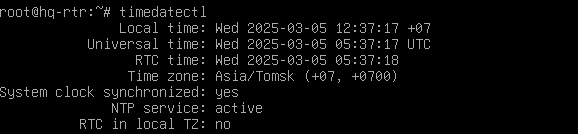
**host имя машины**

**Задание 11**

**Настройка даты и времени согласно месту проведения экзамена**

**timedatectl set-timezone Asia/Tomsk**

**Команда для проверки: timedatectl**

Рисунок 30 — Проверка Даты и времени

**МОДУЛЬ 2**

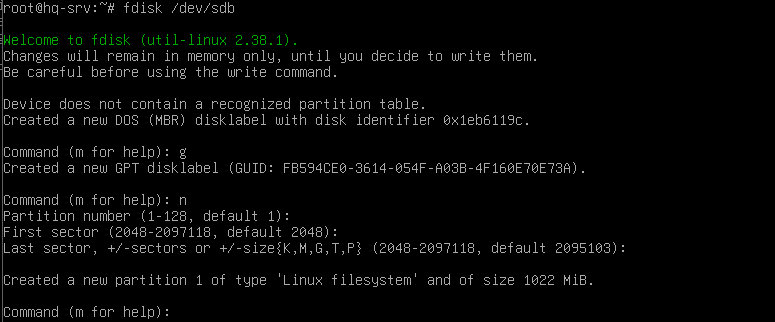
Задание 2

Для выполнения задания будет использоваться утилита MDADM. Её нужно установить: apt install mdadm .

Далее прописываем команду lsblk для отображения дисков(Рисунок 31)

Рисунок 31 — Отображение дисков

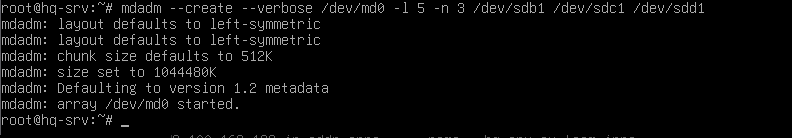
Для создания рейда будут использоваться диски sdb, sdc и sdd. Для начала на них нужно создать разделы командой fdisk /dev/sdb. Сначала вводим g, чтобы создать раздел, затем вводим n и прокликиваем enter. Для выхода и сохранения вводим w. (Рисунок 32)

Рисунок 32 — создание разделов

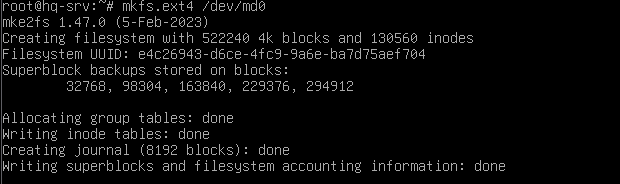
Всё тоже самое проделываем с дисками sdc и sdd.

Теперь можно приступить к созданию рейд-массива(Рисунок 33):

mdadm --create --verbose /dev/md0 -l 5 -n 3 /dev/sdb1 /dev/sdc/1 /dev/sdd1

Рисунок 33 — создание массива

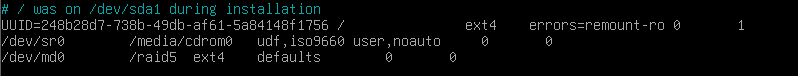
Теперь можно приступить к созданию файловой системы. Для начала отформатируем разделы в ext4: mkfs.ext4 /dev/md0 (Рисунок 34)

Рисунок 34 — форматирование

Следующим шагом нужно создать директорию /raid5 в корне системы:

mkdir /raid5 и примонтировать её к рейду: mount /dev/md0 /raid5.

Для автоматического монтажа необходимо зайти в /etc/fstab и привести его к виду, показанному на рисунке 35:

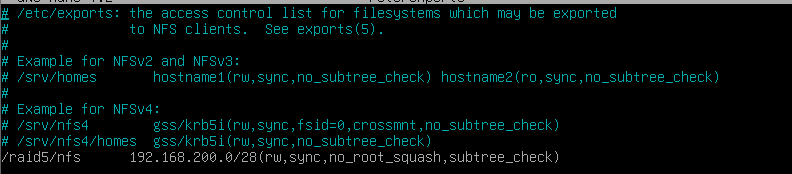
Рисунок 35 — настройка автомонтирования

Теперь устанавливаем серверную часть nfs: apt install nfs-kernel-server.

После установки нужно создть общую папку: mkdir /raid/nfs и задать права:

chmod -R 777 /raid/nfs.

Переходим в файл /etc/exports и добавляем строчку, как показано на рисунке 36.

Рисунок 36 — создание папки, доступной для сети

Выполняем экспорт данных: exportfs -a

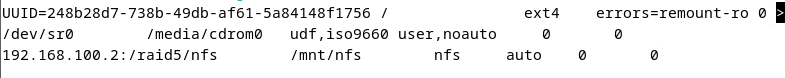
Теперь устанавливаем клиентскую часть nfs на HQ-CLI:

apt install nfs-common.

Создаём директорию: mkdir /mnt/nfs и монтируем её:

mount -t nfs 192.168.100.2:/raid5/nfs /mnt/nfs

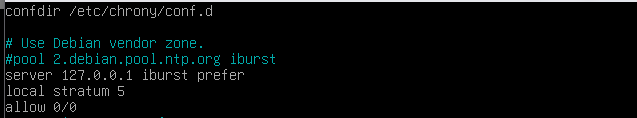
Для автоматического монтирования заходим в /etc/fstab и приводим его к виду, показанному на рисунке 37

Рисунок 37 - автомонтирование

**Задание 3 — NTP**

**Для начала на hq-rtr нужно установить chrony: apt install chrony**

**Заходим в файл /etc/chrony/chrony.conf и приводим его к виду рисунка 38.**

**Рисунок 38 — Конфигурация серверами**

**Перезапускаем chrony: systemcl restart chronyd**

**Теперь на каждую машину, кроме ISP устанавливаем chrony: apt install chrony и в файле конфигурации указать сервер hq-rtr(рисунок 39)**

****

**Рисунок 39 — указание сервера**

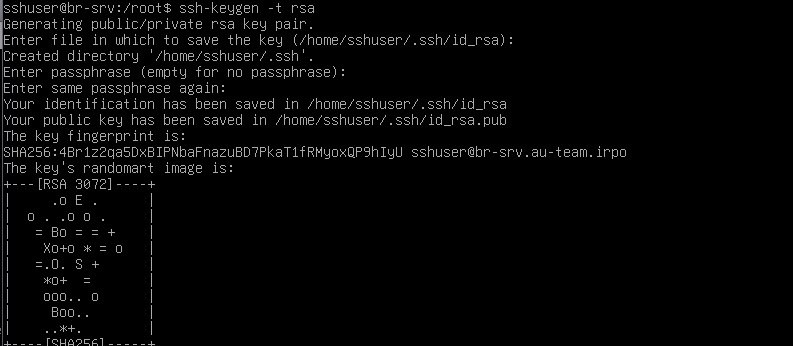
**перезапускаем chrony: systemctl restart chrony**

**Проверяем работу командой сhronyc sources**

Задание 4 — файл инвентаря

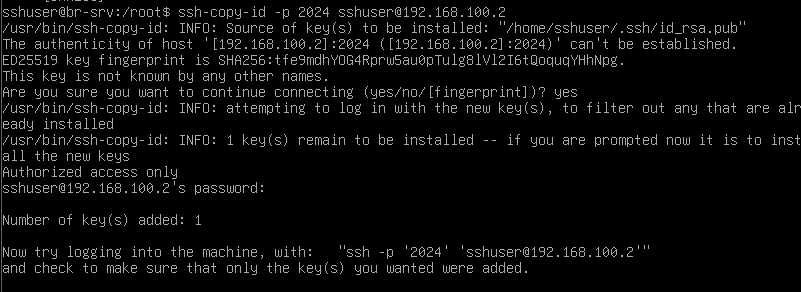
Для начала нужно установить ansible: apt install ansible

Теперь нужно создать ключи rsa(Рисунок 38)

Рисунок 38 — Генерация ключа

Теперь это ключ нужно переместить на остальные машины командой:

ssh-copy-id -p 2024 sshuser@192.168.100.2

Рисунок 39 — передача ключа на HQ-SRV

Тоже самое нужно сделать для остальных машин

Теперь нужно залогиниться обратно под root и создать директорию /etc/ansible

и зайти в файл /etc/ansible/hosts для конфигурации файла инвентаря(Рисунок 40)

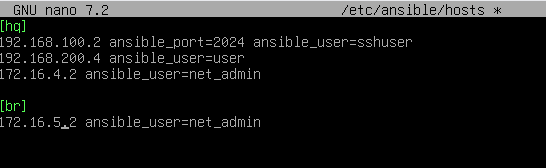
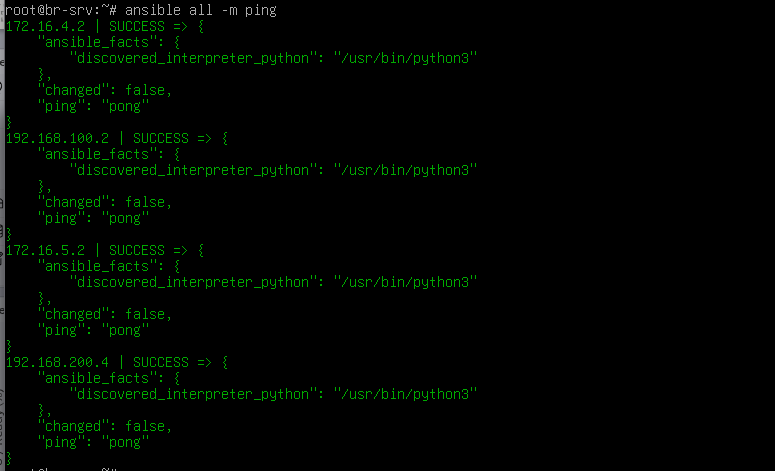


Рисунок 40 — файл инвентаря

Для проверки файла инвентаря используется команда ansible all -m ping

Рисунок 41 - проверка

**Задание 5 — mediawiki**

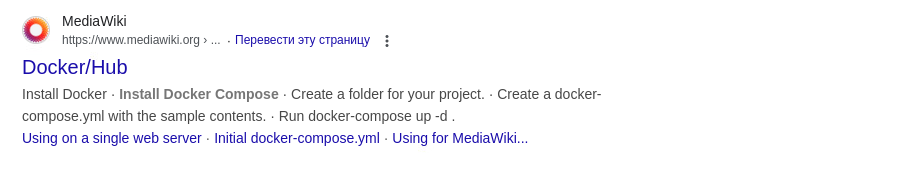
**Для установки DOCKER нужно запустить скрипт**

**wget -qO- https://get.docker.com | bash**

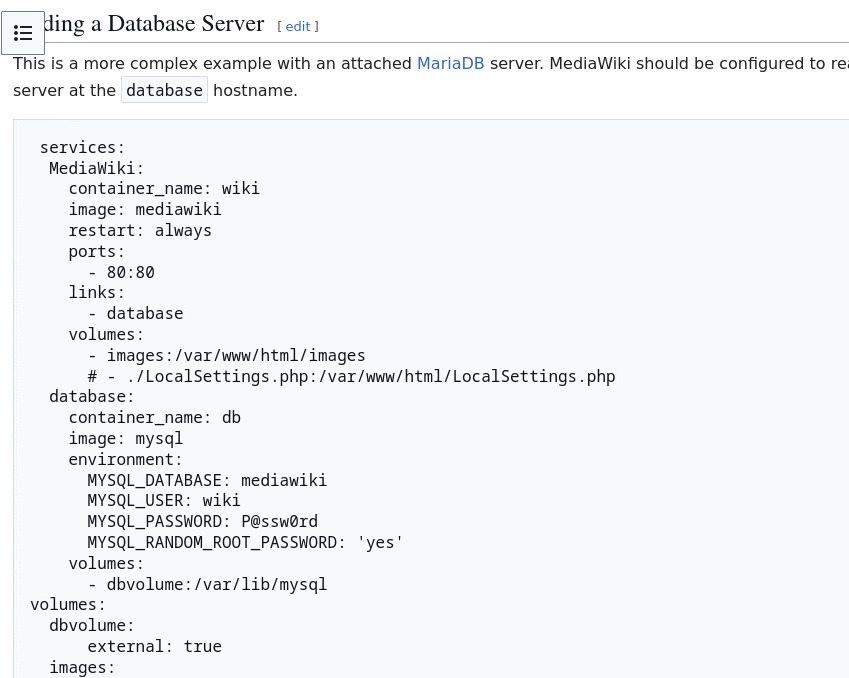
**и установить docker-compos: apt install docker-compose**

**Для упрощённого создания файла wiki.yml нужно с HQ-CLI по ssh подключится к BR-SRV: ssh -p 2024 sshuser@192.168.0.2**

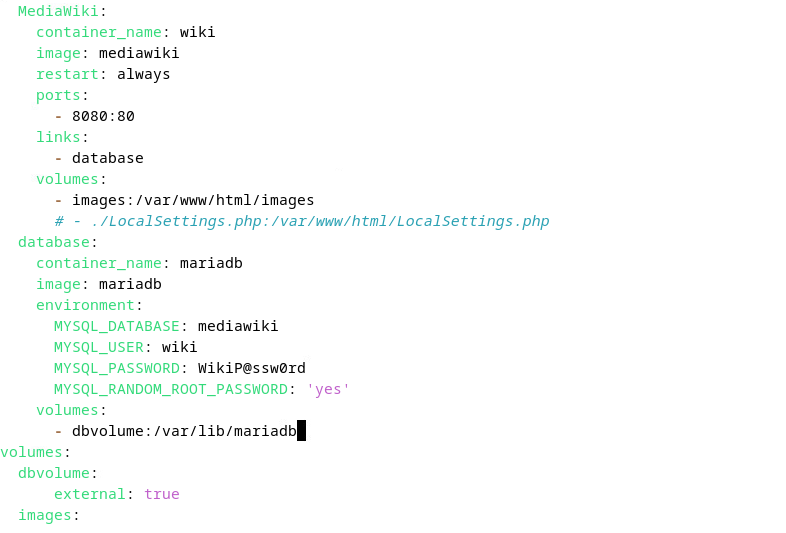
**После подключения по ssh на hq-cli открываем браузер и ищем mediawiki docker-compose. Нужно перейти по ссылке показанной на рисунке 42.**

**Рисунок 42 — Нужная ссылка**

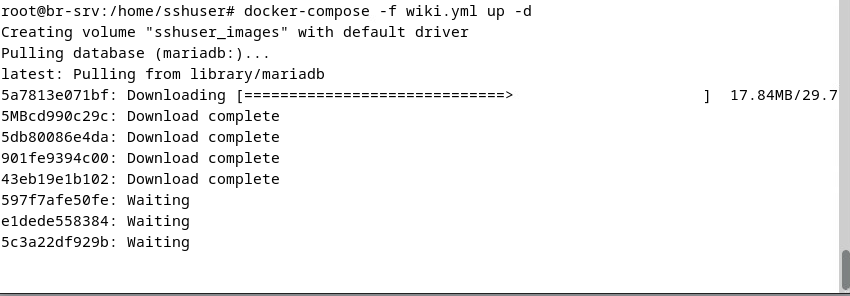
**Ищем пункт «Adding a database server» и копируем весь конфиг(рисунок 43)**

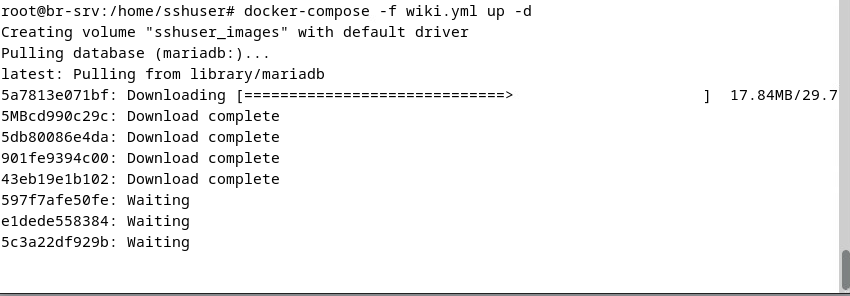
**Рисунок 43 — конфиг mediawiki**

**теперь переходим в директорию /home/sshuser и создаём в ней файл wiki.yml. Заходим в этой файл. ВСЕ СТРОКИ, ОТМЕЧЕННЫЕ СТРЕЛКАМИ НЕОБХОДИМО ЗАПОЛНИТЬ КАК ПОКАЗАНО НА РИСУНКЕ 44!!!!!!!!!!!!!!!**

**Рисунок 44 — изменённый конфиг**

**Теперь создаём volume для докера: docker volume create dbvolume**

**После этого выполняем команду docker-compose -f wiki.yml up -d и запускаем стек контейнеров(Рисунок 45)**

**Рисунок 45 — Запуск стека**

**Ждём пока запуститься стек. После запуска открываем браузер и переходи по ip: 192.168.0.2:8080(Адрес br-srv с указанием порта для mediawiki)**

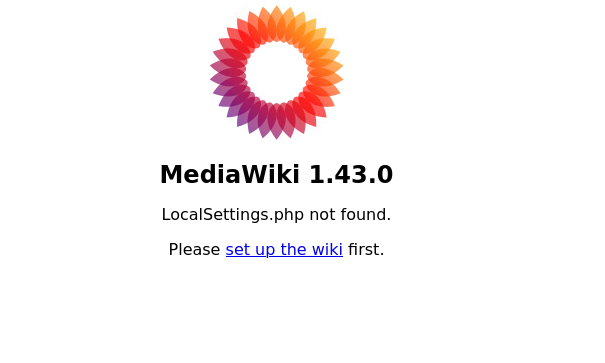
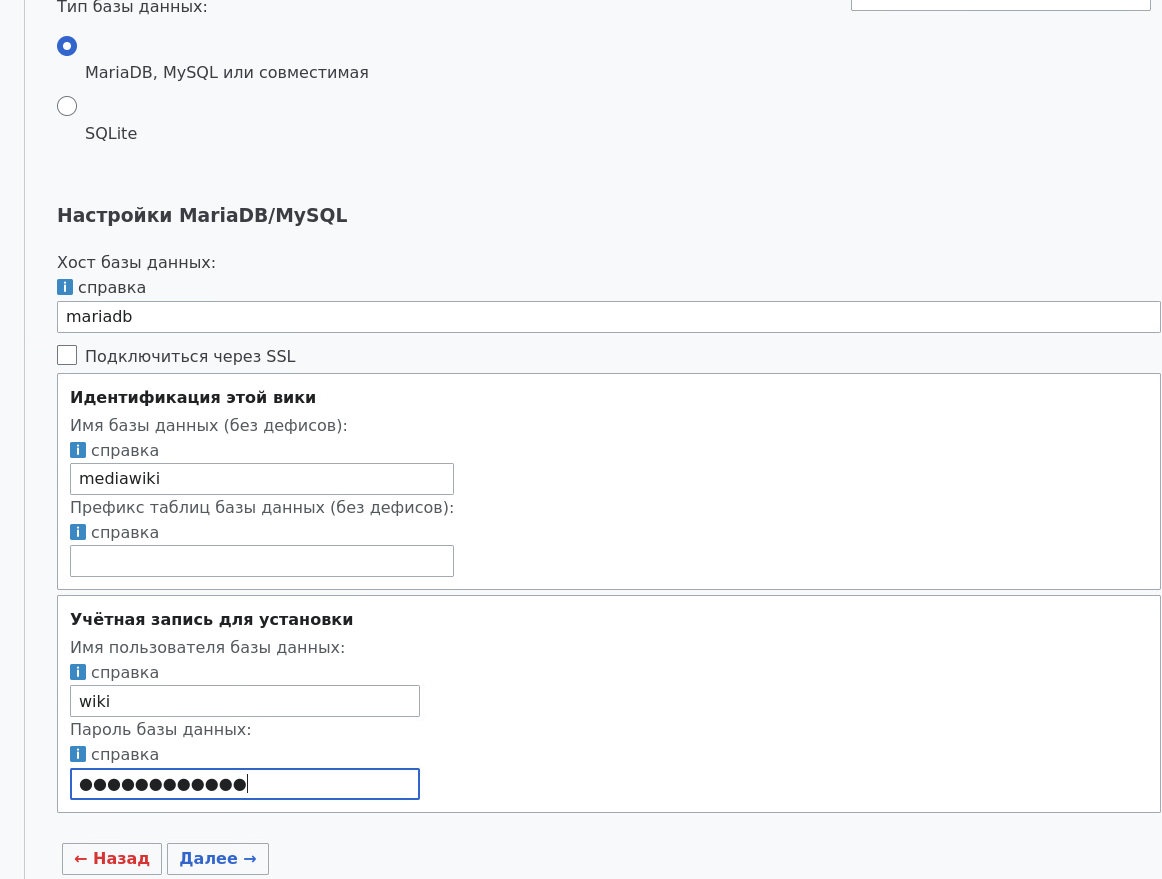
****

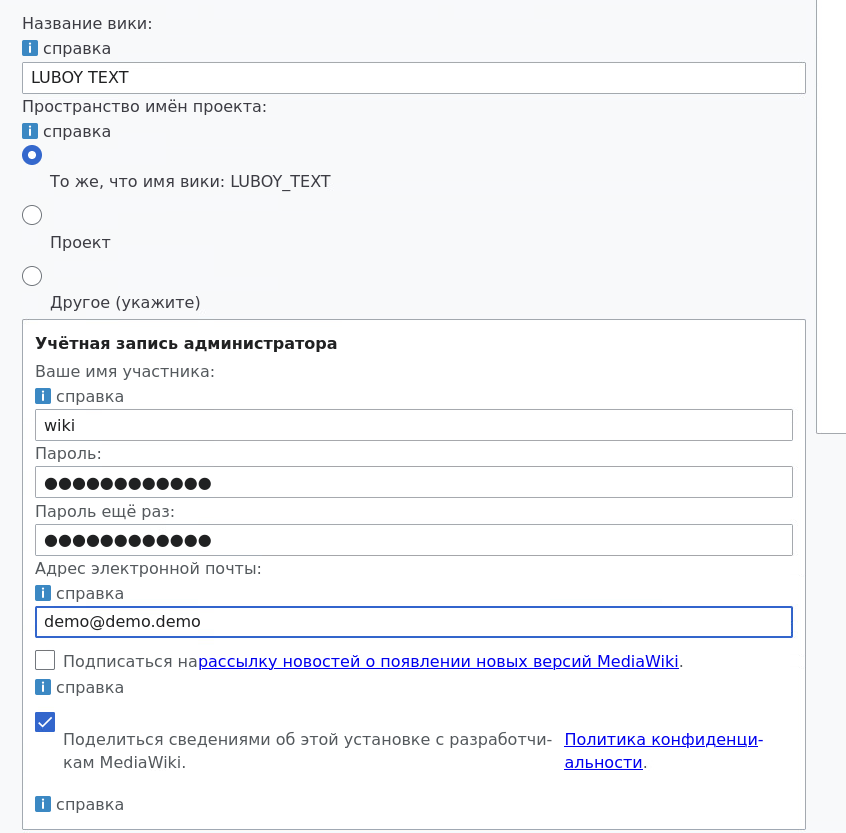
Рисунок 46 — приветственное окно

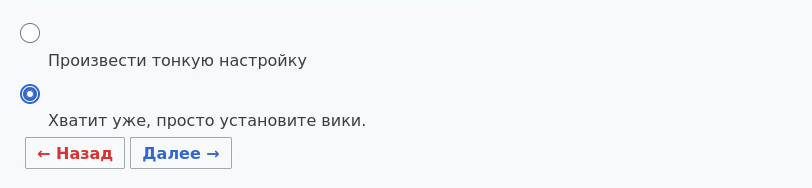
Нажимаем СИНЮЮ ССЫЛКУ и выбираем язык. Соглашаемся с Авторскими правами и условиями.

На рисунке 47 выбираем базу данных. ТАКЖЕ СЛЕДУЕМ СТРЕЛОЧКАМ. ПАРОЛЬ: WikiP@ssw0rd

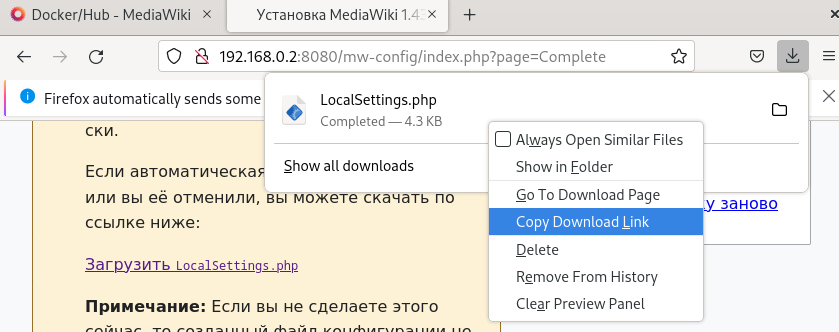
Рисунок 47 — Выбор базы данных

На рисунке 48 идёт задача названия страницы, создание пользователя для авторизации. ТАКЖЕ СЛЕДУЕМ СТРЕЛОЧКАМ. НА РИСУНКЕ 49 ИДЁТ ПРОДОЛЖЕНИЕ РИСУНКА 48. Там нужно просто поставить галочку.

Рисунок 48 — создание базовой страницы и пользователям

Рисунок 49 — ТА САМАЯ ГАЛОЧКА

На рисунке 50 показан файл.

Рисунок 50 — Файл для установки

**Перекидываем файл на br-srv:**

**scp -P 2024 /home/locadm/Downoloads/LocalSettings.php sshuser@192.168.0.2:/home/sshuser**

Переходим в файл wiki.yml и раскмоментируем единственную закоментированную строчку(рисунок 51). УБЕРИТЕ ЛИШНИЙ ПРОБЕЛ: СТРОКИ images и раскоменченная строка должны быть на одно уровне

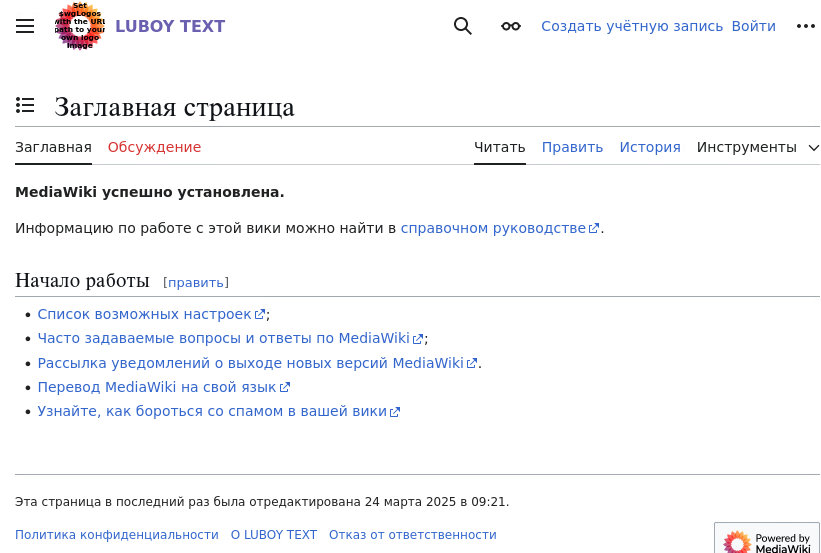
Рисунок 51 — Строка которую нужно раскоментировать

**перезапускаем сервисы:**

**docker-compose -f wiki.yml stop**

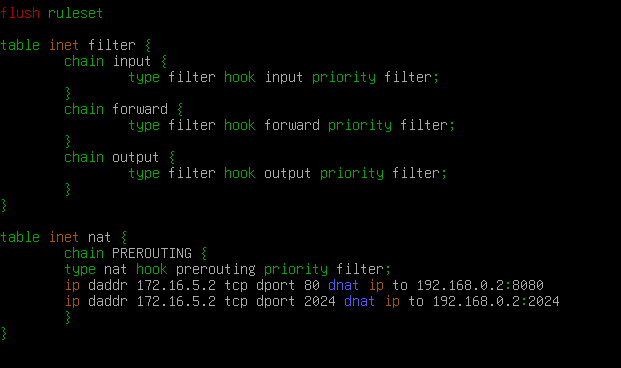
**docker-compose -f wiki.yml up -d**

**Заходим в браузер на HQ-CLI и вводим 192.168.0.2:8080. Вы должны увидеть лицевую страницу mediawiki:**

Рисунок 52 — Готовый mediawiki

**Задание 6 — Проброс портов**

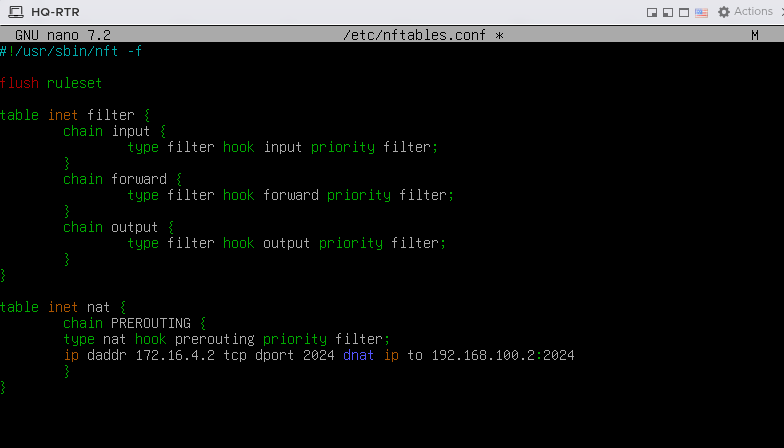
**На br-rtr заходи в файл /etc/nftables.conf и приводим его к виду, показанному на рисунке 53.**

Рисунок 53 — проброс порта для mediawiki и ssh на роутере br-rtr

Перезапускаем службу nftables

**Пробуем зайти на mediawiki по адресу 172.16.5.2**

**Также пытаемся подключится по ssh: ssh -p 2024 sshuser@172.16.5.2**

Рисунок 54 — Проброс порта для ssh на hq-rtr

Задание 7 — moodle

Для удобства также подключаемся с hq-cli к hq-srv по ssh.

Ssh -p 2024 sshuser@192.168.100.2

Теперь устанавливаем apache2: apt install apache2

Также устанавливаем php и доп. расширения

apt install php php-mysqlnd php-pdo php-gd php-mbstring php-zip php-intl php-soap php-curl

Далее заходи в файл /etc/php/8.2/apache2/php.ini и добавляем там строку max\_input\_vars=6000

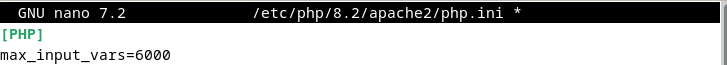


Рисунок 55 — php.ini

перезапускаем apache2: systemctl restart apache2

Устанавливаем mariadb:apt install mariadb-server

Настраиваем mariadb: mysql\_secure\_installation, прокликиваем enter до момента ввода пароля, вводим пароль [P@ssw0rd](mailto:P@ssw0rd) и прокликиваем enter до конца.

Заходим в базу данных: mysql -u root -p и вводим пароль P@ssw0rd

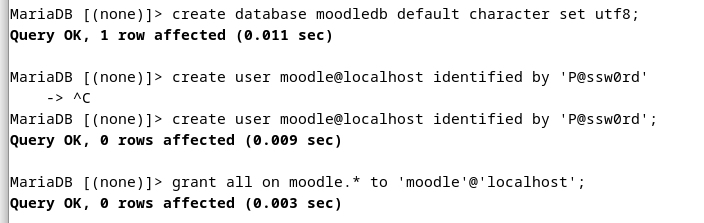
Создадим базу данных и пользователя, а также выдадим ему права для этой базы данных(Рисунок 56)

CREATE DATABASE moodledb DEFAULT CHARACTER SET utf8;

CREATE USER moodle@localhost IDENTIFIED BY 'P@ssw0rd';

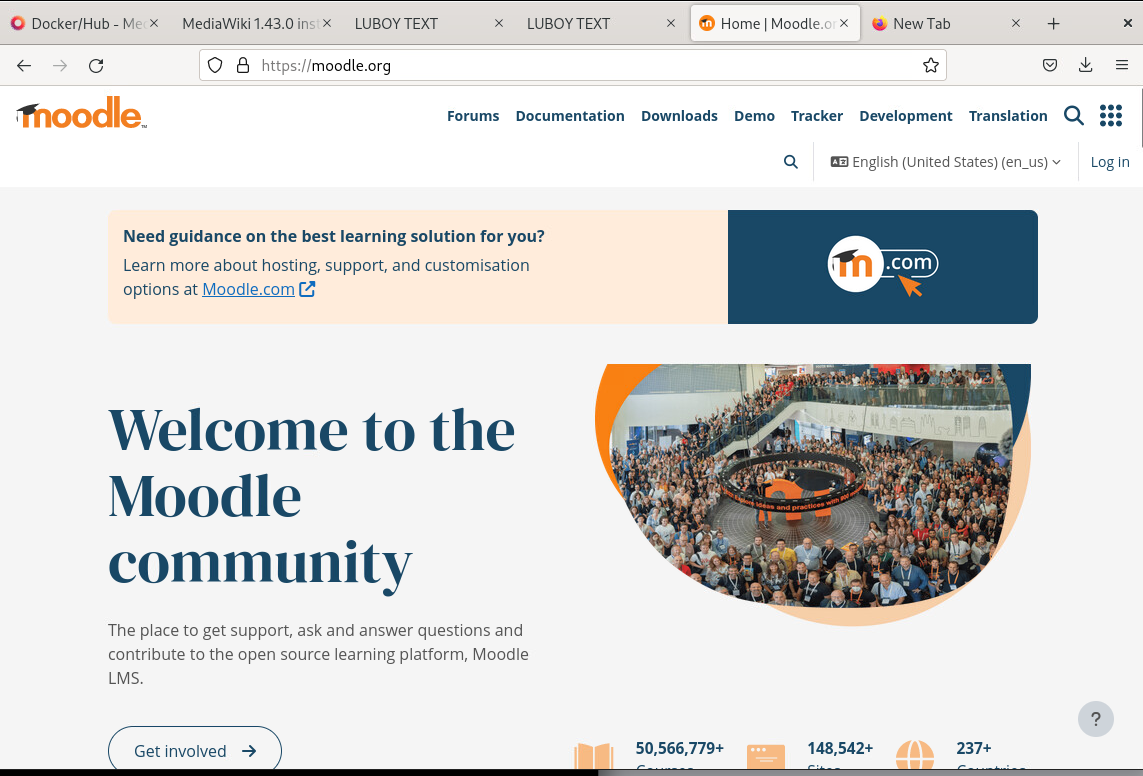
GRANT ALL ON moodledb.\* TO 'moodle'@'localhost';

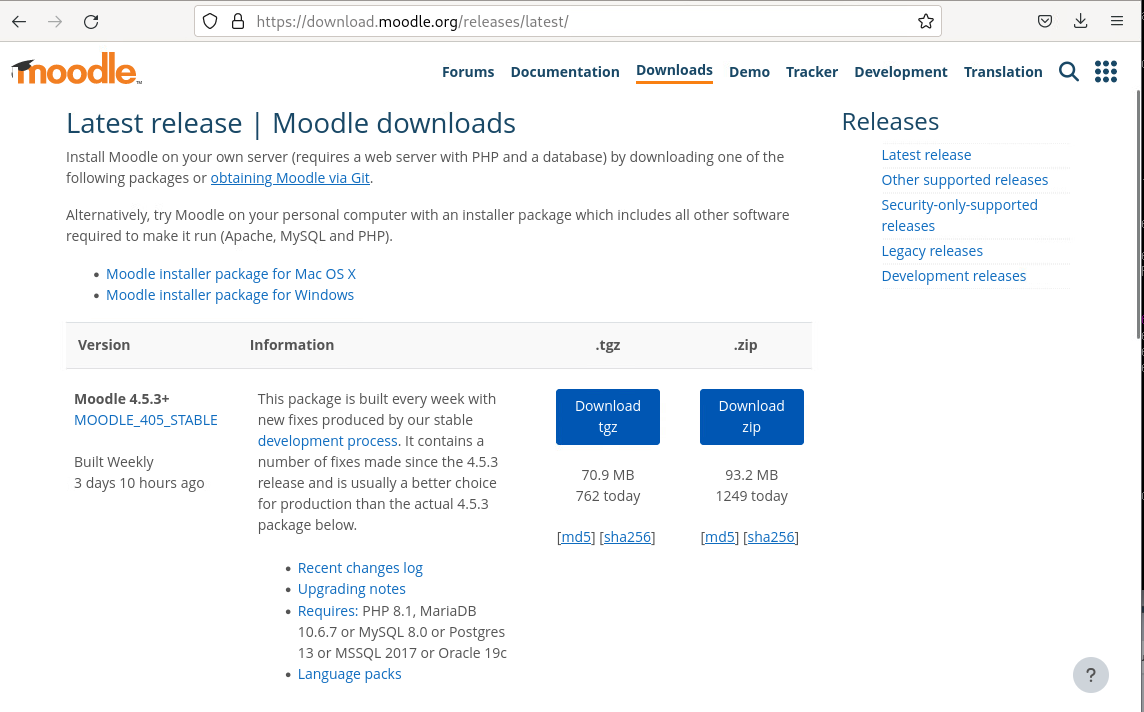
flush privileges;

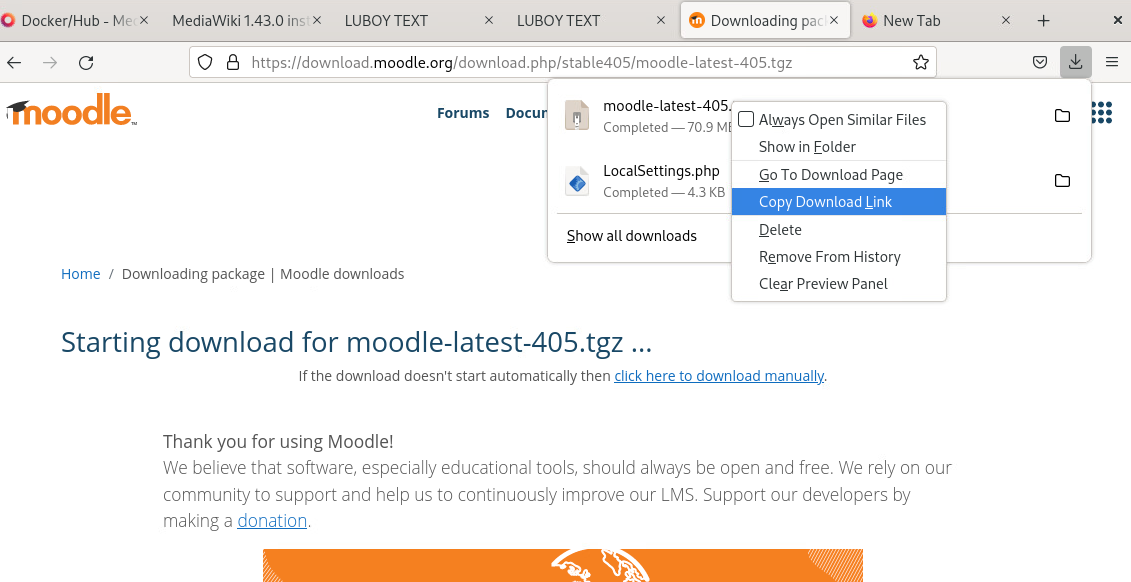
Рисунок 56 — создание базы данных и пользователя

Перезапускаем mariadb: systemctl restart mariadb

Теперь необходимо перейти на официальный сайт moodle.org и перейти во вкладку downoloads(Рисунок 57)

Рисунок 57 — сайт мудл

Рисунок 58 — Ссылка для скачивания

Рисунок 59 — ссылка на файл

wget https://packaging.moodle.org/stable405/moodle-latest-405.tgz -P /tmp

переходим в директорию /tmp: cd /tmp и распаковываем архив

**tar -xzf /tmp/moodle-latest-405.tgz**

Переместим всё содержимое в директорию /var/www/html

mv -f /tmp/moodle/{.,}\* /var/www/html/

Установка прав на /var/www/html

chmod -R 0755 /var/www/html/

chown -R www-data:www-data /var/www/html/

Теперь нужно создать каталог /var/moodledata для мудл:

mkdir /var/moodledata

И выдать права

chmod -R 0755 /var/moodledata

chown -R www-data:www-data /var/moodledata

Удаляем файл index.html: rm /var/www/html/index.html

Перезапускаем apache2: systemctl restart apache2

В поисковой строке браузера вбиваем ip-адрес hq-srv(192.168.100.2) и выбираем язык мудл(рисунок 60)

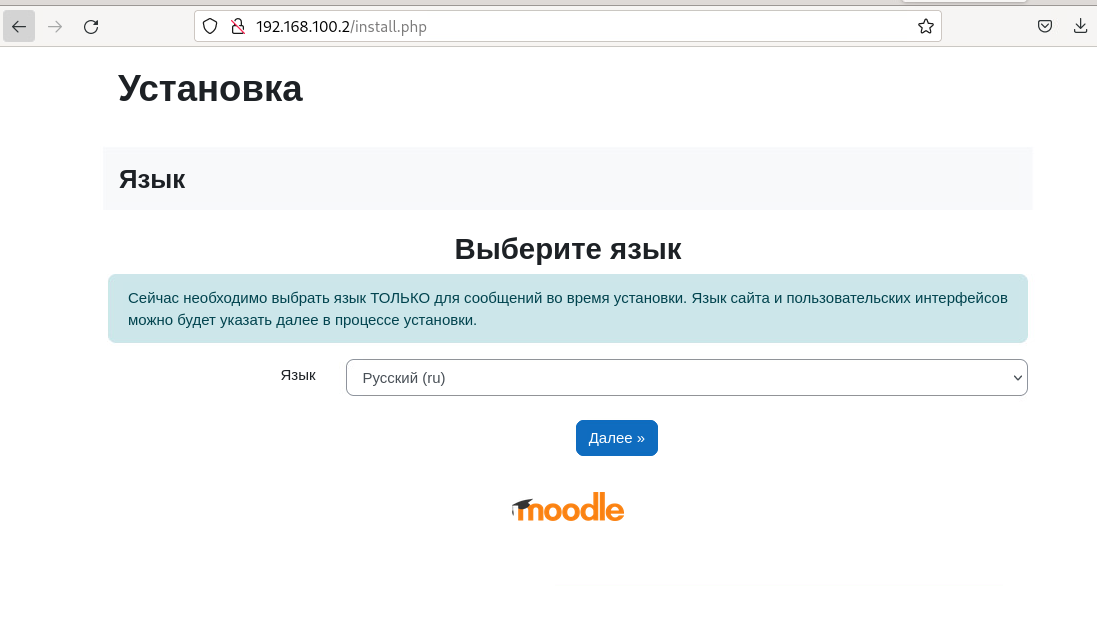


Рисунок 60 — выбор языка

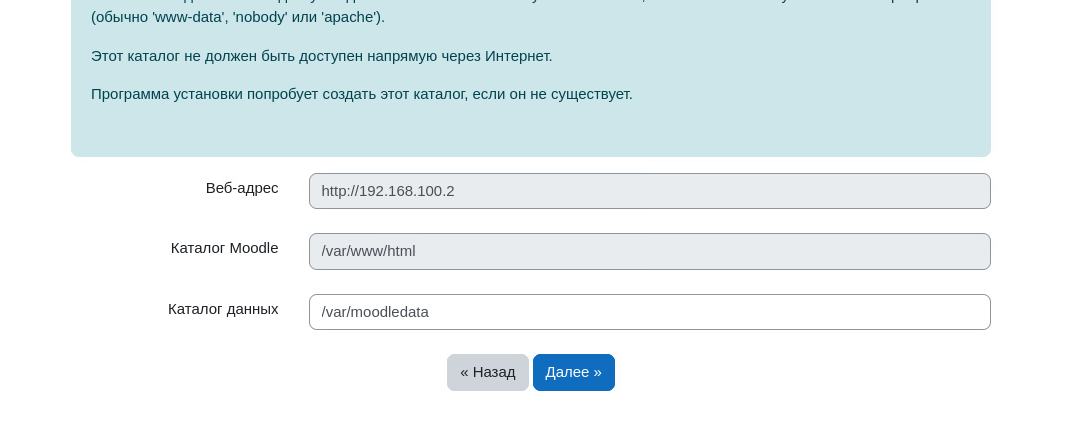


Рисунок 61 — выбор пути

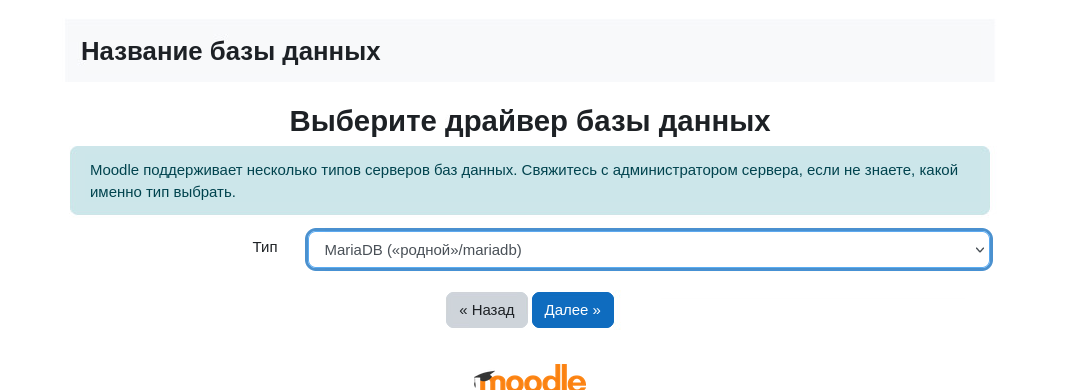


Рисунок 62 — выбор базы данных

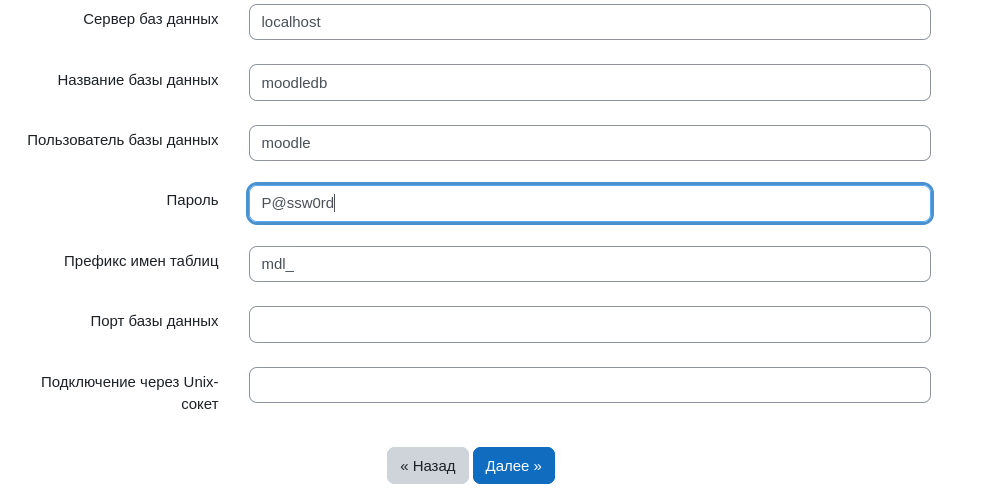
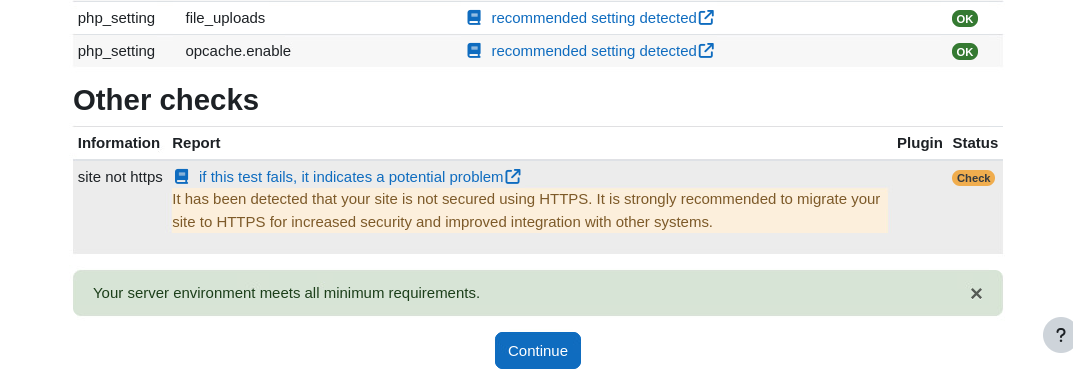


Рисунок 63 — база данных

Возможно возникнет ошибка. Поэтому заходим на сервер и скачиваем php-xml. Apt install php-xml и перезапускаем apache2.

Рисунок 64 — Нажимаем далее

После этого начнётся установка. ПРОСТО ЖДЁМ

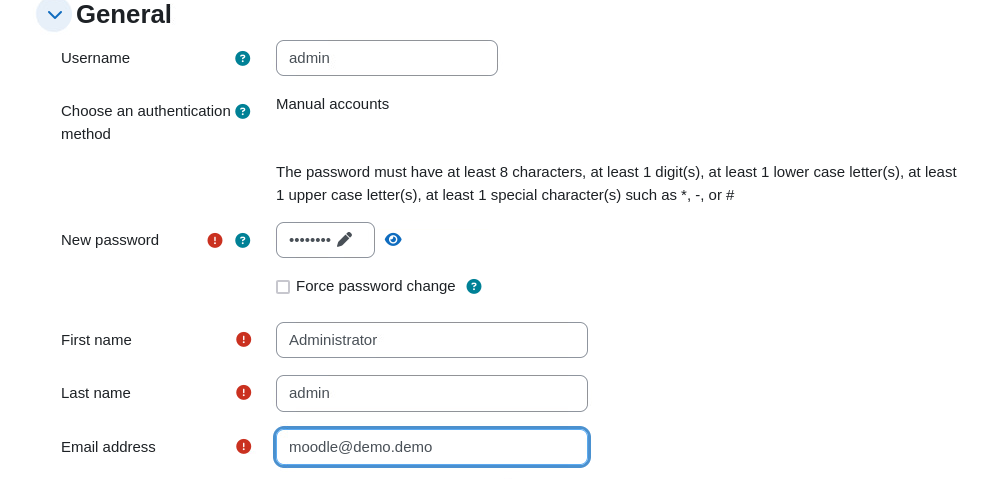


Рисунок 65 — Заполняем базовые данные

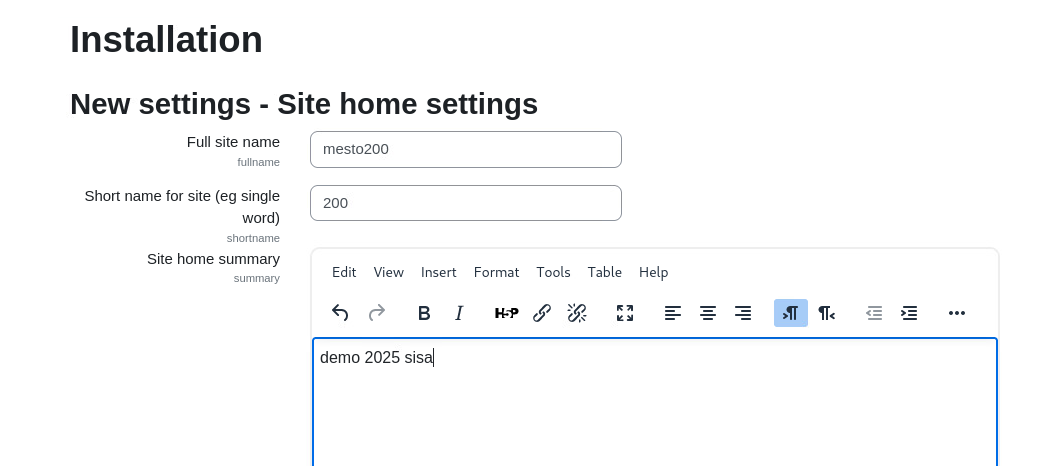
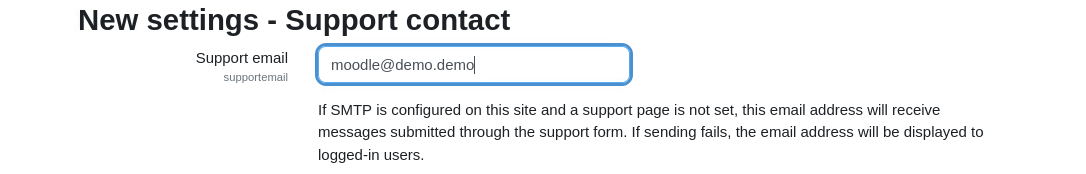


Рисунок 66 — Вместо 200 указываете номер своего рабочего места

Рисунок 67 — делается на той же странице, что и рисунок 66

После этого на главной странице выведется номер вашего места(рисунок 68)

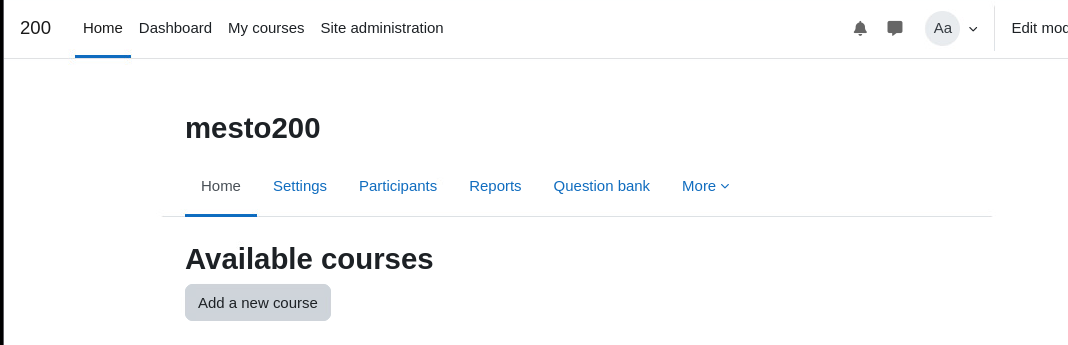
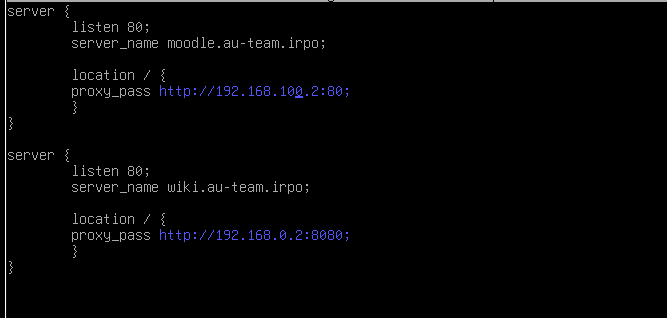


Рисунок 68 — номер места

Задание 8 — nginx

Для начала нужно установить nginx на hq-rtr: apt install nginx

теперь заходи в файл /etc/nginx/sites-enabled/hq-rtr.conf и приводим его к виду рисунка 69.

Рисунок 69 — конфигурация nginx

Теперь нужно проверить конфигурацию на наличие ошибок: nginx -t

Если ошибок не найдено, перезапускаем nginx.

Также заходим в /etc/resolv.conf (Рисунок 70). Так нужно проделать на всех машинах, кроме ISP

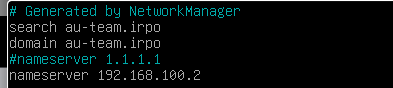
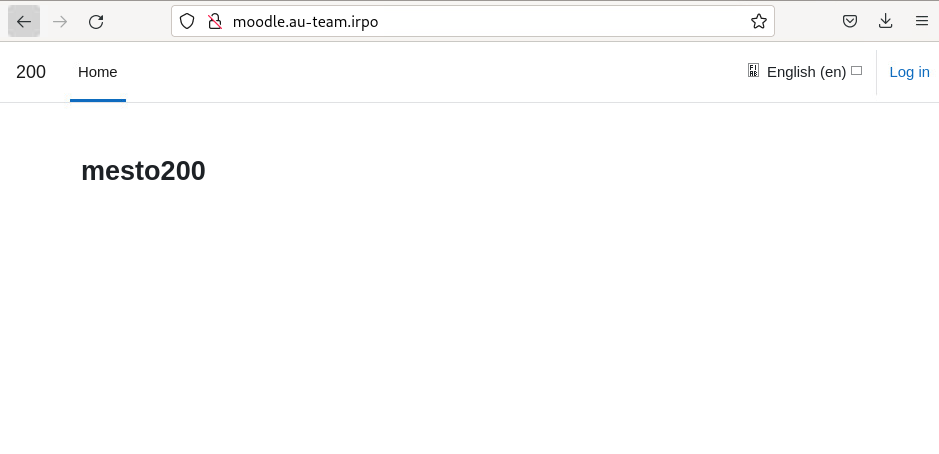
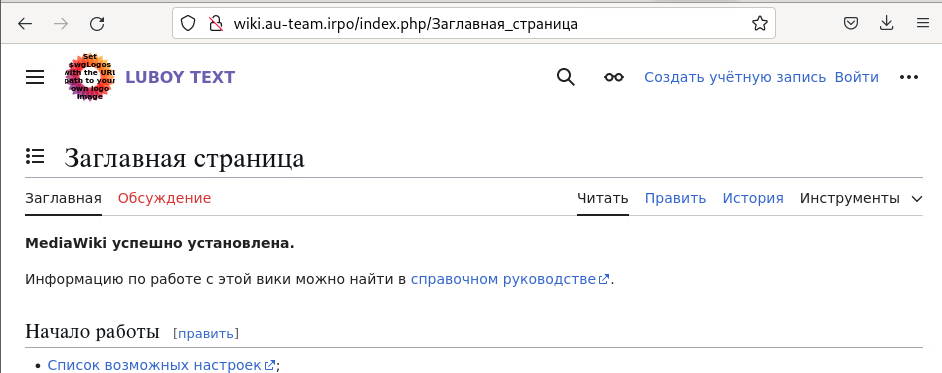


Рисунок 70 — resolv.conf

Теперь в браузере пытаемся подключится к мудл и медиавики по доменному имени (Рисунок 71 и 72)

Рисунок 71 — Доступность мудл

Рисунок 72 — Доступность Медиавики