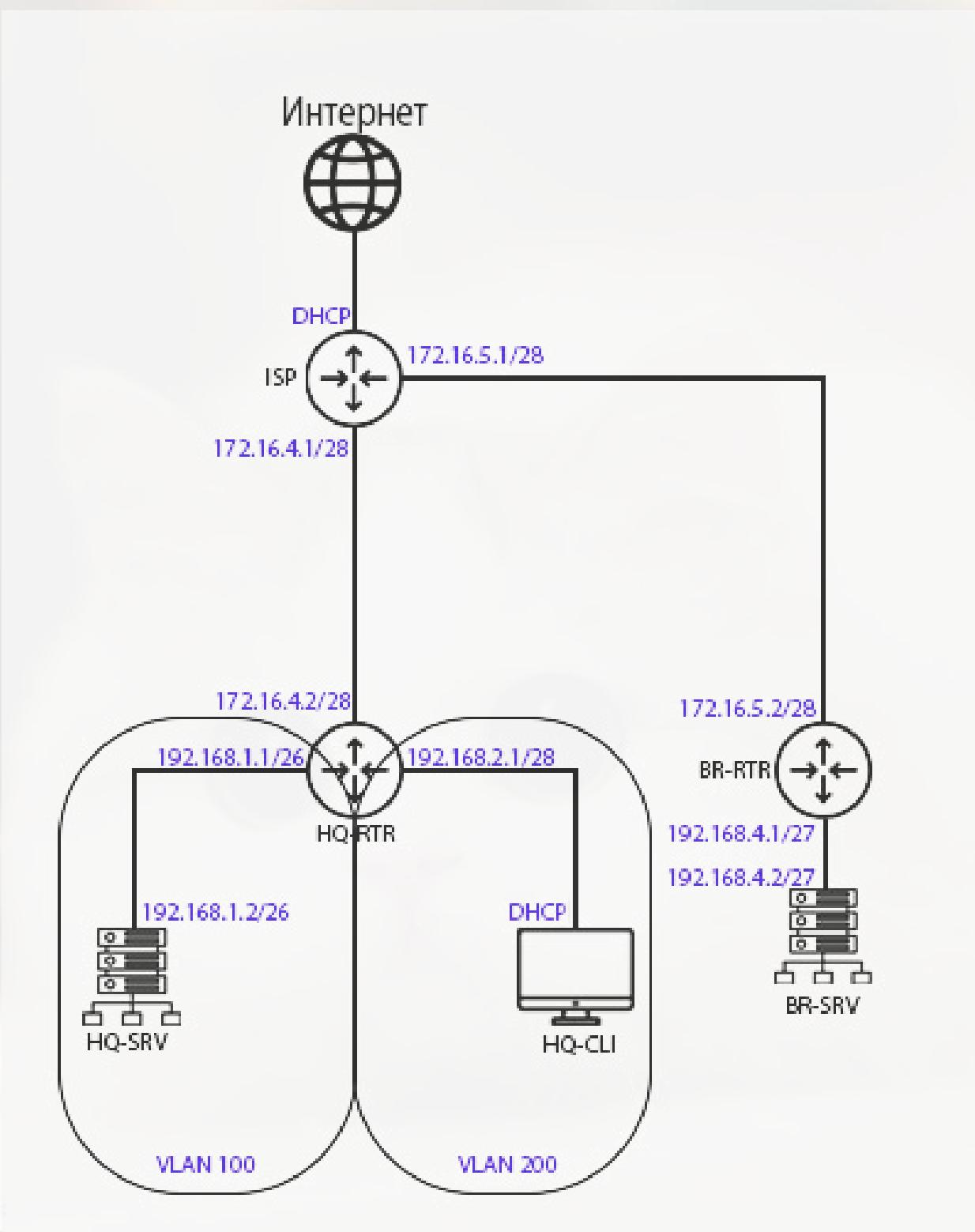


## Топология сети



AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

**Таблица адресации**

Устройство	Интерфейс	IP-адрес	Маска	VLAN	Подсеть	Шлюз
ISP	eth0 (к интернету)	DHCP	DHCP	-	DHCP	DHCP
	eth1 (к HQ-RTR)	172.16.4.1	255.255.255.240	-	172.16.4.0/28	-
	eth2 (к BR-RTR)	172.16.5.1	255.255.255.240	-	172.16.5.0/28	-
HQ-RTR	eth0 (к ISP)	172.16.4.2	255.255.255.240	-	172.16.4.0/28	172.16.4.1
	eth1 (Trunk)	-	-	Trunk	-	-
	eth1.100	192.168.1.1	255.255.255.192	100	192.168.1.0/26	-
	eth1.200	192.168.2.1	255.255.255.240	200	192.168.2.0/28	-
	eth1.999	192.168.3.1	255.255.255.248	999	192.168.3.0/29	-
	gre1 (IP туннель)	10.10.10.1	255.255.255.252	-	10.10.10.0/30	-
HQ-SRV	enp0s3 (Trunk)	-	-	Trunk	-	-
HQ-CLI	enp0s3.100	192.168.1.2	255.255.255.192	100	192.168.1.0/26	192.168.1.1
BR-RTR	enp0s3.200	192.168.2.2	255.255.255.240	200	192.168.2.0/28	192.168.2.1
BR-RTR	eth0 (к ISP)	172.16.5.2	255.255.255.240	-	172.16.5.0/28	172.16.5.1
	eth1 (к BR-SRV)	192.168.4.1	255.255.255.224	-	192.168.4.0/27	-
	gre1 (IP туннель)	10.10.10.2	255.255.255.252	-	10.10.10.0/30	-
BR-SRV	enp0s3 (к BR-RTR)	192.168.4.2	255.255.255.224	-	192.168.4.0/27	192.168.4.1

**Версии дистрибутивов к соответствующим устройствам (ссылки):**

**ISP, HQ-RTR, BR-RTR –**

[https://dl.astralinux.ru/astra/stable/2.12\\_x86-64/iso/alce-2.12.46.6-17.04.2023\\_15.09.iso](https://dl.astralinux.ru/astra/stable/2.12_x86-64/iso/alce-2.12.46.6-17.04.2023_15.09.iso)

**HQ-SRV, BR-SRV –**

[https://download.basealt.ru/pub/distributions/ALTLinux/p10/images/server/x86\\_64/alt-server-10.2-x86\\_64.iso](https://download.basealt.ru/pub/distributions/ALTLinux/p10/images/server/x86_64/alt-server-10.2-x86_64.iso)

**HQ-CLI –**

[https://download.basealt.ru/pub/distributions/ALTLinux/p10/images/workstation/x86\\_64/alt-workstation-10.1-x86\\_64.iso](https://download.basealt.ru/pub/distributions/ALTLinux/p10/images/workstation/x86_64/alt-workstation-10.1-x86_64.iso)

AUTHORS:

NECHAEV  
NAUMOV  
NAGORNOVA

## Таблица масок

Маска подсети	CIDR префикс	Всего IP адресов	Используемых IP адресов
255.255.255.255	/32	1	1
255.255.255.254	/31	2	0
255.255.255.252	/30	4	2
255.255.255.248	/29	8	6
255.255.255.240	/28	16	14
255.255.255.224	/27	32	30
255.255.255.192	/26	64	62
255.255.255.128	/25	128	126
255.255.255.0	/24	256	254
255.255.254.0	/23	512	510
255.255.252.0	/22	1024	1022
255.255.248.0	/21	2048	2046
255.255.240.0	/20	4096	4094
255.255.224.0	/19	8192	8190
255.255.192.0	/18	16384	16382
255.255.128.0	/17	32768	32766
255.255.0.0	/16	65536	65534
255.254.0.0	/15	131072	131070
255.252.0.0	/14	262144	262142
255.248.0.0	/13	524288	524286
255.240.0.0	/12	1048576	1048574
255.224.0.0	/11	2097152	2097150
255.192.0.0	/10	4194304	4194302
255.128.0.0	/9	8388608	8388606
255.0.0.0	/8	16777216	16777214
254.0.0.0	/7	33554432	33554430
252.0.0.0	/6	67108864	67108862
248.0.0.0	/5	134217728	134217726
240.0.0.0	/4	268435456	268435454
224.0.0.0	/3	536870912	536870910
192.0.0.0	/2	1073741824	1073741822
128.0.0.0	/1	2147483648	2147483646
0.0.0.0	/0	4294967296	4294967294

AUTHORS:  
 NECHAEV  
 NAUMOV  
 NAGORNOVA

# МОДУЛЬ №1

## 1. Произведите базовую настройку устройств

**ВСЕ СЛЕДУЮЩИЕ НАСТРОЙКИ ПРОИЗВОДЯТСЯ ОТ root!!!**

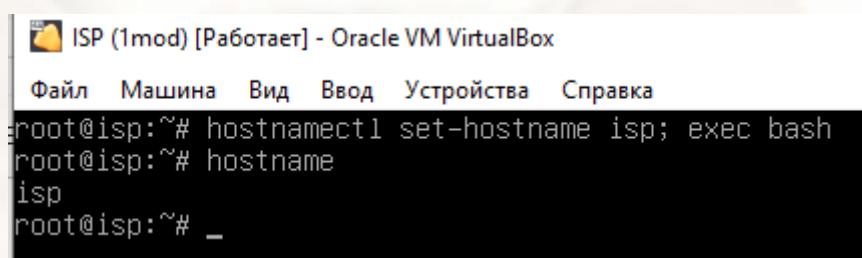
**Команда для перехода в режим суперпользователя:**

**su - (ALT Linux)**

**sudo -i (ASTRA Linux)**

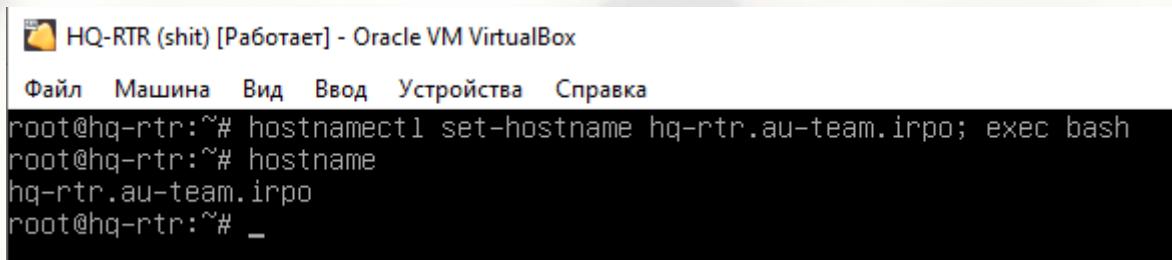
**a) Настройте имена устройств согласно топологии. Используйте полное доменное имя.**

Настроим имя на ISP:



```
ISP (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@isp:~# hostnamectl set-hostname isp; exec bash
root@isp:~# hostname
isp
root@isp:~# _
```

Настроим им на HQ-RTR:



```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@hq-rtr:~# hostnamectl set-hostname hq-rtr.au-team.irpo; exec bash
root@hq-rtr:~# hostname
hq-rtr.au-team.irpo
root@hq-rtr:~# _
```

**АНАЛОГИЧНО НА ДРУГИХ УСТРОЙСТВАХ!**

**b) На всех устройствах необходимо сконфигурировать IPv4**

**Адресация на ISP:**

Настраивать будем через следующую команду:

**mcedit /etc/network/interfaces**

**AUTHORS:**

NECHAEV

NAUMOV

NAGORNOVA

```

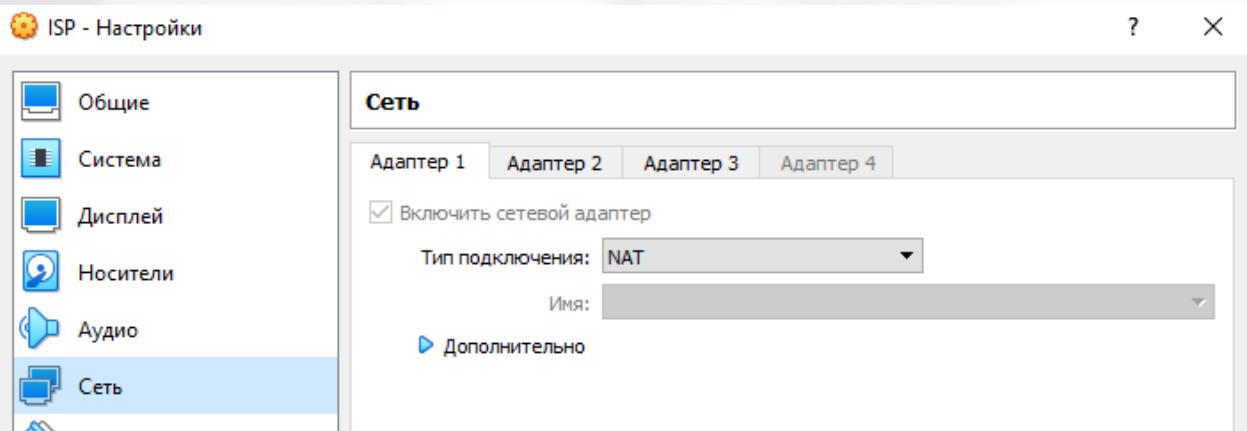
/etc/network/interfaces      [----] 25 L:[ 1+15 16/ 16] *(400 / 400b) <EOF>
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

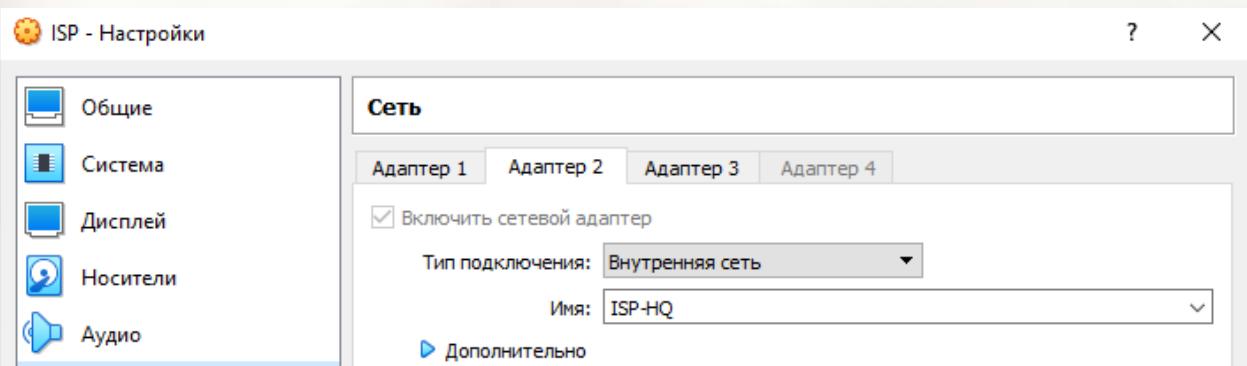
# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
auto eth1
iface eth1 inet static
    address 172.16.4.1/28
auto eth2
iface eth2 inet static
    address 172.16.5.1/28

```

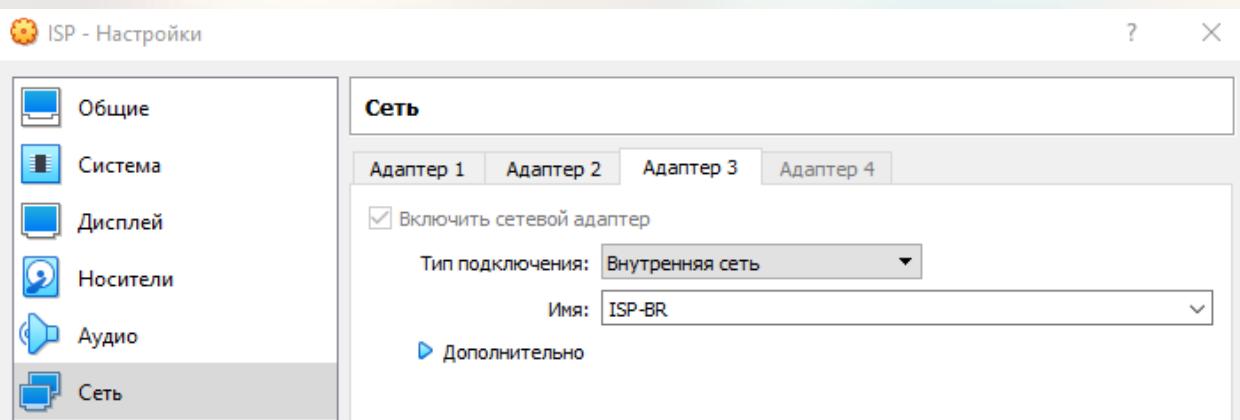
**eth0** – интерфейс, подключенный к провайдеру (Интернет), должен быть по dhcp



**eth1** – интерфейс, подключенный к ISP-HQ, должна быть настроена static (см. [Таблица адресации](#))



**eth2** – интерфейс, подключенный к ISP-BR, должна быть настроена static (см. [Таблица адресации](#)).



Маска 255.255.255.240 (/28) была выбрана с условием, что сеть должна вмещать не более 32 хостов (см. [Таблица масок](#))

Из **mcedit** выходим нажатием **F2** для сохранения изменений и **F10** для выхода из него.

**systemctl restart networking** (перезапуск службы сети для применения изменений на Astra Linux)

**systemctl restart network** (тоже самое, только на Alt Linux)

### Адресация на HQ-RTR:

Настраивать будем через следующую команду:

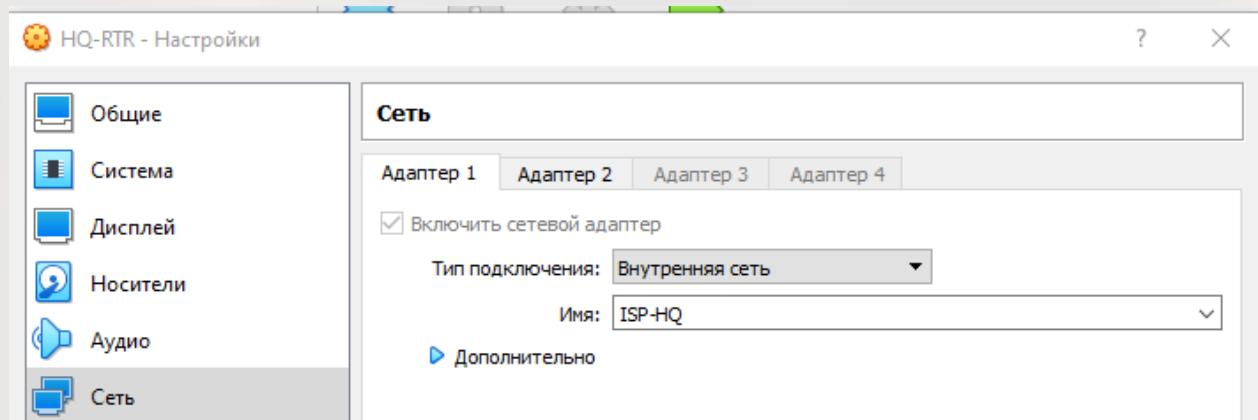
**mcedit /etc/network/interfaces**

```
althome.zapto.org:7015 QEMU (HQ-RTR) - noVNC
/etc/network/interfaces [----] 24 L:[ 1+25 26/ 34] *(657 / 815b) 0010 0x00A
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

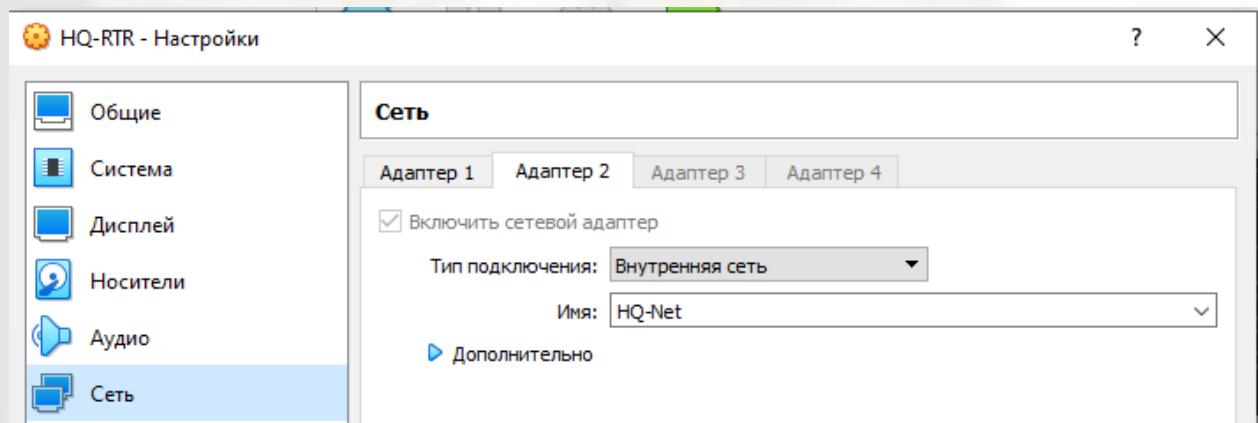
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 172.16.4.2/28
gateway 172.16.4.1
auto eth1
iface eth1 inet manual
auto eth1.100
iface eth1.100 inet static
address 192.168.1.1/26
vlan-raw-device eth1
auto eth1.200
iface eth1.200 inet static
address 192.168.2.1/28
vlan-raw-device eth1
auto eth1.300
iface eth1.300 inet static
address 192.168.3.1/29
vlan-raw-device eth1_
```

**eth0** – интерфейс, подключенный к ISP-HQ, должна быть настроена static (см. [Таблица адресации](#)).



**eth1** – интерфейс, подключенный к HQ-Net, должен быть настроен на manual, так как далее мы на нём будем настраивать VLAN'ы.



**eth1.100** – интерфейс, подключенный к HQ-Net, должен быть настроен на static и настроен на VLAN 100 с маской /26. Локальная сеть в сторону HQ-SRV(VLAN100) должна вмещать не более 64 адресов.

**eth1.200** – интерфейс, подключенный к HQ-Net, должен быть настроен на static и настроен на VLAN 200 с маской /28. Локальная сеть в сторону HQ-CLI(VLAN200) должна вмещать не более 16 адресов.

**eth1.999** – интерфейс, подключенный к HQ-Net, должен быть настроен на static и настроен на VLAN 999 с маской /29. Локальная сеть для управления(VLAN999) должна вмещать не более 8 адресов.

#### AUTHORS:

NECHAEV **systemctl restart networking** (перезапуск службы сети для применения изменений)

#### NAGORNOVA

#### Адресация на BR-RTR:

Настраивать будем через следующую команду:

**mcedit /etc/network/interfaces**

```

/etc/network/interfaces [-M--] 26 L:[ 1+14 15/ 15] *(389 / 389b) <EOF>
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 172.16.5.2/28
    gateway 172.16.5.1
auto eth1
iface eth1 inet static
    address 192.168.4.1/27

```

**eth0** - интерфейс, подключенный к ISP-BR, должна быть настроена static (см. [Таблица адресации](#)).

**eth1** - интерфейс, подключенный к BR-Net, должна быть настроена static (см. [Таблица адресации](#)). Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов.

**systemctl restart networking** (перезапуск службы сети для применения изменений)!

### Адресация на BR-SRV:

Альт отличается настройкой, как минимум тем, что в нём для настройки интерфейса нужно использовать отдельный каталог и внутри ещё каталоги, сейчас всё увидите, перейдём в каталог нужного нам интерфейса, но для начала посмотрим наши интерфейсы через команду:

**ip a**

```

QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge
HTTPS://192.168.4.85:8006/?console=kvm&novnc=1&vmid=104&vmname=BR-SRV&node=serv
[roo...@dc1qhcwqkfop ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a6:7c:1f:76:2c:7f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::a67c:1fff:fe76:2c7f/64 scope link
        valid_lft forever preferred_lft forever
[roo...@dc1qhcwqkfop ~]#

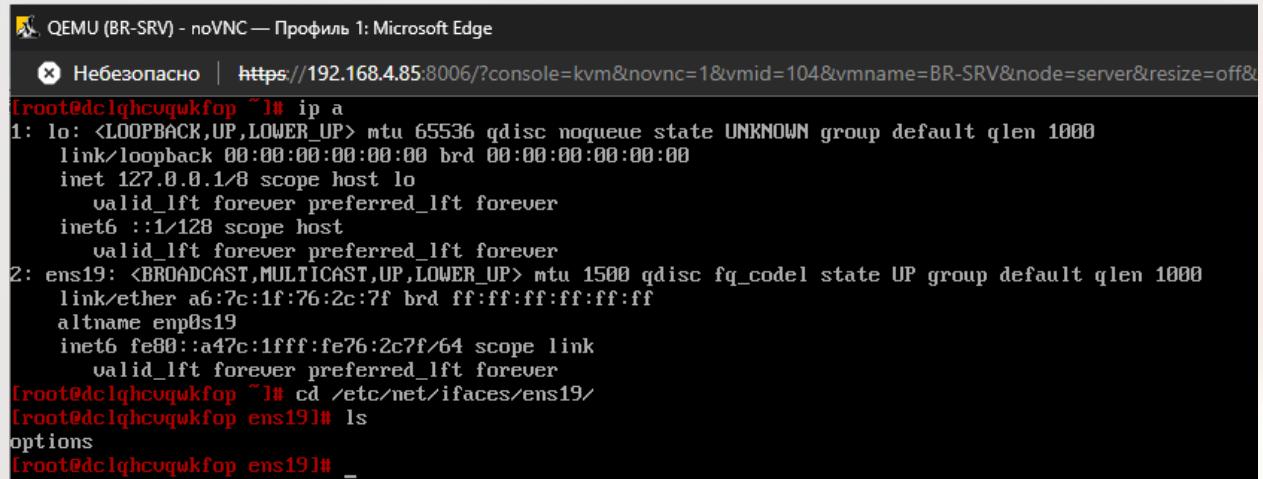
```

Видим, что нужный нам интерфейс имеет название **ens19** (У вас может отличаться, смотрите внимательно)

Переходим в каталог этого интерфейса:

```
cd /etc/net/ifaces/ens19
```

**ls (выводим содержимое этого каталога)**



```
QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge
✗ Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=104&vmname=BR-SRV&node=server&resize=off&
[root@dc1qhcwqwkfop ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a6:7c:1f:76:2c:7f brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::a47c:1fff:fe76:2c7f/64 scope link
        valid_lft forever preferred_lft forever
[root@dc1qhcwqwkfop ~]# cd /etc/net/ifaces/ens19/
[root@dc1qhcwqwkfop ens19]# ls
options
[root@dc1qhcwqwkfop ens19]# _
```

Теперь будем настраивать файл, который здесь лежит, остальные создадим сами, приступаем.

Первым делом настраивать будем options через следующую команду:

```
mcedit /etc/net/ifaces/ens19/options
```

Если вы уже в каталоге, и делали всё по нашим шагам, то просто:

```
mcedit options
```

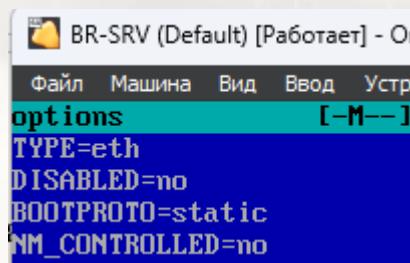
Приведём строки в файле к следующему виду:

**TYPE=eth**

**DISABLED=no**

**BOOTPROTO=static**

**NM\_CONTROLLED=no**



AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

**СОХРАНЯЕМ ИЗМЕНЕНИЯ НАЖАТИЕМ КЛАВИШИ F2 И ЗАКРОЕМ КЛАВИШЕЙ F10, ЗАПОМНИТЕ, РЕБЯТИШКИ!!!**

Далее настроим файл ipv4address (если его нет, то он создаётся):

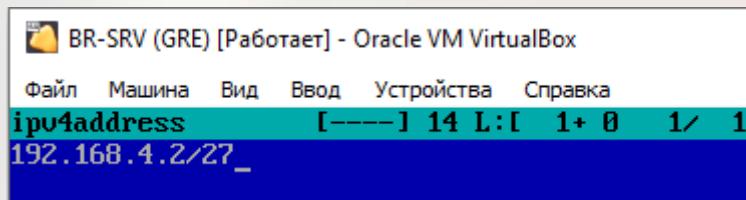
**mcedit /etc/net/ifaces/ens19/ipv4address**

Если вы уже в каталоге, и делали всё по нашим шагам, то просто:

**mcedit ipv4address**

Внесём туда следующую строку:

**192.168.4.2/27** (см. [Таблица адресации](#))



Далее настроим файл ipv4route:

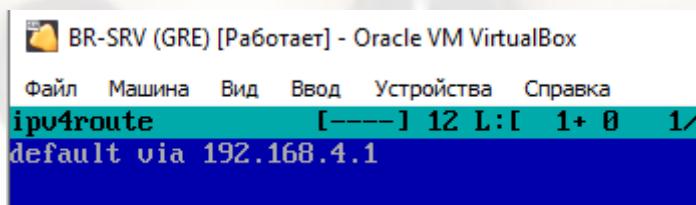
**mcedit /etc/net/ifaces/ens19/ipv4route**

Если вы уже в каталоге, и делали всё по нашим шагам, то просто:

**mcedit ipv4route**

Внесём туда следующую строку:

**default via 192.168.4.1** (см. [Таблица адресации](#))



Настройка адресации на **BR-SRV** завершена!

Перезапускаем службу network командой:

**systemctl restart network**

И смотрим ещё раз данные об интерфейсах командой:

**ip a**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
[root@dc1qhcwqwkfop ens19]# mcedit ipv4address
[root@dc1qhcwqwkfop ens19]# mcedit ipv4route
[root@dc1qhcwqwkfop ens19]# systemctl restart network
[root@dc1qhcwqwkfop ens19]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether a6:7c:1f:76:2c:7f brd ff:ff:ff:ff:ff:ff
    altnet enp0s19
    inet 192.168.4.2/27 brd 192.168.4.31 scope global ens19
        valid_lft forever preferred_lft forever
    inet6 fe80::a47c:1fff:fe76:2c7f/64 scope link tentative
        valid_lft forever preferred_lft forever
[root@dc1qhcwqwkfop ens19]#
```

Всё успешно! Но у алты есть тенденция не назначать адрес на интерфейс после перезагрузки системы, поэтому добавим, пожалуй, запись о перезагрузке службы **network** в **crontab**.

Делаем это следующим образом, пишем команду:

**export EDITOR=mcedit**

А затем:

**crontab -e**

```
demo.peacedeath.su:7015
QEMU (BR-SRV) - noVNC
[root@br-srv ~]# export EDITOR=mcedit
[root@br-srv ~]# crontab -e_
```

Мы попадаем в конфиг, где указываются различные задачи, которые выполняются в назначенное время. В нашем случае нужно перезагружать службу **network** каждый раз после перезапуска системы.

Для этого мы в конце файла пишем следующее:

**@reboot /bin/systemctl restart network**

**!ВАЖНО!** Оставляем пустую строку после введённой строки выше, иначе

AUTHORS: не будет сохранения! В этом файле всегда нужно оставлять снизу  
NECHAEV  
NAUMOV

NAGORNOVA

```
crontab.DGoorh [M--] 0 L:[ 1+ 8 9/ 9] *(201 / 201b) <EOF>
#|minute (0-59),
#|<---->hour (0-23),
#|<---->|<---->day of the month (1-31),
#|<---->|<---->|<---->month of the year (1-12),
#|<---->|<---->|<---->|<---->day of the week (0-6 with 0=Sunday).
#|<---->|<---->|<---->|<---->|<---->commands

@reboot /bin/systemctl restart network
-
```

Если всё сделано успешно, то появится следующее сообщение в консоли:

```
crontab: installing new crontab
[root@br-srv ~]#
```

И теперь вы можете перезагружать спокойно машину, не боясь, что адрес с интерфейса может пропасть. (ПО РФ ☐)

## Настройка HQ-SRV и HQ-CLI производится по заданию позже!

### 2. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

Настройка производится встроенной службой, настроим зону на **HQ-SRV** следующей командой:

**timedatectl set-timezone Asia/Barnaul**

```
set-time      set-timezone
[root@hq-srv ~]# timedatectl set-timezone Asia/Barnaul

```

И проверим правильность настройки:

**timedatectl status**

```
[root@hq-srv ~]# timedatectl set-timezone Asia/Barnaul
[root@hq-srv ~]# timedatectl status
    Local time: Thu 2024-09-12 21:20:56 +07
    Universal time: Thu 2024-09-12 14:20:56 UTC
        RTC time: Thu 2024-09-12 14:20:56
        Time zone: Asia/Barnaul (+07, +0700)
System clock synchronized: yes
          NTP service: active
    RTC in local TZ: no
[root@hq-srv ~]# -
```

Аналогично на других устройствах

Настройка часового пояса завершена завершена.

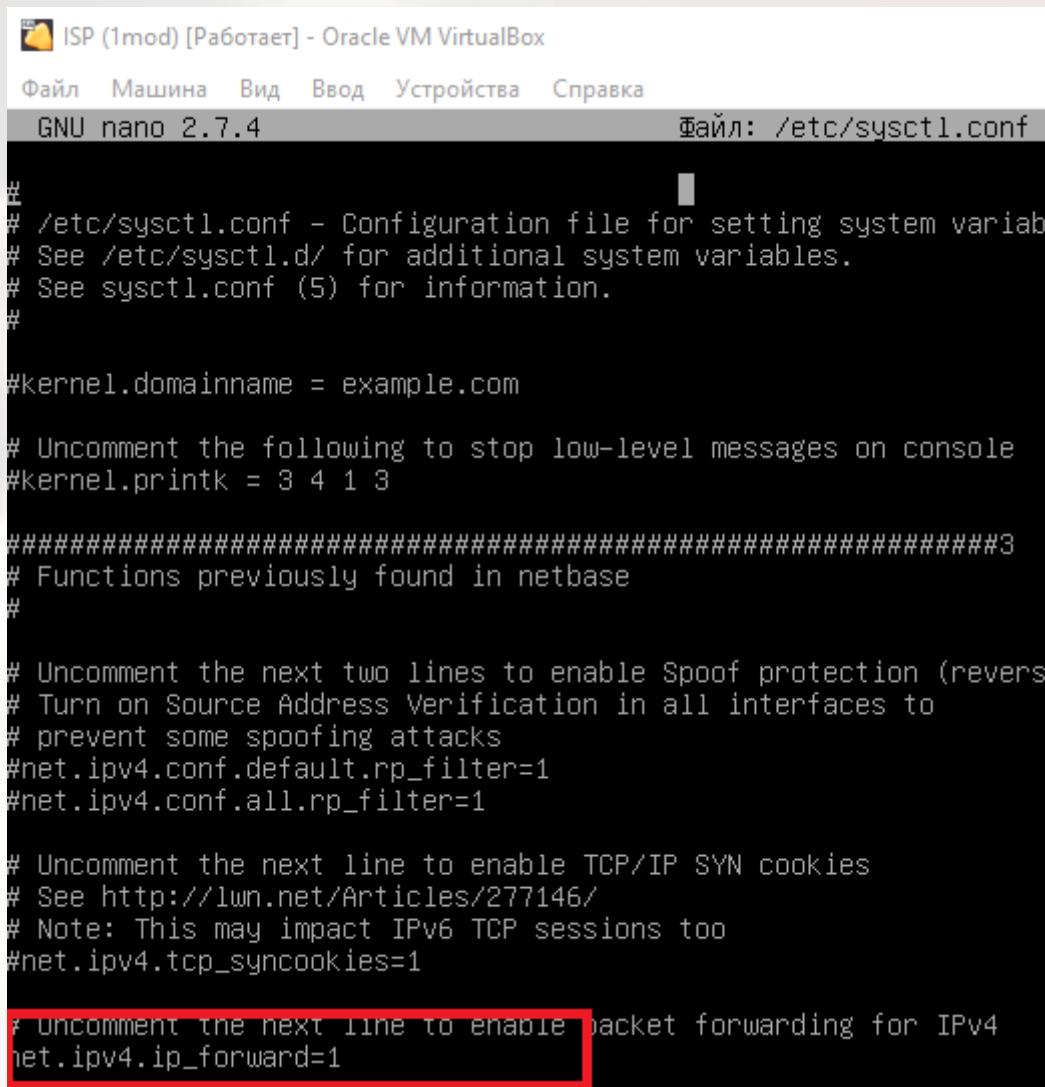
### 3. Настройка forward пакетов:

ISP:

**mcedit /etc/sysctl.conf**

Убрать знак комментария на этой строке:

**net.ipv4.ip\_forward=1**



```
ISP (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
GNU nano 2.7.4                                Файл: /etc/sysctl.conf

#
# /etc/sysctl.conf - Configuration file for setting system variables.
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (revers
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```

И применить изменения:

**sysctl -p**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
root@isp:~# sysctl -p
net.ipv4.ip_forward = 1
root@isp:~# _
```

**АНАЛОГИЧНО НА ДРУГИХ РОУТЕРАХ!**

## 4. Настройка NAT:

**ISP:**

Пишем в консоль следующие команды:

**iptables -t nat -A POSTROUTING -s 172.16.4.0/28 -o eth0 -j MASQUERADE** (Правило для доступа в интернет для устройств сети HQ)

**iptables -t nat -A POSTROUTING -s 172.16.5.0/28 -o eth0 -j MASQUERADE** (Правило для доступа в интернет для устройств сети BR)

**iptables -t nat -L** (Вывод прописанных правил для **nat**)

```
root@isp:~# iptables -t nat -A POSTROUTING -s 172.16.4.0/28 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -A POSTROUTING -s 172.16.5.0/28 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all  --  172.16.4.0/28      anywhere
MASQUERADE  all  --  172.16.5.0/28      anywhere
root@isp:~# _
```

Сохраним наши правила, пишем в консоль следующую команду:

**iptables-save > /root/rules**

```
root@isp:~# iptables-save > /root/rules
root@isp:~# _
```

Запишем в **crontab** одну команду, чтобы при старте системы, правила загружались из файла, в котором они хранятся.

Пишем в консоль следующие команды:

**export EDITOR=mcedit** (Команда одноразовая, для комфортной работы с crontab её нужно писать каждый раз)

**crontab -e**

Добавляем в конец файла следующие строки:

**@reboot /sbin/iptables-restore < /root/rules**

**!ВАЖНО!** Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу ПУСТУЮ СТРОКУ!

```
/tmp/crontab.sA3xop/crontab [----] 0 L:[ 1+24 25/ 25] *(934 / 934
# Edit this file to introduce tasks to be run by cron.
#.
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#.
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#.
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#.
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#.
# For more information see the manual pages of crontab(5) and cron(8)
#.
# m h dom mon dow   command
@reboot /sbin/iptables-restore < /root/rules
-
```

Перезагружаем машину и смотрим список правил, применяются ли они при запуске системы:

**iptables –t nat -L**

AUTHORS:

NECHAEV  
NAUMOV  
NAGORNOVA

```
root@isp:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all  --  172.16.4.0/28      anywhere
MASQUERADE  all  --  172.16.5.0/28      anywhere
root@isp:~#
```

## HQ-RTR:

Пишем в консоль следующие команды:

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/26 -o eth0 -j
MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 192.168.2.0/28 -o eth0 -j
MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 192.168.3.0/29 -o eth0 -j
MASQUERADE
```

```
iptables -t nat -L
```

```
root@isp:~# iptables -t nat -A POSTROUTING -s 192.168.1.0/26 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -A POSTROUTING -s 192.168.2.0/28 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -A POSTROUTING -s 192.168.3.0/29 -o eth0 -j MASQUERADE
root@isp:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
AUTHORS   Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
NECHAEV   MASQUERADE  all  --  192.168.1.0/26      anywhere
NAUMOV    MASQUERADE  all  --  192.168.2.0/28      anywhere
NAGORNOV  MASQUERADE  all  --  192.168.3.0/29      anywhere
root@isp:~#
```

Сохраним наши правила, пишем в консоль следующую команду:

**iptables-save > /root/rules**

```
root@hq-rtr:~# iptables-save > /root/rules
root@hq-rtr:~#
```

Запишем в **crontab** одну команду, чтобы при старте системы, правила загружались из файла, в котором они хранятся.

Ппишем в консоль следующие команды:

```
export EDITOR=mcedit
```

```
crontab -e
```

Добавляем в конец файла следующие строки:

```
@reboot /sbin/iptables-restore < /root/rules
```

**!ВАЖНО!** Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу ПУСТУЮ СТРОКУ!

```
/tmp/crontab.sA3xop/crontab [----] 0 L:[ 1+24 25/ 25] *(934 / 934
# Edit this file to introduce tasks to be run by cron.
#.
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#.
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#.
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#.
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#.
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#.
# For more information see the manual pages of crontab(5) and cron(8)
AUTHORS#
NECHAEV#
NAUMOV#
NAGORNOV@reboot /sbin/iptables-restore < /root/rules
```

Перезагружаем машину и смотрим список правил, применяются ли они при запуске системы:

## **iptables -t nat -L**

```
root@hq-rtr:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source               destination
Chain INPUT (policy ACCEPT)
target    prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source               destination
MASQUERADE  all  --  192.168.1.0/26      anywhere
MASQUERADE  all  --  192.168.2.0/28      anywhere
MASQUERADE  all  --  192.168.3.0/29      anywhere
root@hq-rtr:~# _
```

## **BR-RTR:**

Пишем в консоль следующие команды:

```
iptables -t nat -A POSTROUTING -s 192.168.4.0/27 -o eth0 -j  
MASQUERADE
```

## **iptables -t nat -L**

```
root@br-rtr:~# iptables -t nat -A POSTROUTING -s 192.168.4.0/27 -o eth0 -j MASQUERADE
root@br-rtr:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source               destination
Chain INPUT (policy ACCEPT)
target    prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source               destination
MASQUERADE  all  --  192.168.4.0/27      anywhere
root@br-rtr:~#
```

## **AUTHORS:**

**NECHAEV** Сохраним наши правила, пишем в консоль следующую команду:  
**NAUMOV**  
**NAGORNOY**

```
iptables-save > /root/rules
```

```
root@br-rtr:~# iptables-save > /root/rules
root@br-rtr:~#
```

Запишем в **crontab** одну команду, чтобы при старте системы, правила загружались из файла, в котором они хранятся.

Ппишем в консоль следующие команды:

```
export EDITOR=mcedit
```

```
crontab -e
```

Добавляем в конец файла следующие строки:

```
@reboot /sbin/iptables-restore < /root/rules
```

**!ВАЖНО!** Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу ПУСТУЮ СТРОКУ!

```
/tmp/crontab.sA3xop/crontab [----] 0 L:[ 1+24 25/ 25] *(934 / 934
# Edit this file to introduce tasks to be run by cron.
#.
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#.
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#.
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#.
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#.
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#.
# For more information see the manual pages of crontab(5) and cron(8)
#.
# m h dom mon dow   command
@reboot /sbin/iptables-restore < /root/rules
-
```

#### AUTHORS:

NECHAEV  
NAUMOV

#### NAGORNOVA

**iptables –t nat -L**

```

root@br-rtr:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all   --  192.168.4.0/27      anywhere
root@br-rtr:~# 

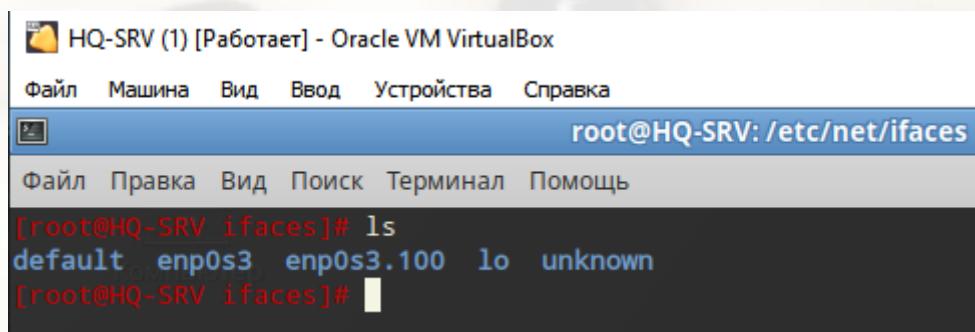
```

## 5. Настройка VLAN для HQ-SRV и HQ-CLI:

### HQ-SRV:

Каталог **enp0s3** (у вас может быть своё название интерфейса, будьте внимательны) оставлять без изменений и перейти к настройке VLAN:

**mkdir /etc/net/ifaces/enp0s3.100** (создание каталога под VLAN интерфейс)



Создадим файл options и откроем его командой

**mcedit /etc/net/ifaces/enp0s3.100/options**

Запишем в него следующее содержимое:

**TYPE=vlan**

**AUTHORS:**

**HOST= enp0s3** (основной интерфейс, но у вас может быть иное название)

**NECHAEV**

**NAUMOV**

**VID=100** (id VLAN'a)

**NAGORNOVA**

**DISABLED=no**

**BOOTPROTO=static**

```
root@HQ-SRV: /etc/net/ifaces/enp0s3.100
options          [----] 16 L:[ 1+ 4   5/  5] *(58   /   58b) <EOF>
TYPE=vlan
HOST=enp0s3
VID=100
DISABLED=no
BOOTPROTO=static
```

Создадим файлы **ipv4address** и **ipv4route** и откроем их командой:

**mcedit /etc/net/ifaces/enp0s3.100/ipv4address**

Записать туда следующую строку:

**192.168.1.2/26**

```
 ipv4address      [----] 14 L:[ 1+ 0   1/  1] *(14   /   14b) <EOF>
192.168.1.2/26_
```

**mcedit /etc/net/ifaces/enp0s3.100/ipv4route**

Записать туда следующую строку:

**default via 192.168.1.1**

```
 ipv4route       [----] 23 L:[ 1+ 0   1/  1] *(23   /   23b) <EOF>
default via 192.168.1.1
```

В итоге должен получится такой набор файлов в каталоге интерфейса:

```
[root@HQ-SRV ifaces]# ls
default enp0s3 enp0s3.100 lo unknown
[root@HQ-SRV ifaces]# cd enp0s3.100
[root@HQ-SRV enp0s3.100]# ls
ipv4address ipv4route options
[root@HQ-SRV enp0s3.100]#
```

Обязательно после всех настроек интерфейсов ввести:

**systemctl restart network**

Также добавим запись о перезагрузке службы **network** в **crontab**.

Делаем это следующим образом, пишем команду:

**export EDITOR=mcedit**

А затем:

**crontab -e**

```
[root@hq-srv ~]# export EDITOR=mcedit
[root@hq-srv ~]# crontab -e
```

И в конце файла пишем следующее:

**@reboot /bin/systemctl restart network**

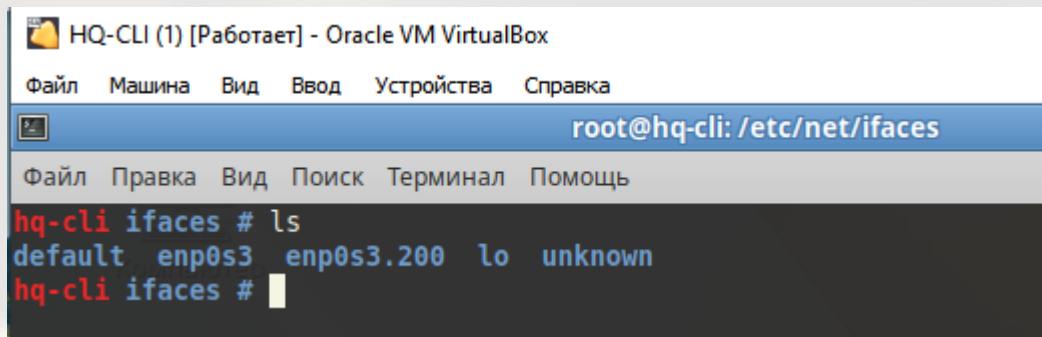
**!ВАЖНО!** Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу ПУСТУЮ СТРОКУ!

```
crontab.1rHLM      [---] 0 L:[ 1+ 0  1/  9] *(0    / 201b) 0035 0x023
AUTHORS
NECHAEV
NAUMOV
NAGORNOV
@reboot /bin/systemctl restart network
```

## HQ-CLI:

Каталог `enp0s3` оставлять без изменений и перейти к настройке VLAN:

`mkdir /etc/net/ifaces/enp0s3.200` (создание каталога под VLAN интерфейс)



```
hq-cli ifaces # ls
default enp0s3 enp0s3.200 lo unknown
hq-cli ifaces #
```

Создадим файл `options` и откроем его командой:

`mcedit /etc/net/ifaces/enp0s3.200/options`

Запишем в него следующее содержимое:

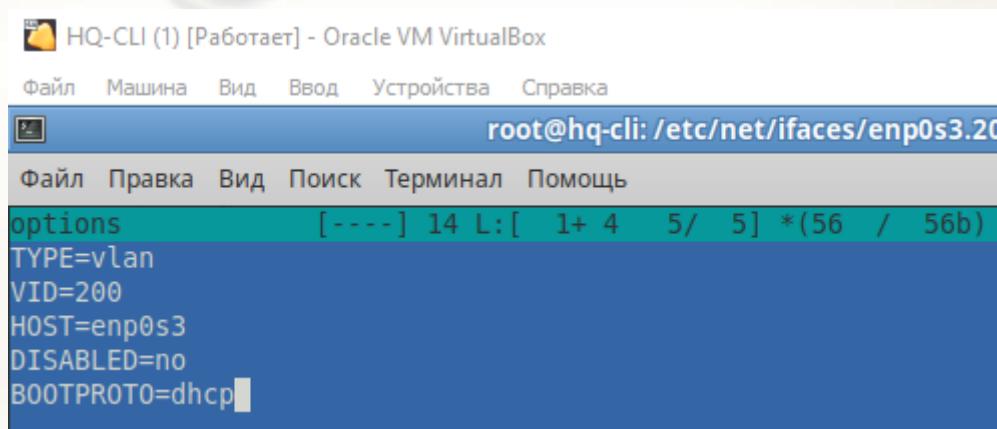
**TYPE=vlan**

**VID=200** (id VLAN'a)

**HOST=enp0s3** (основной интерфейс)

**DISABLED=no**

**BOOTPROTO=dhcp**



```
root@hq-cli:/etc/net/ifaces/enp0s3.200
options          [----] 14 L:[ 1+ 4 5/ 5] *(56 / 56b)
TYPE=vlan
VID=200
HOST=enp0s3
DISABLED=no
BOOTPROTO=dhcp
```

Создавать файлы `ipv4address` и `ipv4route` не нужно, т.к. мы получаем на **HQ-CLI** настройки по **DHCP**, который далее будет настроен на роутере.

Обязательно после всех настроек интерфейсов ввести:

**systemctl restart network** (Альт)

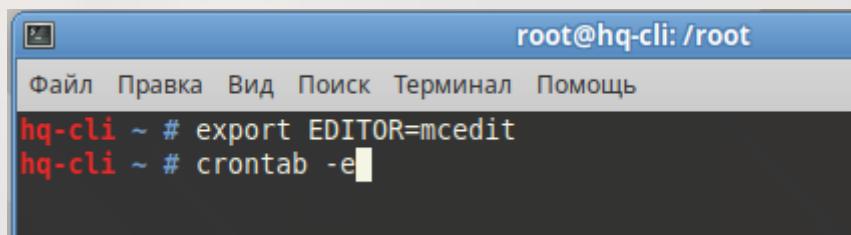
Также добавим запись о перезагрузке службы **network** в **crontab**.

Делаем это следующим образом, пишем команду:

```
export EDITOR=mcedit
```

А затем:

```
crontab -e
```

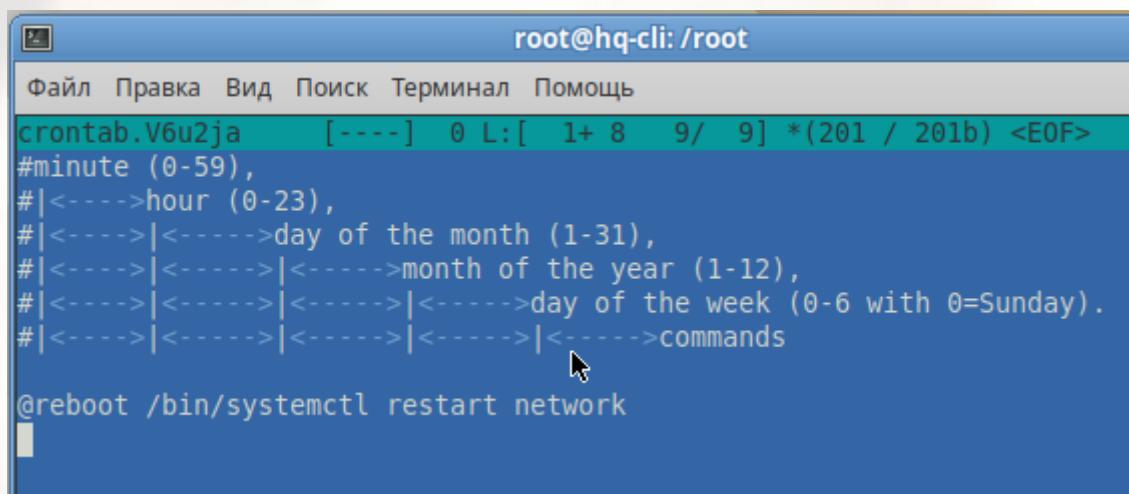


```
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
hq-cli ~ # export EDITOR=mcedit
hq-cli ~ # crontab -e
```

И в конце файла пишем следующее:

```
@reboot /bin/systemctl restart network
```

**!ВАЖНО!** Оставляем пустую строку после введённой строки выше, иначе не будет сохранения! В этом файле всегда нужно оставлять снизу **ПУСТУЮ СТРОКУ!**



```
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
crontab.V6u2ja      [---]  0 L:[ 1+ 8   9/  9] *(201 / 201b) <EOF>
#minute (0-59),
#|<---->hour (0-23),
#|<---->|<---->day of the month (1-31),
#|<---->|<---->|<---->month of the year (1-12),
#|<---->|<---->|<---->|<---->day of the week (0-6 with 0=Sunday).
#|<---->|<---->|<---->|<---->|<---->commands
@reboot /bin/systemctl restart network
```

## 6. Настройка IP-туннеля между офисами HQ и BR:

Создание туннеля производится на маршрутизаторах **HQ-RTR** и **BR-RTR**.

### HQ-RTR:

Для создания туннеля необходимо добавить новый интерфейс в файл **/etc/network/interfaces**

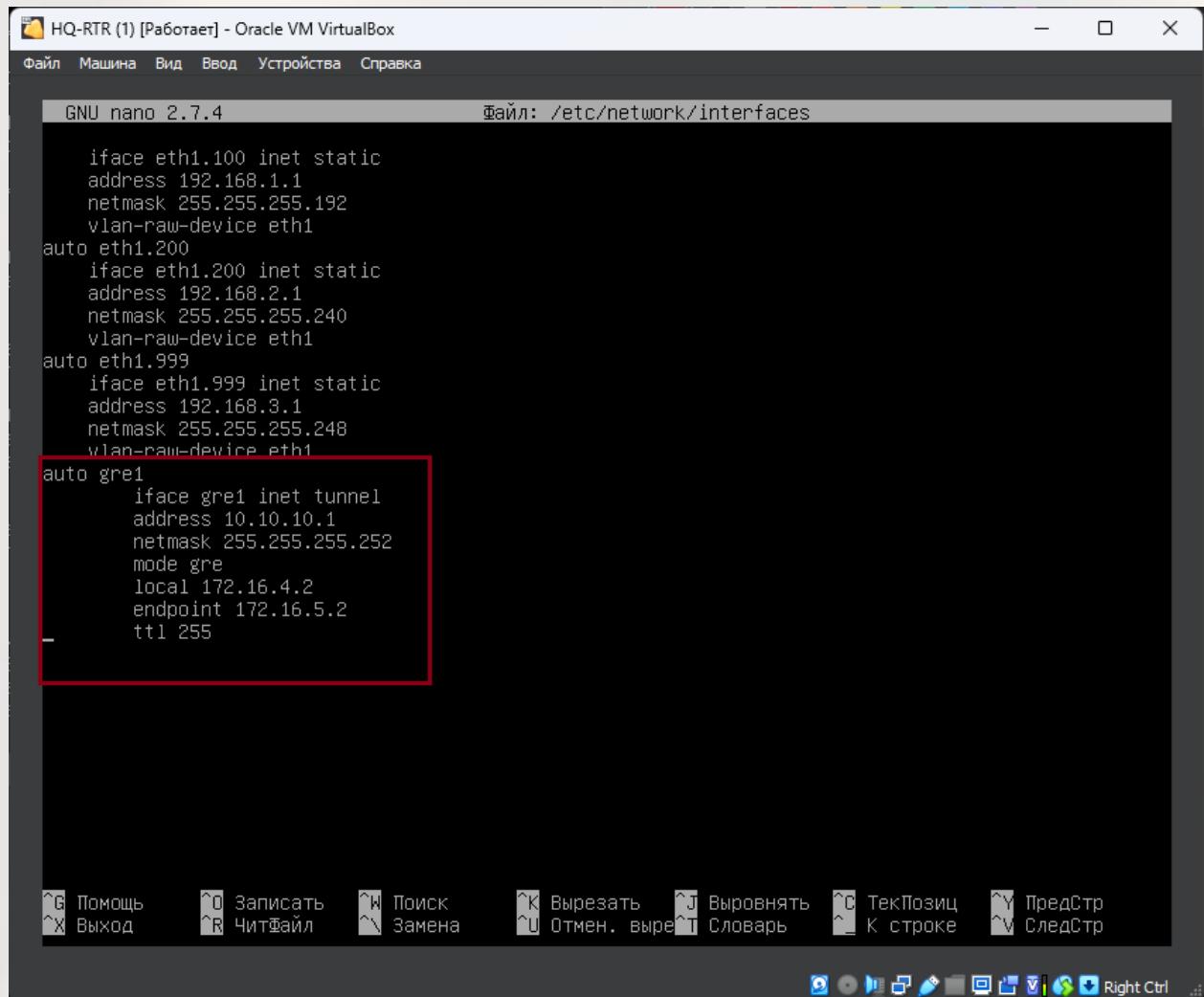
AUTHORS  
NECHAEV

NAUMOV Откроем этот файл текстовым редактором следующей командой:

NAGORNOVA

```
mcedit /etc/network/interfaces
```

Добавляем в конец файла то, что выделено на скриншоте:



```
GNU nano 2.7.4                               Файл: /etc/network/interfaces

iface eth1.100 inet static
address 192.168.1.1
netmask 255.255.255.192
vlan-raw-device eth1
auto eth1.200
iface eth1.200 inet static
address 192.168.2.1
netmask 255.255.255.240
vlan-raw-device eth1
auto eth1.999
iface eth1.999 inet static
address 192.168.3.1
netmask 255.255.255.248
vlan-raw-device eth1
auto gre1
iface gre1 inet tunnel
address 10.10.10.1
netmask 255.255.255.252
mode gre
local 172.16.4.2
endpoint 172.16.5.2
ttl 255
```

Сохраняем файл, выходим из редактора.

Перезапускаем службу networking для применения изменений:

**systemctl restart networking**

Проверяем наличие IP-туннеля:

**ip a**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
inet6 fe80::a00:27ff:fee5:bd61/64 scope link
    valid_lft forever preferred_lft forever
10: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
11: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
12: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
18: eth1.100@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:e5:bd:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/26 brd 192.168.1.63 scope global eth1.100
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:bd61/64 scope link
        valid_lft forever preferred_lft forever
19: eth1.200@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:e5:bd:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/28 brd 192.168.2.15 scope global eth1.200
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:bd61/64 scope link
        valid_lft forever preferred_lft forever
20: eth1.999@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:e5:bd:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.1/29 brd 192.168.3.7 scope global eth1.999
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:bd61/64 scope link
        valid_lft forever preferred_lft forever
21: gre1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/gre 172.16.4.2 peer 172.16.5.2
    inet 10.10.10.1/30 scope global gre1
        valid_lft forever preferred_lft forever
    inet6 fe80::ac10:402/64 scope link
        valid_lft forever preferred_lft forever
root@HQ-RTR:~#
```

Туннель появился.

## BR-RTR:

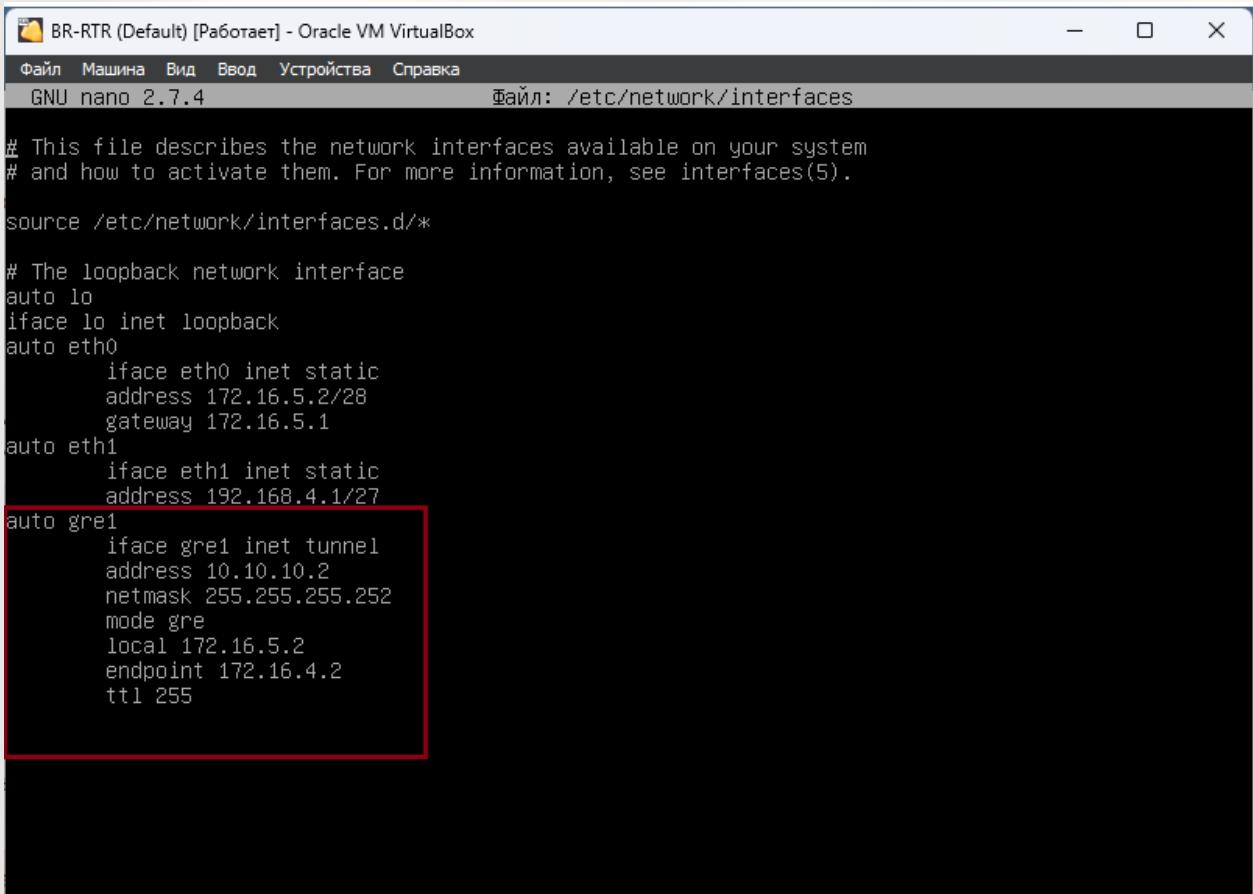
На этом роутере тоже самое, только нужно поменять IP-адрес туннеля и IP-адреса local и endpoint.

Открываем файл текстовым редактором **mcedit** следующей командой:

**mcedit /etc/network/interfaces**

Прописываем в конец файла следующее содержимое:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



```
BR-RTR (Default) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
GNU nano 2.7.4                                     Файл: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
    iface eth0 inet static
        address 172.16.5.2/28
        gateway 172.16.5.1

auto eth1
    iface eth1 inet static
        address 192.168.4.1/27

auto gre1
    iface gre1 inet tunnel
        address 10.10.10.2
        netmask 255.255.255.252
        mode gre
        local 172.16.5.2
        endpoint 172.16.4.2
        ttl 255
```

Сохраняем файл, выходим из редактора.

Также перезапускаем службу networking для применения изменений:

**systemctl restart networking**

Проверяем наличие IP-туннеля:

**ip a**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
BR-RTR (Default) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@BR-RTR:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
0
    link/ether 08:00:27:18:5c:57 brd ff:ff:ff:ff:ff:ff
        inet 172.16.5.2/28 brd 172.16.5.15 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe18:5c57/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
0
    link/ether 08:00:27:9e:5e:be brd ff:ff:ff:ff:ff:ff
        inet 192.168.4.1/27 brd 192.168.4.31 scope global eth1
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe9e:5ebe/64 scope link
            valid_lft forever preferred_lft forever
4: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN group default qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
5: gretap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
6: erspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
7: gre1@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default qlen 1000
    link/gre 172.16.5.2 peer 172.16.4.2
        inet 10.10.10.2/30 scope global gre1
            valid_lft forever preferred_lft forever
        inet6 fe80::ac10:502/64 scope link
            valid_lft forever preferred_lft forever
root@BR-RTR:~# _
```

Туннель между офисами настроен, полностью проверить его работу можно после настройки **OSPF**. Но пинги между **10.10.10.1** и **10.10.10.2** уже должны доходить.

Отправим с **HQ-RTR** эхо-запрос до **BR-RTR** по туннелю:

**ping 10.10.10.2**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
root@HQ-RTR:~# ip --br a
lo          UNKNOWN      127.0.0.1/8 ::1/128
eth0         UP          172.16.4.2/28 fe80::a00:27ff:fe5:665e/64
eth1         UP          fe80::a00:27ff:fe5:bd61/64
gre0@NONE   DOWN
gretap0@NONE DOWN
erspan0@NONE DOWN
eth1.100@eth1 UP          192.168.1.1/26 fe80::a00:27ff:fe5:bd61/64
eth1.200@eth1 UP          192.168.2.1/28 fe80::a00:27ff:fe5:bd61/64
eth1.999@eth1 UP          192.168.3.1/29 fe80::a00:27ff:fe5:bd61/64
gre1@NONE   UNKNOWN      10.10.10.1/30 fe80::ac10:402/64
root@HQ-RTR:~# ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.398 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.420 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.417 ms
^C
--- 10.10.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.398/0.411/0.420/0.025 ms
root@HQ-RTR:~# _
```

Работает, приступаем к следующему этапу для полной работы туннеля

## 7. Настройка динамической маршрутизации с помощью link-state протокола OSPF.

Для работы OSPF нам нужна служба frr, которой по умолчанию нет на наших маршрутизаторах HQ-RTR и BR-RTR, поэтому проделаем следующие шаги.

### HQ-RTR:

Нужно закомментировать в /etc/apt/sources.list первую строку с репозиторием АСТРЫ, т.к. он не имеет пакета frr даже после обновлений репозиториев, вместо него мы будем использовать debian репозиторий.

AUTHORS:

NECHAEV Для начала зайдём туда следующей командой:

NAUMOV

**mcedit /etc/apt/sources.list**

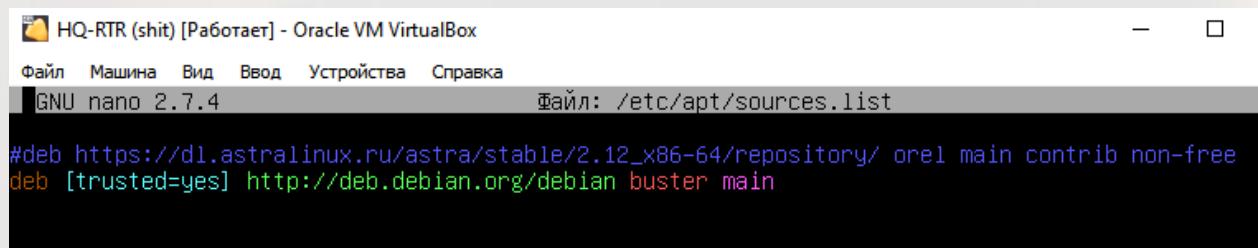
NAGORNOVA

Комментируем первую строку знаком #:

#deb [https://dl.alinux.ru/alinux/stables/2.12\\_x86-64/repository/](https://dl.alinux.ru/alinux/stables/2.12_x86-64/repository/) orel main contrib non-free

Ниже пишем следующую строку:

**deb [trusted=yes] <http://deb.debian.org/debian> buster main**



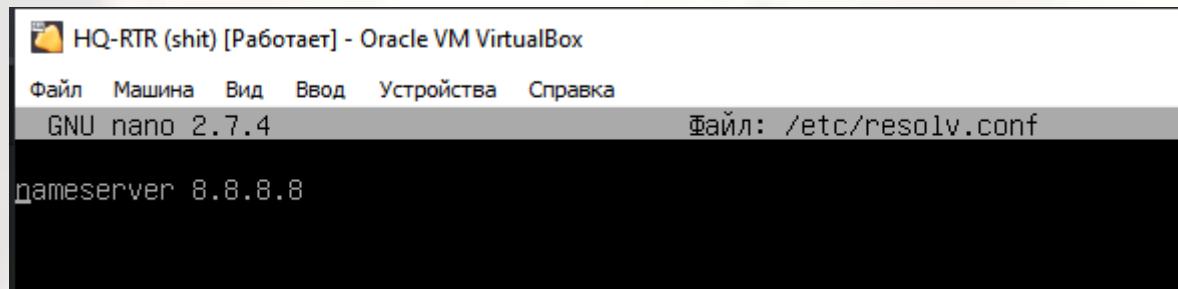
The screenshot shows a terminal window titled "HQ-RTR (shit) [Работает] - Oracle VM VirtualBox". The menu bar includes "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The title bar shows "GNU nano 2.7.4" and "Файл: /etc/apt/sources.list". The main area of the terminal contains the command: "#deb https://dl.astralinux.ru/astra/stable/2.12\_x86-64/repository/ ore1 main contrib non-free deb [trusted=yes] http://deb.debian.org/debian buster main".

Ещё нам нужно добавить в /etc/resolv.conf сервер Google, иначе мы не сможем обновить репозитории, поэтому идём его редактировать следующей командой:

**mcedit /etc/resolv.conf**

И добавляем следующую строку в него:

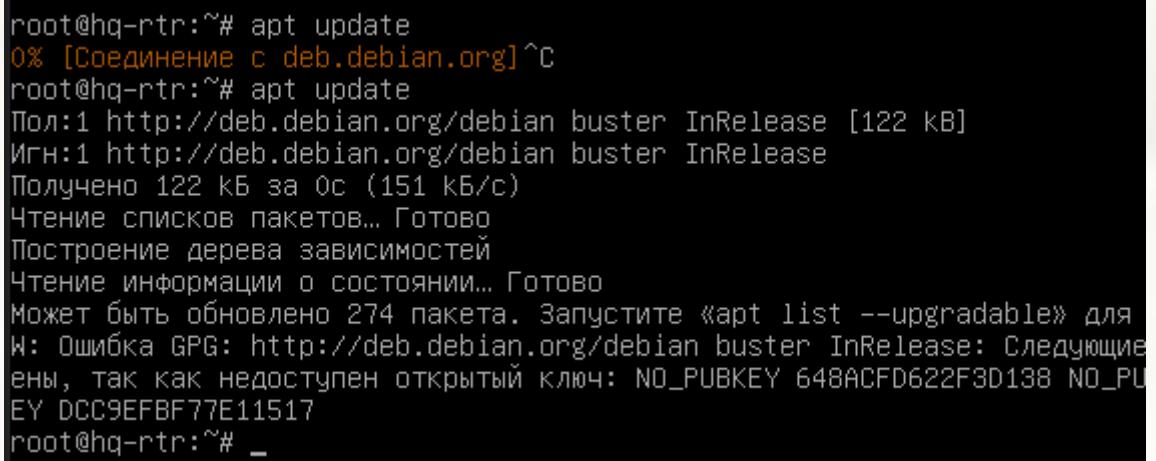
**nameserver 8.8.8.8**



The screenshot shows a terminal window titled "HQ-RTR (shit) [Работает] - Oracle VM VirtualBox". The menu bar includes "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The title bar shows "GNU nano 2.7.4" and "Файл: /etc/resolv.conf". The main area of the terminal contains the command: "nameserver 8.8.8.8".

Сохраняем и идём теперь обновлять список пакетов:

**apt update**



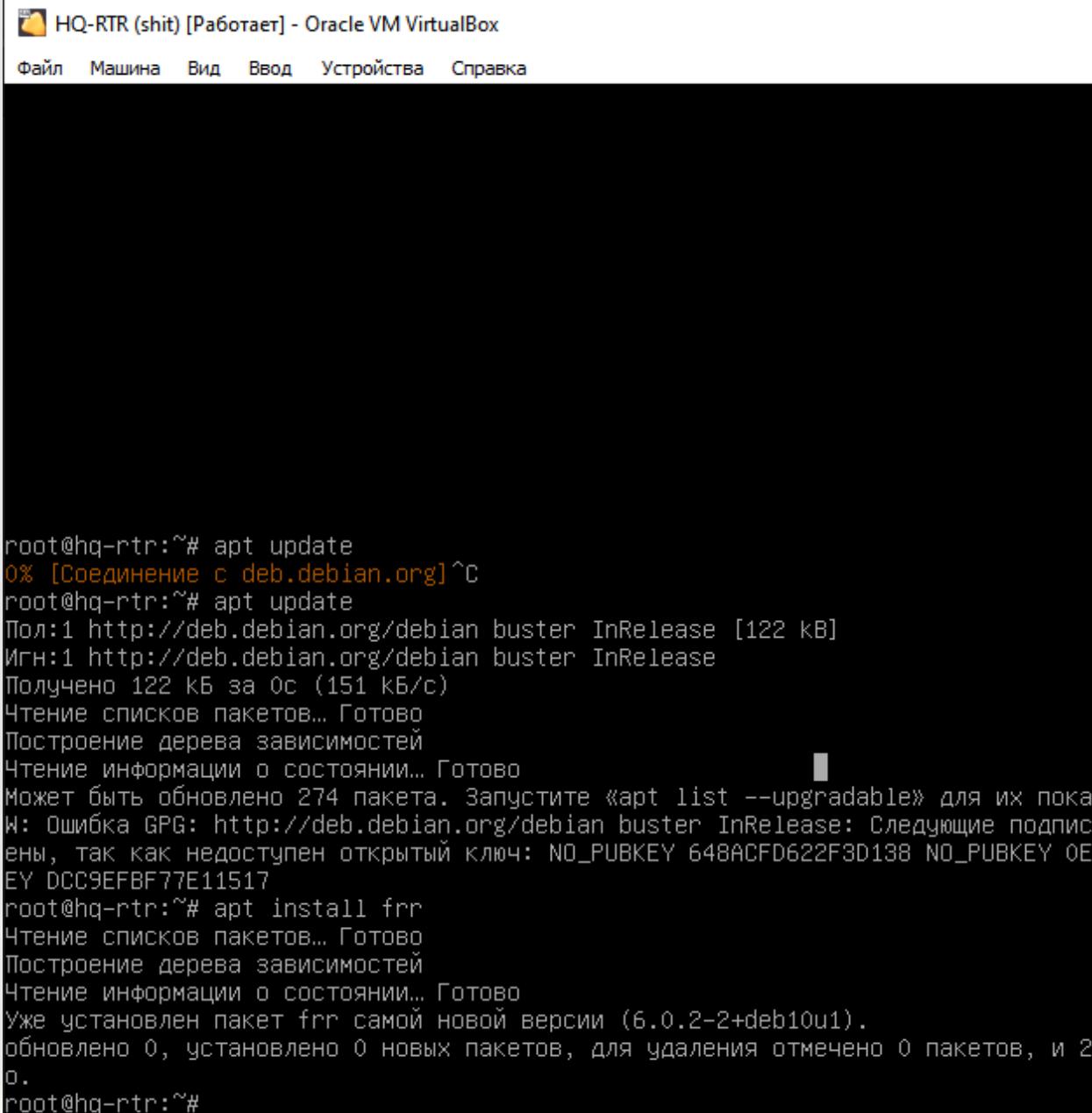
The screenshot shows a terminal window with a "AUTHORS:" watermark on the left. The terminal output shows the execution of "apt update":

```
root@hq-rtr:~# apt update
0% [Соединение с deb.debian.org] ^C
root@hq-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (151 kB/c)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 274 пакета. Запустите «apt list --upgradable» для
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PU
EY DCC9EFBF77E11517
root@hq-rtr:~# _
```

То, что он может ругаться на недоступный открытый ключ, это нормально, идём дальше!

Теперь качаем сам пакет frr:

**apt install frr**



```
root@hq-rtr:~# apt update
0% [Соединение с deb.debian.org]^C
root@hq-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (151 kB/c)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 274 пакета. Запустите «apt list --upgradable» для их показа
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY OE9
EY DCC9EFBF77E11517
root@hq-rtr:~# apt install frr
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет frr самой новой версии (6.0.2-2+deb10u1).
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 2
0.
root@hq-rtr:~#
```

У меня он уже установлен, поэтому не обращаем внимание, скриншот нужен для того, чтобы вы поняли.

Затем нам нужно включить настройку ospf через конфигурационный файл /etc/frr/daemons:

**AUTHORS:**

**NECHAEV** **mcedit /etc/frr/daemons**

**NAUMOV**

NAGORNO Находим в нём следующую строку и приводим её к такому виду:

**ospfd=yes**

```
# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
#
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr and zebra daemons are always started.
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhrpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfdd=no
```

А затем перезагрузим службу командой:

**systemctl restart frr**

А затем начнём настройку:

**vtysh** (зайти в режим настройки)

**conf t** (режим конфигурации, ВСПОМИНАЕМ ЦИСКО, РЕБЯТКИ!)

**router ospf**

**network 10.10.10.0/30 area 0**

**AUTHORS:**  
**NECHAEV**

**NAUMOV**

**NAGORNOVA**

**network 192.168.1.0/26 area 0**

**network 192.168.2.0/28 area 0**

**network 192.168.3.0/29 area 0**

**do wr mem**

```
Astra Linux CE 2.12.46 (ore1) hq-rtr.au-team.irpo tty1
hq-rtr login: root
Password:
Last login: Thu Sep 26 21:25:54 +07 2024 on tty1
root@hq-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-rtr.au-team.irpo# conf t
hq-rtr.au-team.irpo(config)# router ospf
hq-rtr.au-team.irpo(config-router)# network 10.10.10.0/30 area 0
hq-rtr.au-team.irpo(config-router)# network 192.168.1.0/26 area 0
hq-rtr.au-team.irpo(config-router)# network 192.168.2.0/28 area 0
hq-rtr.au-team.irpo(config-router)# network 192.168.3.0/29 area 0
hq-rtr.au-team.irpo(config-router)# do wr mem
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-rtr.au-team.irpo(config-router)#

```

Теперь настроим парольную защиту на нашем GRE туннеле через frr:

**vtysh**

**conf t**

**int gre1**

**ip ospf authentication message-digest**

**ip ospf message-digest-key 1 md5 P@ssw0rd**

**do wr mem**

**AUTHORS:**

**NECHAEV**

**NAUMOV**

**NAGORNOVA**

```
hq@hq-rtr:~# vtysh
Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-rtr.au-team.irpo# conf t
hq-rtr.au-team.irpo(config)# int gre1
hq-rtr.au-team.irpo(config-if)# ip ospf authentication message-digest
hq-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
OSPF: Key 1 already exists
hq-rtr.au-team.irpo(config-if)# no ip ospf message-digest-key 1 md5 P@ssw0rd
hq-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
hq-rtr.au-team.irpo(config-if)# do wr mem
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-rtr.au-team.irpo(config-if)# _
```

OSPF на HQ-RTR настроен.

ПОСЛЕ ПРОДЕЛАННОЙ РАБОТЫ, РАСКОММЕНТИРУЙТЕ РЕПОЗИТОРИЙ АСТРЫ И ЗАКОММЕНТИРУЙТЕ РЕПОЗИТОРИЙ DEBIAN!!! ВОТ ТАК:

```
GNU nano 2.7.4          Файл: /etc/apt/sources.list          Изменён
deb https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository/ orel main contrib non-free
#deb [trusted=yes] http://deb.debian.org/debian buster main
```

## BR-RTR:

Проделываем тоже самое с репозиториями.

Для начала зайдём туда следующей командой:

**mcedit /etc/apt/sources.list**

Комментируем первую строку знаком #:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA  
#deb [https://dl.astralinux.ru/astra/stables/2.12\\_x86-64/repository/](https://dl.astralinux.ru/astra/stables/2.12_x86-64/repository/) orel main  
contrib non-free

Ниже пишем следующую строку:

**deb [trusted=yes] <http://deb.debian.org/debian> buster main**

```
#deb https://d1.astralinux.ru/astra/stable/2.12_x86-64/repository/ orei main contrib non-free
deb [trusted=yes] http://deb.debian.org/debian buster main
```

Теперь нам нужно добавить в /etc/resolv.conf сервер Google:

**mcedit /etc/resolv.conf**

И добавляем следующую строку в него:

**nameserver 8.8.8.8**

```
nameserver 8.8.8.8
```

Сохраняем и идём теперь обновлять список пакетов:

**apt update**

```
Astra Linux CE 2.12.46 (orei) br-rtr.au-team.irpo tty1
br-rtr login: root
Password:
Last login: Fri Sep 27 18:32:52 +07 2024 on tty1
root@br-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (220 kB/c)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 285 пакетов. Запустите «apt list --upgradable» для их показа.
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи не могут быть
      проверены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E98404D386FA1D9
      EY DCC9EFBF77E11517
root@br-rtr:~#
```

**AUTHORS**

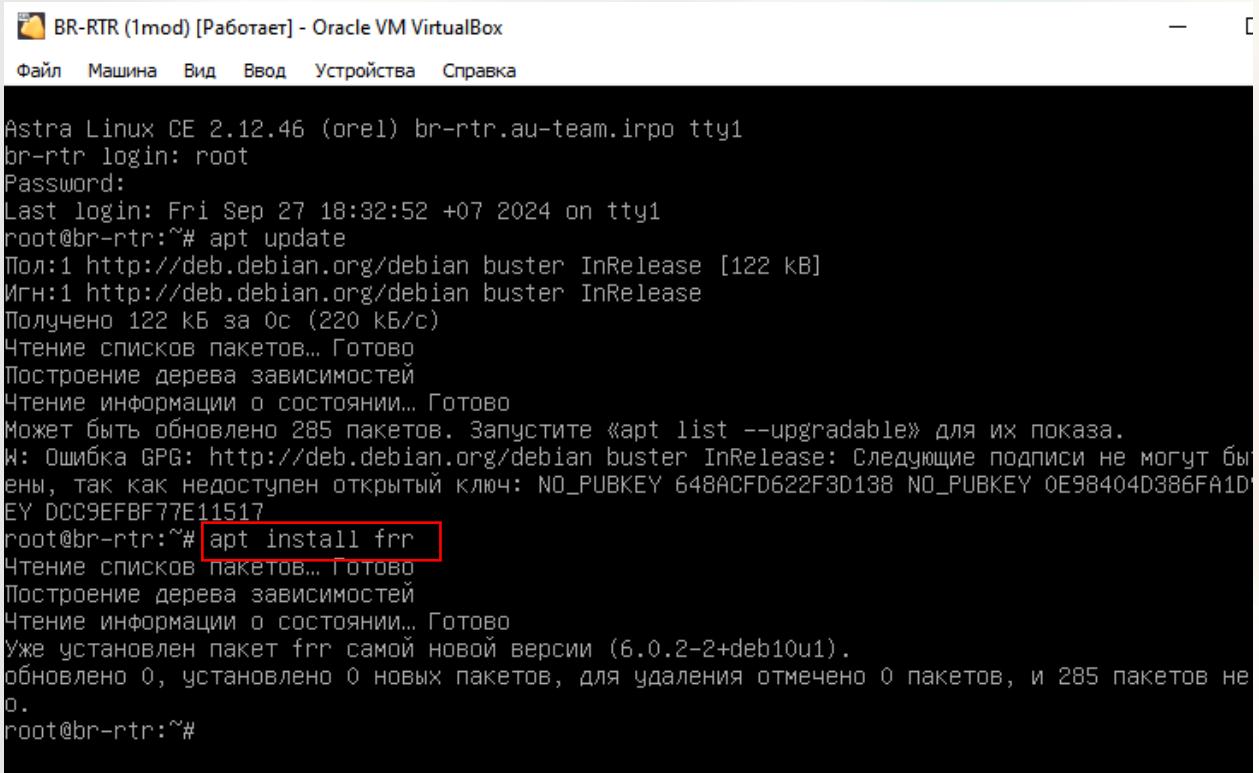
Теперь качаем сам пакет frr:

**NECHAEV**

**NAUMOV**

**apt install frr**

**NAGORNOVA**



```
Astra Linux CE 2.12.46 (orel) br-rtr.au-team.irpo tty1
br-rtr login: root
Password:
Last login: Fri Sep 27 18:32:52 +07 2024 on tty1
root@br-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (220 kB/c)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Может быть обновлено 285 пакетов. Запустите «apt list --upgradable» для их показа.
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи не могут быть
ены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E98404D386FA1D
EY DCC9EFBF77E11517
root@br-rtr:~# apt install frr
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет frr самой новой версии (6.0.2-2+deb10u1).
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 285 пакетов не
0.
root@br-rtr:~#
```

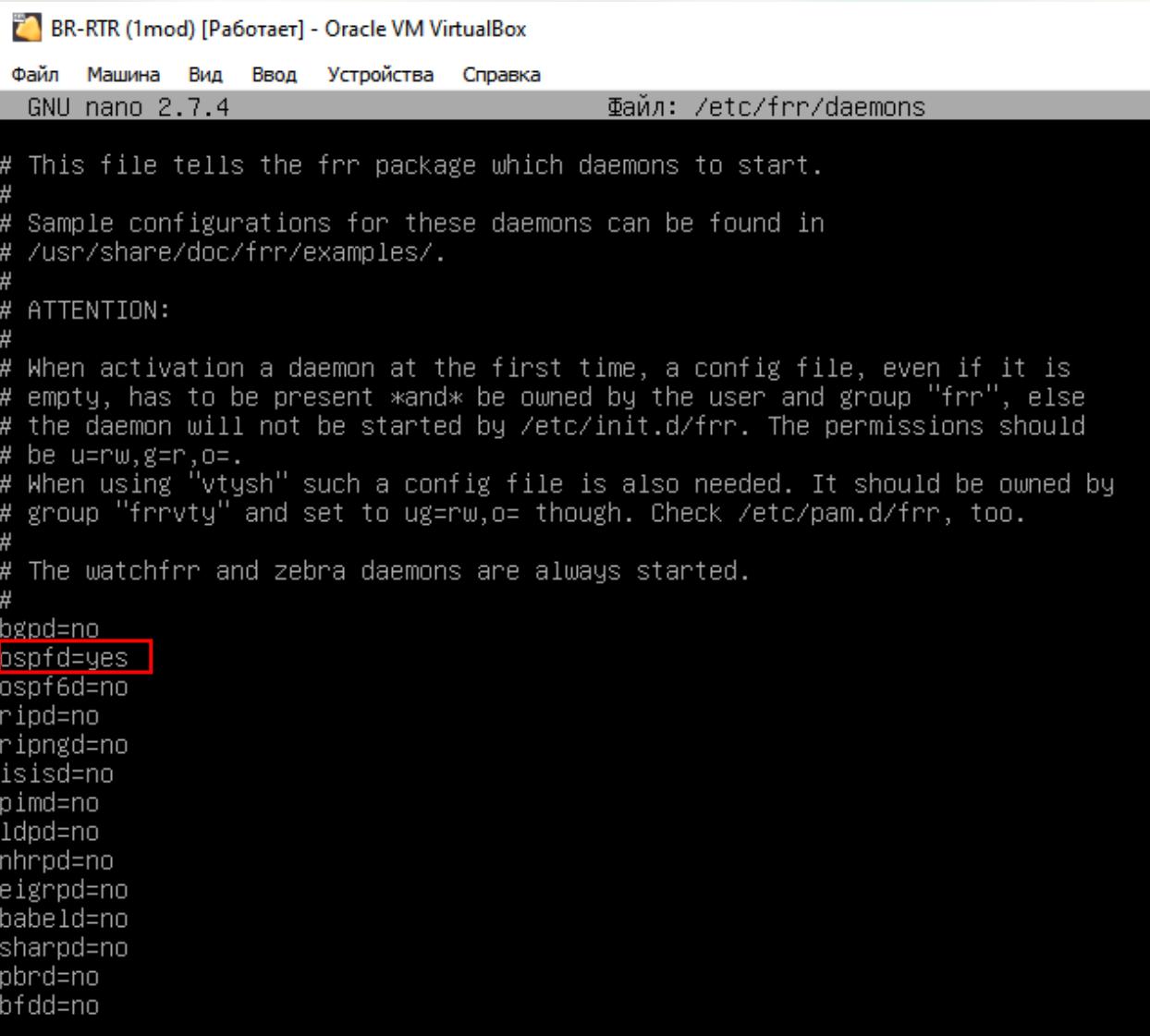
Затем нам нужно включить настройку ospf через конфигурационный файл **/etc/frr/daemons**:

**mcedit /etc/frr/daemons**

Находим в нём следующую строку и приводим её к такому виду:

**ospfd=yes**

**AUTHORS:**  
NECHAEV  
NAUMOV  
NAGORNOVA



```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
GNU nano 2.7.4                                     Файл: /etc/frr/daemons

# This file tells the frr package which daemons to start.
#
# Sample configurations for these daemons can be found in
# /usr/share/doc/frr/examples/.
#
# ATTENTION:
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /etc/init.d/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
# The watchfrr and zebra daemons are always started.
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhrpdb=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfdd=no
```

А затем перезагрузим службу командой:

**systemctl restart frr**

А затем начнём настройку:

**vtysh**

**conf t**

**router ospf**

**network 10.10.10.0/30 area 0**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOY

**network 192.168.4.0/27 area 0**

**do wr mem**

```

BR-RTR (1mod) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка
root@br-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

br-rtr.au-team.irpo# conf t
br-rtr.au-team.irpo(config)# router ospf
br-rtr.au-team.irpo(config-router)# network 10.10.10.0/30 area 0
br-rtr.au-team.irpo(config-router)# network 192.168.4.0/27 area 0
br-rtr.au-team.irpo(config-router)# do wr mem
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
br-rtr.au-team.irpo(config-router)#

```

Теперь настроим парольную защиту на нашем GRE туннеле через **frr** на второй стороне тоже:

**vtysh**

**conf t**

**int gre1**

**ip ospf authentication message-digest**

**ip ospf message-digest-key 1 md5 P@ssw0rd**

**do wr mem**

```

BR-RTR (1mod) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка
Astra Linux CE 2.12.46 (orel) br-rtr.au-team.irpo tty1
br-rtr login: root
Password:
Last login: Thu Sep 26 22:24:17 +07 2024 on tty1
root@br-rtr:~# vtysh

Hello, this is FRRouting (version 6.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

AUTHORS
NECHAEV br-rtr.au-team.irpo# conf t
NAUMOV br-rtr.au-team.irpo(config)# int gre1
NAGORNOV br-rtr.au-team.irpo(config-if)# ip ospf authentication message-digest
OSPF: Key 1 already exists
br-rtr.au-team.irpo(config-if)# no ip ospf message-digest-key 1 md5 P@ssw0rd
br-rtr.au-team.irpo(config-if)# ip ospf message-digest-key 1 md5 P@ssw0rd
br-rtr.au-team.irpo(config-if)#

```

**OSPF на BR-RTR настроен.**

Также нужно вернуть репозиторий астры обратно, смотрите выше, как мы это делали, но в обратном порядке выполняя шаги.

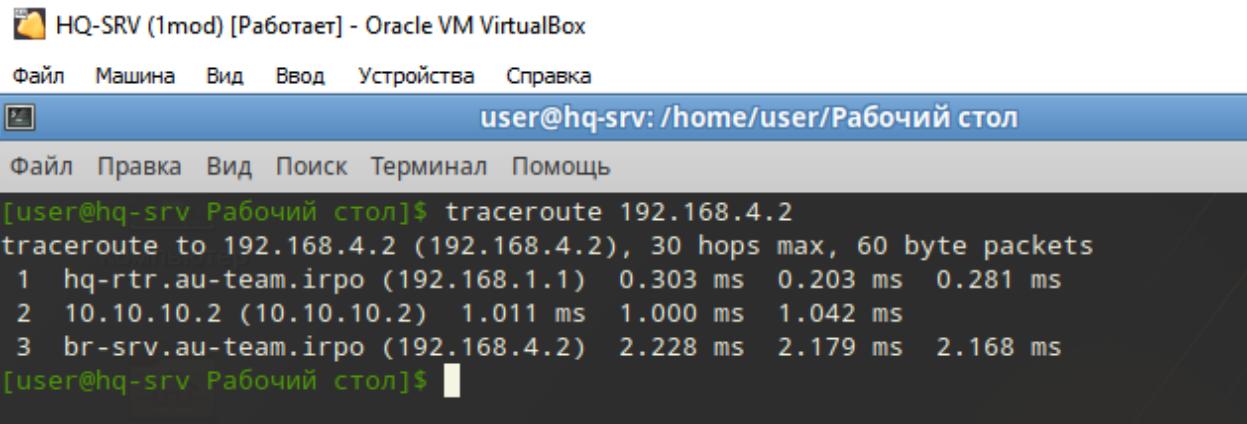
**OSPF** полностью настроен, теперь пинг должен идти везде и по туннелям, проверим это.

**ИНОГДА НУЖНО ЧУТЬ ПОДОЖДАТЬ, ПОКА ПОЯВИТСЯ СОСЕД, ПОЭТОМУ ПИНГ И ТРАССИРОВКА МОГУТ СРАЗУ НЕ ПОЙТИ, ПРОВЕРЯЙТЕ СОСЕДЕЙ ЧЕРЕЗ VTYSH С ПОМОЩЬЮ КОМАНДЫ:**

**do show ip ospf neighbor**

Сделаем трассировку от сервера **HQ-SRV** до **BR-SRV**:

**traceroute 192.168.4.2**



```
user@hq-srv: /home/user/Рабочий стол
traceroute to 192.168.4.2 (192.168.4.2), 30 hops max, 60 byte packets
 1  hq-rtr.au-team.irgo (192.168.1.1)  0.303 ms  0.203 ms  0.281 ms
 2  10.10.10.2 (10.10.10.2)  1.011 ms  1.000 ms  1.042 ms
 3  br-srv.au-team.irgo (192.168.4.2)  2.228 ms  2.179 ms  2.168 ms
```

Всё отлично проходит **через** наш туннель, поздравляю!

(Доменные имена будут показываться после настройки **DNS**, просто мы это проделали для себя ранее, а вы следуйте пунктам дальше!)

## 8. Настройка протокола динамической конфигурации хостов (DHCP):

Настройка будет производиться на **HQ-RTR**!

Использовать в качестве **DHCP** мы будем **dnsmasq**, служба, которой по умолчанию нет в наших ОС Российской производств.

Ещё нам нужно добавить в **resolv.conf** сервер **Google**, иначе мы не сможем обновить репозитории, поэтому идём его редактировать следующей командой:

**mcedit /etc/resolv.conf**

И добавляем следующую строку в него:

**nameserver 8.8.8.8**

```
GNU nano 2.7.4
Файл: /etc/resolv.conf
nameserver 8.8.8.8
```

Обновим пакеты и установим её командами:

**apt update**

**apt install dnsmasq**

```
root@hq-rtr:~# apt update
root@hq-rtr:~# apt install dnsmasq
root@hq-rtr:~#
```

Затем зайдем в настройки конфигурационного файла командой:

**AUTHORS:**

**NECHAEV**

**NAUMOV**

**NAGORNOY** И внесем в него следующие строки (можно прямо в начало файла):

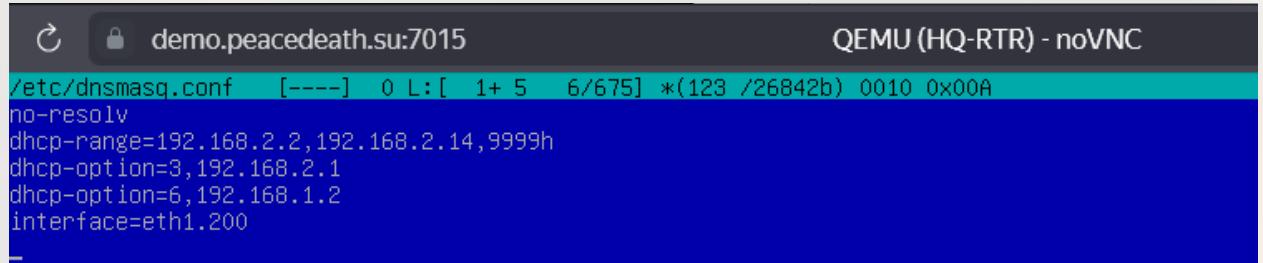
**no-resolv**

**dhcp-range=192.168.2.2,192.168.2.14,9999h**

**dhcp-option=3,192.168.2.1**

**dhcp-option=6,192.168.1.2**

**interface=eth1.200**



```
/etc/dnsmasq.conf  [----]  0 L:[ 1+ 5   6/675] *(123 /26842b) 0010 0x00A
no-resolv
dhcp-range=192.168.2.2,192.168.2.14,9999h
dhcp-option=3,192.168.2.1
dhcp-option=6,192.168.1.2
interface=eth1.200
-
```

Затем перезапускаем службу и посмотрим её статус:

**systemctl restart dnsmasq**

**systemctl status dnsmasq**

```
root@hq-rtr:~# systemctl restart dnsmasq
root@hq-rtr:~# systemctl status dnsmasq
● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
  Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-09-26 10:27:21 +07; 6s ago
    Process: 1231 ExecStop=/etc/init.d/dnsmasq systemd-stop-resolvconf (code=exited, status=0/SUCCESS)
    Process: 1257 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf (code=exited, status=0/SUCCESS)
    Process: 1243 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited, status=0/SUCCESS)
    Process: 1242 ExecStartPre=/usr/sbin/dnsmasq --test (code=exited, status=0/SUCCESS)
  Main PID: 1256 (dnsmasq)
     Tasks: 1 (limit: 4915)
    CGroup: /system.slice/dnsmasq.service
            └─1256 /usr/sbin/dnsmasq -x /run/dnsmasq/dnsmasq.pid -u dnsmasq -7 /etc/dnsmasq.d,.dp

сен 26 10:27:21 hq-rtr.au-team.irpo systemd[1]: Stopped dnsmasq - A lightweight DHCP and caching
сен 26 10:27:21 hq-rtr.au-team.irpo systemd[1]: Starting dnsmasq - A lightweight DHCP and caching
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1242]: dnsmasq: syntax check OK.
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: started, version 2.76 cachesize 150
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: compile time options: IPv6 GNU-getopt DBus i18n NLS iconv
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: warning: no upstream servers configured
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq-dhcp[1256]: DHCP, IP range 192.168.2.2 -- 192.168.2.254
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq-dhcp[1256]: DHCP, sockets bound exclusively to interface eth1.200
сен 26 10:27:21 hq-rtr.au-team.irpo dnsmasq[1256]: read /etc/hosts - 5 addresses
сен 26 10:27:21 hq-rtr.au-team.irpo systemd[1]: Started dnsmasq - A lightweight DHCP and caching
lines 1-22/22 (END)
```

Проверим работу службы на **HQ-CLI**, перезапускаем службу **network** на нём и посмотрим, выдался ли нам адрес:

**systemctl restart network**

**ip a**

**AUTHORS:**

NECHAEV  
NAUMOV  
NAGORNOVA

```
hq-cli ifaces # ls
default enp0s3 enp0s3.200 lo unknown
hq-cli ifaces # cd enp0s3.200/
hq-cli enp0s3.200 # mcedit options

hq-cli enp0s3.200 # ls
options
hq-cli enp0s3.200 # systemctl restart network
hq-cli enp0s3.200 # ipa
-bash: ipa: команда не найдена
hq-cli enp0s3.200 # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group 1000
    link/ether 08:00:27:f7:e6:e1 brd ff:ff:ff:ff:ff:ff
        inet6 fe80::a00:27ff:fed7:e6e1/64 scope link
            valid_lft forever preferred_lft forever
5: enp0s3.200@enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state DOWN group 1000
    link/ether 08:00:27:f7:e6:e1 brd ff:ff:ff:ff:ff:ff
        inet 192.168.2.5/28 brd 192.168.2.15 scope global dynamic noprefixroute enp0s3.200
            valid_lft 3596346sec preferred_lft 3146796sec
        inet6 fe80::a00:27ff:fed7:e6e1/64 scope link
            valid_lft forever preferred_lft forever
hq-cli enp0s3.200 #
```

**enp0s3.200** на **HQ-CLI** успешно получил адрес из диапазона.

## 9. Настройка DNS для офисов HQ и BR:

Для начала необходимо отключить несовместимую службу bind если она есть, командой

**systemctl disable --now bind**

Для работы **DNS** есть служба **dnsmasq** (она же и для **DHCP**)

AUTHORS  
NECHAEV  
NAUMOV  
NAGORNOY  
Установим её на наш сервер **HQ-SRV** (если есть, как у нас, то переходите к следующему шагу).

Ещё нам нужно добавить в **resolv.conf** сервер **Google**, иначе мы не сможем обновить репозитории, поэтому идём его редактировать следующей командой:

**mcedit /etc/resolv.conf**

И добавляем следующую строку в него:

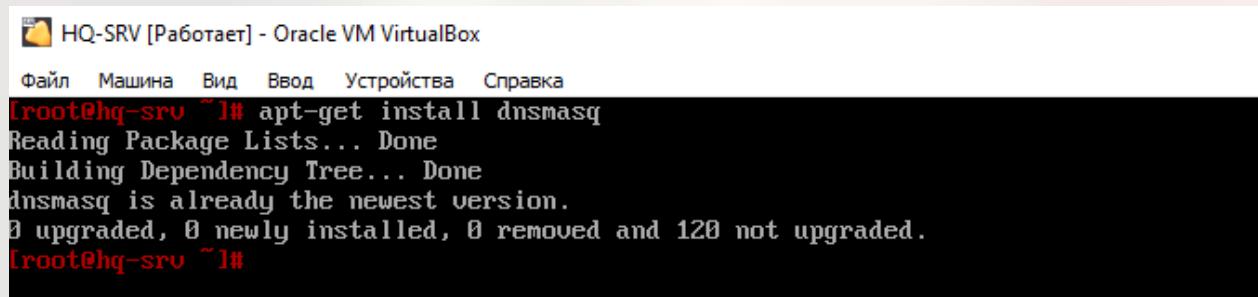
## **nameserver 8.8.8.8**

Обновим пакеты и установим её командами:

**apt-get update**

**apt-get install dnsmasq** (Установка пакета dnsmasq)

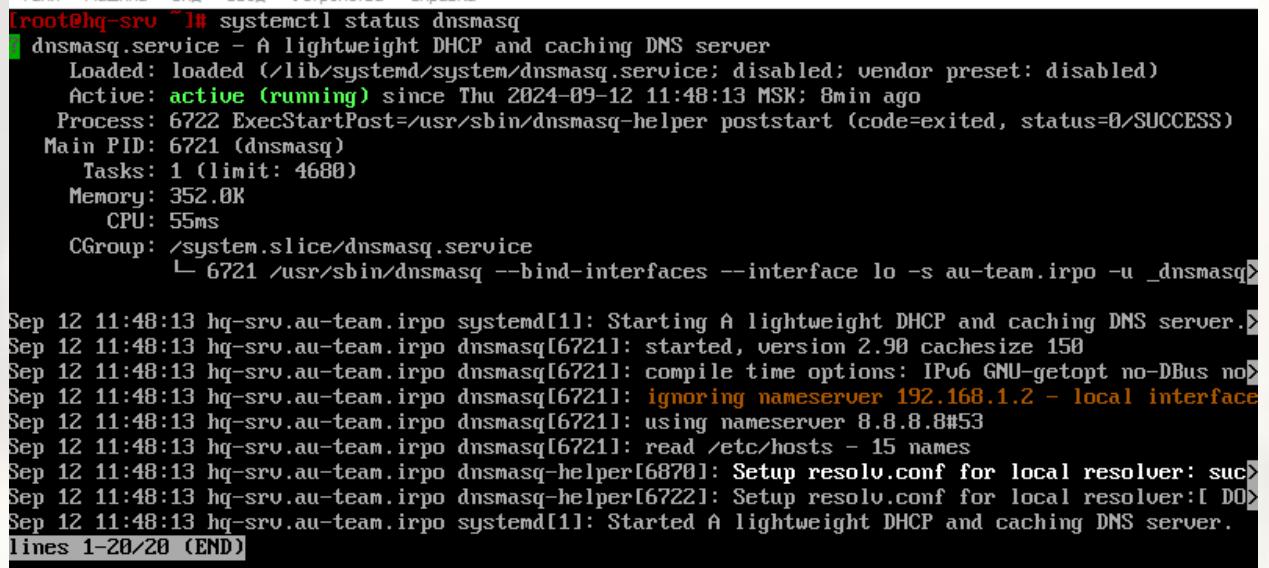
**systemctl enable --now dnsmasq** (Добавление службы в автозапуск)



```
[root@hq-srv ~]# apt-get install dnsmasq
Reading Package Lists... Done
Building Dependency Tree... Done
dnsmasq is already the newest version.
0 upgraded, 0 newly installed, 0 removed and 120 not upgraded.
[root@hq-srv ~]#
```

Проверим её состояние перед работой:

**systemctl status dnsmasq**



```
[root@hq-srv ~]# systemctl status dnsmasq
● dnsmasq.service - A lightweight DHCP and caching DNS server
  Loaded: loaded (/lib/systemd/system/dnsmasq.service; disabled; vendor preset: disabled)
  Active: active (running) since Thu 2024-09-12 11:48:13 MSK; 8min ago
    Process: 6722 ExecStartPost=/usr/sbin/dnsmasq-helper poststart (code=exited, status=0/SUCCESS)
   Main PID: 6721 (dnsmasq)
     Tasks: 1 (limit: 4680)
    Memory: 352.0K
      CPU: 55ms
     CGroup: /system.slice/dnsmasq.service
             └─ 6721 /usr/sbin/dnsmasq --bind-interfaces --interface lo -s au-team.irpo -u _dnsmasq>

Sep 12 11:48:13 hq-srv.au-team.irpo systemd[1]: Starting A lightweight DHCP and caching DNS server...
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: started, version 2.90 cachesize 150
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: compile time options: IPv6 GNU-getopt no-DBus no-Lib
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: ignoring nameserver 192.168.1.2 - local interface
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: using nameserver 8.8.8.8#53
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq[6721]: read /etc/hosts - 15 names
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq-helper[6870]: Setup resolv.conf for local resolver: success
Sep 12 11:48:13 hq-srv.au-team.irpo dnsmasq-helper[6722]: Setup resolv.conf for local resolver: success
Sep 12 11:48:13 hq-srv.au-team.irpo systemd[1]: Started A lightweight DHCP and caching DNS server.
Lines 1-20/20 (END)
```

Затем откроем файл для редактирования конфигурации нашего DNS-сервера:

**mcedit /etc/dnsmasq.conf**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

**domain=au-team.irpo**

**server=8.8.8.8** (адрес общедоступного DNS-сервера)

**interface=\*** (на каком интерфейсе будет работать служба)

**address=/hq-rtr.au-team.irpo/192.168.1.1**  
**ptr-record=1.1.168.192.in-addr.arpa,hq-rtr.au-team.irpo**  
**cname=moodle.au-team.irpo,hq-rtr.au-team.irpo**  
**cname=wiki.au-team.irpo,hq-rtr.au-team.irpo**

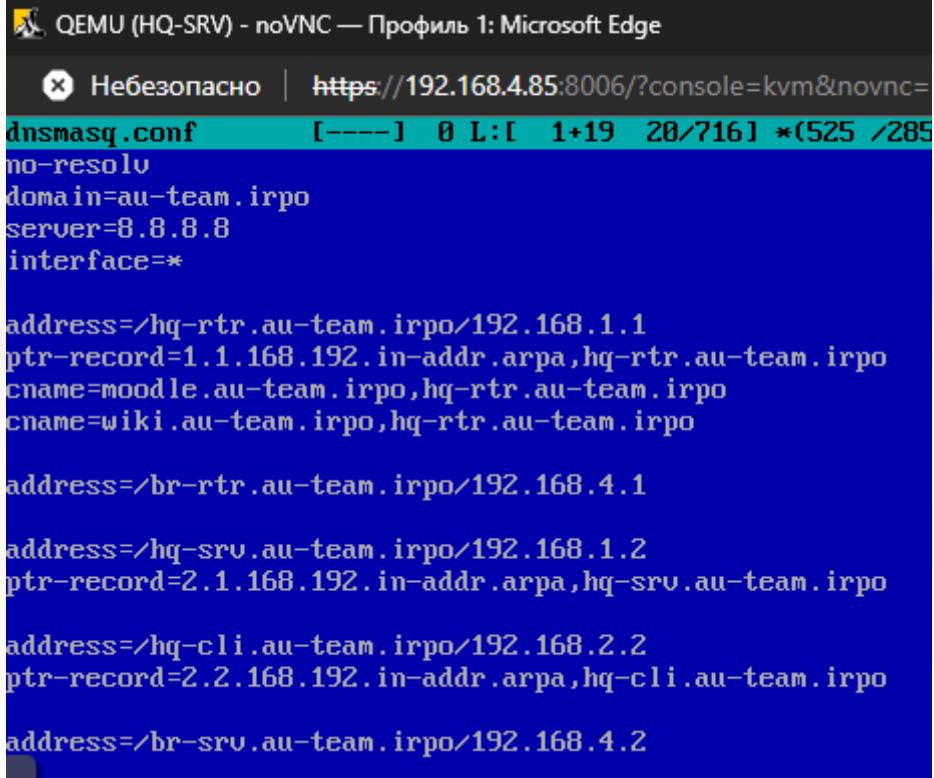
**address=/br-rtr.au-team.irpo/192.168.4.1**

**address=/hq-srv.au-team.irpo/192.168.1.2**  
**ptr-record=2.1.168.192.in-addr.arpa,hq-srv.au-team.irpo**

**address=/hq-cli.au-team.irpo/192.168.2.2** (Смотрите адрес на HQ-CLI, т.к он выдаётся по DHCP)

**ptr-record=2.2.168.192.in-addr.arpa,hq-cli.au-team.irpo**

**address=/br-srv.au-team.irpo/192.168.4.2**



```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
× Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=
dnsmasq.conf      [---] 0 L:1 1+19 20/716 *(525 /285
no-resolv
domain=au-team.irpo
server=8.8.8.8
interface=*

address=/hq-rtr.au-team.irpo/192.168.1.1
ptr-record=1.1.168.192.in-addr.arpa,hq-rtr.au-team.irpo
cname=moodle.au-team.irpo,hq-rtr.au-team.irpo
cname=wiki.au-team.irpo,hq-rtr.au-team.irpo

address=/br-rtr.au-team.irpo/192.168.4.1

address=/hq-srv.au-team.irpo/192.168.1.2
ptr-record=2.1.168.192.in-addr.arpa,hq-srv.au-team.irpo

address=/hq-cli.au-team.irpo/192.168.2.2
ptr-record=2.2.168.192.in-addr.arpa,hq-cli.au-team.irpo

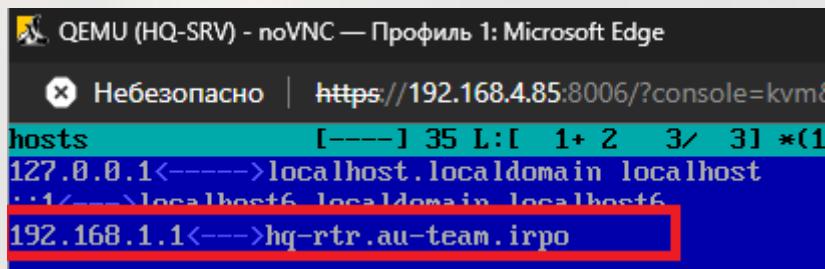
address=/br-srv.au-team.irpo/192.168.4.2
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

Сохраняем файл нажатием кнопки **F2**, а затем выход с помощью **F10**.

Теперь необходимо добавить строку **192.168.1.1 hq-rtr.au-team.irpo** в файл **/etc/hosts**:

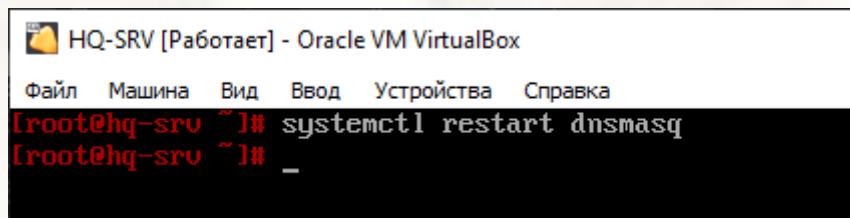
**mcedit /etc/hosts**



Сохраняем файл, выходим из редактора.

Перезапускаем службу командой:

**systemctl restart dnsmasq**



Проверим пинг сначала с HQ-SRV на google.com и hq-rtr.au-team.irpo:

**ping google.com**

**ping hq-rtr.au-team.irpo**

```
[root@hq-srv ~]# ping google.com
PING google.com (64.233.162.102) 56(84) bytes of data.
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=1 ttl=105 time=63.9 ms
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=2 ttl=105 time=63.4 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 63.353/63.604/63.855/0.251 ms
[root@hq-srv ~]# ping hq-rtr.au-team.irpo
PING hq-rtr.au-team.irpo (192.168.1.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=1 ttl=64 time=0.406 ms
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=2 ttl=64 time=0.730 ms
^C
--- hq-rtr.au-team.irpo ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1054ms
rtt min/avg/max/mdev = 0.406/0.568/0.730/0.162 ms
[root@hq-srv ~]#
```

AUTHORS  
NECHAEV  
NAUMOV  
NAGORNOVA

Теперь проверим пинг с HQ-CLI:

**ping google.com**

**ping hq-rtr.au-team.irpo**

HQ-CLI [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

root@c1epdhwwroiqk: /etc/net/ifaces/enp0s3.200 (на c1epdhwwroiqk)

Файл Правка Вид Поиск Терминал Помощь

```
hq-cli enp0s3.200 # ping google.com
PING google.com (64.233.162.102) 56(84) bytes of data.
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=1 ttl=105 time=61.2 ms
64 bytes from li-in-f102.1e100.net (64.233.162.102): icmp_seq=2 ttl=105 time=60.7 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 60.722/60.952/61.182/0.230 ms
hq-cli enp0s3.200 # ping hq-rtr.au-team.irpo
PING hq-rtr.au-team.irpo (192.168.1.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=1 ttl=64 time=0.220 ms
64 bytes from hq-rtr.au-team.irpo (192.168.1.1): icmp_seq=2 ttl=64 time=0.616 ms
^C
--- hq-rtr.au-team.irpo ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.220/0.418/0.616/0.198 ms
hq-cli enp0s3.200 #
```

И проверим работу CNAME записей с HQ-CLI:

**dig moodle.au-team.irpo**

user@host-15: /home/user

Файл Правка Вид Поиск Терминал Помощь

```
[user@host-15 ~]$ dig moodle.au-team.irpo

; <>> DiG 9.16.48 <>> moodle.au-team.irpo
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5764
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;moodle.au-team.irpo.           IN      A

;; ANSWER SECTION:
moodle.au-team.irpo.    0       IN      CNAME   hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo.    0       IN      A       192.168.1.1

;; Query time: 0 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Sun Sep 29 17:03:08 +07 2024
;; MSG SIZE  rcvd: 97
[user@host-15 ~]$
```

**dig wiki.au-team.irpo**

```
hq-cli ~ # dig wiki.au-team.irpo
; <>> DiG 9.16.35 <>> wiki.au-team.irpo
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46488
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;wiki.au-team.irpo.           IN      A
;;
;; ANSWER SECTION:
wiki.au-team.irpo.      0      IN      CNAME   hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo.    0      IN      A       192.168.1.1
;;
;; Query time: 1 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Wed Oct 02 16:22:29 +07 2024
;; MSG SIZE rcvd: 95
```

Наш DNS-сервер настроен.

## 10. Создание локальных учетных записей:

### Создание на HQ-SRV:

Для создания пользователя с определённым идентификатором на машине под управлением ОС Alt Linux нужно использовать команду:

**useradd sshuser -u 1010**

```
[root@hq-srv ~]# useradd sshuser -u 1010
```

Для проверки можно использовать команду:

**id sshuser**

```
[root@hq-srv ~]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=1010(sshuser)
```

AUTHORS:

NECHAEV  
NAUMOV

NAGORNOVA

**passwd sshuser**

После чего ввести и подтвердить новый пароль:

**P@ssw0rd**

```
[root@hq-srv ~]# passwd sshuser
passwd: updating all authentication tokens for user sshuser.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use a password containing at least 7 characters from all of these classes, or a password containing at least 8 characters from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as your password: "drag3speech*Fog".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
[root@hq-srv ~]#
```

Чтобы sshuser мог запускать sudo без дополнительной аутентификации, необходимо убрать комментарий с двух строчек в файле /etc/sudoers, откроем его командой:

**mcedit /etc/sudoers**

И уберём комментарий на следующей строке:

**WHEEL\_USERS ALL=(ALL:ALL) NOPASSWD: ALL**

```
## User privilege specification
## root ALL=(ALL:ALL) ALL

## Uncomment to allow members of group wheel to execute any command
#WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL
```

AUTHORS:

NECHAEV

NAUMOV После чего добавить пользователя sshuser в группу wheel:  
NAGORNOVA

**usermod -aG wheel sshuser**

```
[root@hq-srv ~]# usermod -aG wheel sshuser
[root@hq-srv ~]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=10(wheel),1010(sshuser)
[root@hq-srv ~]#
```

## Создание на BR-SRV:

Создание пользователя:

```
[root@br-srv enp0s3]# useradd sshuser -u 1010
[root@br-srv enp0s3]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=1010(sshuser)
[root@br-srv enp0s3]#
```

Редактирование пароля:

```
[root@br-srv enp0s3]# passwd sshuser
passwd: updating all authentication tokens for user sshuser.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use a password containing at least 7 characters from all of these classes, or a password containing at least 8 characters from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as your password: "cold&fort&Merger".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully.
```

Повышение прав:

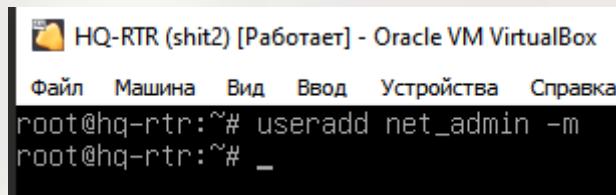
```
##  
root ALL=(ALL:ALL) ALL  
  
## Uncomment to allow members of group wheel to execute any command  
WHEEL_USERS ALL=(ALL:ALL) ALL  
  
## Same thing without a password  
WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL
```

```
[root@br-srv enp0s3]# usermod -aG wheel sshuser
[root@br-srv enp0s3]# id sshuser
uid=1010(sshuser) gid=1010(sshuser) groups=10(wheel),1010(sshuser)
[root@br-srv enp0s3]#
```

## **Создание на HQ-RTR:**

Для создания пользователя на машине под управлением ОС Astra Linux нужно использовать команду:

**useradd net\_admin -m**

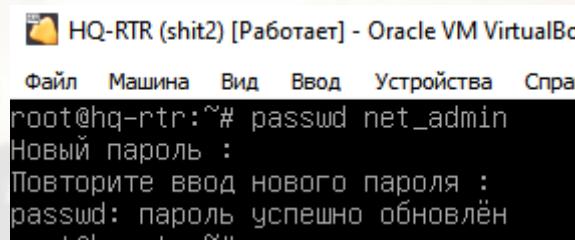


```
root@hq-rtr:~# useradd net_admin -m
root@hq-rtr:~# _
```

Изменим пароль:

**passwd net\_admin**

**P@\$\$word**



```
root@hq-rtr:~# passwd net_admin
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
```

Чтобы **net\_admin** мог запускать **sudo** без дополнительной аутентификации необходимо добавить следующую строчку в файл **/etc/sudoers**, в самый конец:

**mcedit /etc/sudoers**

**net\_admin ALL=(ALL:ALL) NOPASSWD: ALL**

```
#includedir /etc/sudoers.d
%astradmin<-->ALL=(ALL:ALL) NOPASSWD: ALL
net_admin<---->ALL=(ALL:ALL) NOPASSWD: ALL
```

**AUTHORS:**

**NECHAEV**

**NAUMOV**

**NAGORNOY** Создание пользователя:

**useradd net\_admin -m**

```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@br-rtr:~# useradd net_admin -m
root@br-rtr:~#
```

Изменение пароля:

**passwd net\_admin**

**P@\$word**

```
BR-RTR (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@br-rtr:~# passwd net_admin
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
root@br-rtr:~#
```

Повышение прав:

**mcedit /etc/sudoers**

**net\_admin ALL=(ALL:ALL) NOPASSWD: ALL**

```
#includedir /etc/sudoers.d
%astra-admin<-->ALL=(ALL:ALL) NOPASSWD: ALL
net_admin<---->ALL=(ALL:ALL) NOPASSWD: ALL
```

## **11. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV (SSH):**

**Настройка на HQ-SRV :**

Для работы SSH нам понадобится служба **openssh-common**, которой изначально нет, поэтому установим её:

**apt-get install openssh-common**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
[root@hq-srv ~]# apt-get install openssh-common
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  openssh-clients openssh-server openssh-server-control
The following packages will be upgraded:
  openssh-clients openssh-common openssh-server openssh-server-control
4 upgraded, 0 newly installed, 0 removed and 116 not upgraded.
Need to get 1164kB of archives.
After unpacking 0B of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.altlinux.org p10/branch/x86_64/classic openssh-clients 7.9p1-alt4.p10.6:p10+347647.100.1.1e1715086164 [473kB]
Get:2 http://ftp.altlinux.org p10/branch/x86_64/classic openssh-common 7.9p1-alt4.p10.6:p10+347647.100.1.1e1715086164 [290kB]
Get:3 http://ftp.altlinux.org p10/branch/noarch/classic openssh-server-control 7.9p1-alt4.p10.6:p10+347647.100.1.1e1715086164 [22.9kB]
Get:4 http://ftp.altlinux.org p10/branch/x86_64/classic openssh-server 7.9p1-alt4.p10.6:p10+347647.100.1.1e1715086164 [378kB]
Fetched 1164kB in 0s (1827kB/s)
-
```

Затем зайдём в файл конфигурации для внесения изменений:

**mcedit /etc/openssh/sshd\_config**

И внесём туда следующие строки:

**Port 2024**

**MaxAuthTries 2**

**AllowUsers sshuser**

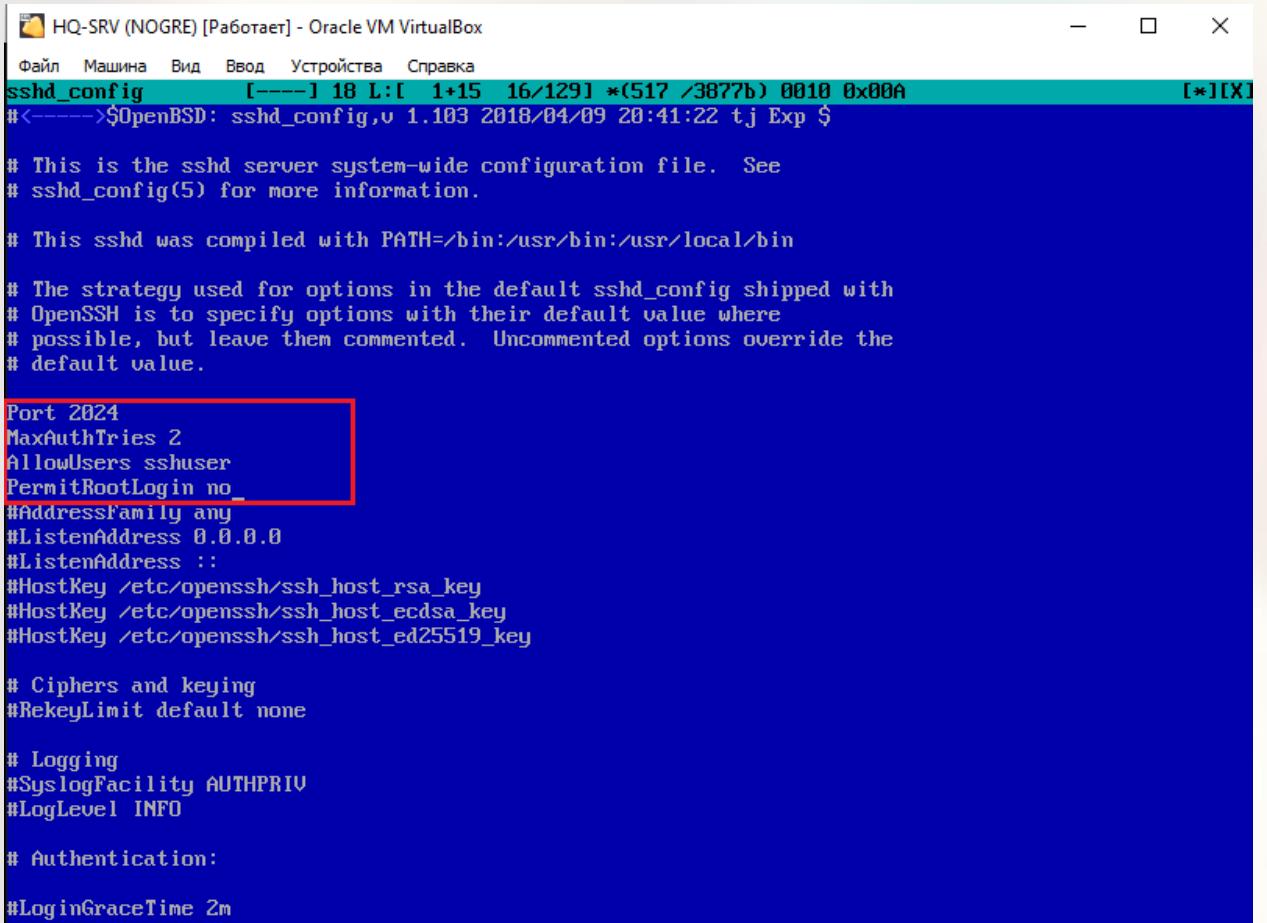
**PermitRootLogin no**

**AUTHORS:**

**NECHAEV**

**NAUMOV**

**NAGORNOVA**



```
File Machine View Input Devices Help
sshd_config [---] 18 L:[ 1+15 16/129] *(517 /3877b) 0010 0x00A
#<---->$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/usr/local/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2024
MaxAuthTries 2
AllowUsers sshuser
PermitRootLogin no_
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress :::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
```

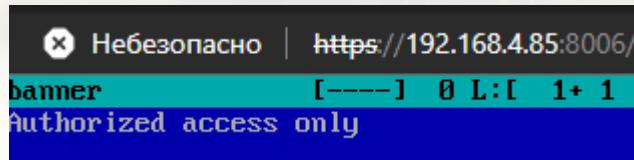
Далее нам нужен баннер.

Создаём его, вносим предложение, которое требуется по заданию через команду:

**mcedit /root/banner**

Пишем туда следующую строку (ОБЯЗАТЕЛЬНО ПОСЛЕ НЕЁ НАЖАТЬ ENTER, чтобы под ней была пустая строка):

**Authorized access only**



AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOY

Затем сохраняем и возвращаемся в /etc/ssh/sshd\_config.

Добавляем/Редактируем следующую строку:

**Banner /root/banner**

```
Файл Машина Вид Ввод Устройства Справка
sshd_config [----] 13 L: 80+27 107/1291 *(3205/
# If you just want the PAM account and session checks to
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
#UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
Banner /root/banner
```

После внесения изменений, сохраняем и выходим. И делаем перезапуск службы:

**systemctl enable --now sshd**

**systemctl restart sshd**

```
Файл Машина Вид Ввод Устройства Справка
[root@hq-srv ~]# systemctl restart sshd
[root@hq-srv ~]#
```

Затем попробуем подключиться по SSH через HQ-CLI:

**ssh sshuser@192.168.1.2 -p 2024**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
hq-cli ~ # ssh sshuser@192.168.1.2 -p 2024
Authorized access only
sshuser@192.168.1.2's password:
Last login: Thu Sep 12 15:58:07 2024 from 192.168.2.2
[sshuser@hq-srv ~]$
```

**sshuser** – пользователь, под которым вы подключаетесь

**192.168.1.2** – адрес сервера, к которому мы подключаемся (**HQ-SRV**)

**-р 2024** – порт, по которому мы подключаемся (мы заменили со стандартного 22 на 2024)

**Проделываем все тоже самое и на сервере BR-SRV.**

Сервис безопасного удаленного доступа настроен.

## МОДУЛЬ №2

### 1. Настройка доменного контроллера Samba на машине BR-SRV.

Перед настройкой самого контроллера домена удалим службу bind с нашего сервера:

**apt-get remove bind**

```
Welcome to ALT Server 10.2 (Mendelevium)!

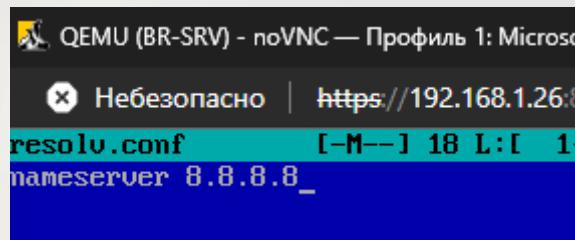
Hostname: br-srv.au-team.ipro
IP: 192.168.4.2
br-srv login: root
Password:
[root@br-srv ~]# apt-get remove bind
Reading Package Lists... Done
Building Dependency Tree... Done
The following packages will be REMOVED:
  alterator-bind alterator-net-domain bind
0 upgraded, 0 newly installed, 3 removed and 0 not upgraded.
Need to get 0B of archives.
After unpacking 2278kB disk space will be freed.
Do you want to continue? [Y/n] _
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

Переходим к настройке BR-SRV:

Проверьте, что /etc/resolv.conf хранит запись:

**nameserver 8.8.8.8**



Теперь ставим долгожданную службу samba на BR-SRV:

**apt-get update**

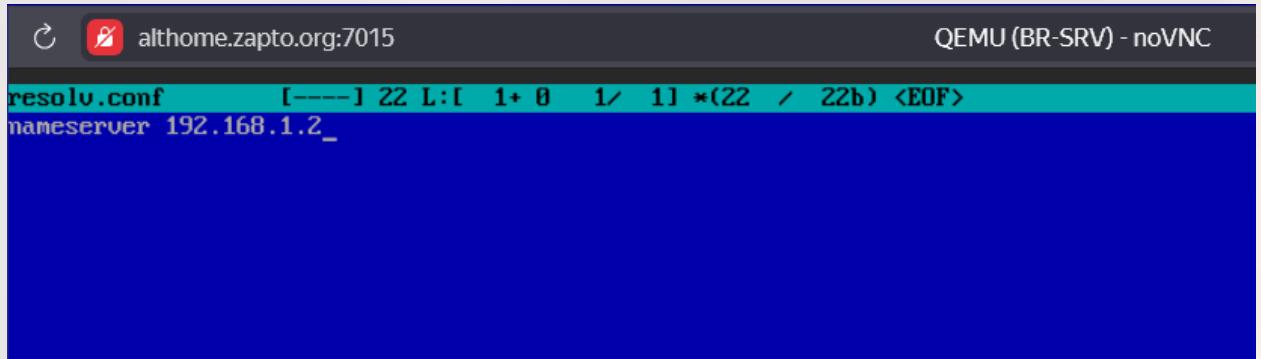
**apt-get install task-samba-dc**

```
BR-SRV (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Get:2 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Get:3 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Fetched 8732B in 0s (8794B/s)
Get:1 http://ftp.altlinux.org p10/branch/x86_64/classic pkglist [24.4MB]
Get:2 http://ftp.altlinux.org p10/branch/x86_64/classic release [137B]
Get:3 http://ftp.altlinux.org p10/branch/x86_64/gostcrypto pkglist [18.5kB]
Get:4 http://ftp.altlinux.org p10/branch/x86_64/gostcrypto release [140B]
Get:5 http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist [17.8MB]
Get:6 http://ftp.altlinux.org p10/branch/x86_64-i586/classic release [142B]
Get:7 http://ftp.altlinux.org p10/branch/noarch/classic pkglist [7275kB]
Get:8 http://ftp.altlinux.org p10/branch/noarch/classic release [137B]
Fetched 49.5MB in 13s (3697kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done
[root@br-srv ~]# apt-get install task-samba-dc
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
admx-samba ldb-tools libboost_iostreams1.76.0 libboost_system1.76.0 libboost_thread1.76.0
libcephfs2 libglusterfs8 libglusterfs8-api libibverbs libldb libldb-modules-ldap liblttng-ust
librados2 librbdmacm libsmclient libwbclient lmdb-utils perl-Parse-Yapp python3-module-pyldb
python3-module-samba samba-client samba-common samba-common-client samba-common-libs
samba-common-tools samba-dc samba-dc-client samba-dc-common samba-dc-libs samba-dcerpc samba-doc
samba-libs samba-pidl samba-winbind samba-winbind-clients samba-winbind-common tdb-utils
The following packages will be upgraded:
libldb libldb-modules-ldap libsmclient libwbclient python3-module-pyldb python3-module-samba
samba-client samba-common-client samba-common-libs samba-dc-libs samba-libs
The following NEW packages will be installed:
admx-samba ldb-tools libboost_iostreams1.76.0 libboost_system1.76.0 libboost_thread1.76.0
libcephfs2 libglusterfs8 libglusterfs8-api libibverbs liblttng-ust librados2 librbdmacm
lmdb-utils perl-Parse-Yapp samba-common samba-common-tools samba-dc samba-dc-client
samba-dc-common samba-dcerpc samba-doc samba-pidl samba-winbind samba-winbind-clients
samba-winbind-common task-samba-dc tdb-utils
11 upgraded, 27 newly installed, 0 removed and 272 not upgraded.
Need to get 33.5MB of archives.
After unpacking 122MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Приводим /etc/resolv.conf к следующему виду:

**nameserver 192.168.1.2**

Это нужно сделать обязательно, т.к. при установке **Samba** как доменного контроллера, будет ещё использоваться DNS-сервер. А у нас уже есть DNS-сервер, и это – **HQ-SRV** (весь это его адрес), вот он и будет использоваться для разрешения доменных имен.



Теперь удалим конфиг smb.conf, чтобы он не мешал при настройке службы:

```
rm -rf /etc/samba/smb.conf
```

```
[root@br-srv ~]# rm -rf /etc/samba/smb.conf
[root@br-srv ~]# _
```

Проверяем, что установлено полное доменное имя у **BR-SRV**:

```
hostname -f
```

```
BR-SRV (1mod) [Работает] - Oracle VM \
Файл  Машина  Вид  Ввод  Устройст
[root@br-srv ~]# hostname -f
br-srv.au-team.irpo
[root@br-srv ~]# _
```

Если запись не соответствует рисунку выше, то нужно его настроить:

```
hostnamectl set-hostname br-srv.au-team.irpo; exec bash
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

Настроим **hosts**, добавив новую запись в конец файла:

**mcedit /etc/hosts**

**192.168.4.2 br-srv.au-team.irpo**

```
BR-SRV (1mod) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
hosts [-M--] 35 L:[ 1+ 2 3/ 31
127.0.0.1<---->localhost.localdomain localhost
::1<---->localhost6.localdomain localhost6
192.168.4.2<---->br-srv.au-team.irpo
```

Теперь в конфигурацию нашего DNS-сервера на **HQ-SRV** добавим следующую строку:

**server=/au-team.irpo/192.168.4.2**

```
HQ-SRV (disksmry) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
dnsmasq.conf [----] 32 L:[ 1+ 2
no-resolv
domain=au-team.irpo
server=/au-team.irpo/192.168.4.2
server=8.8.8.8
interface=*
```

Перезапускаем **dnsmasq** как службу:

**systemctl restart dnsmasq**

А теперь запускаем автонастройку доменного контроллера на **BR-SRV**. Если предложенные значения верны, те, что находятся в [], то нажимаем Enter, если нет, то нужно проверять предыдущие настройки.

**samba-tool domain provision**

**AU-TEAM.IRPO**

**AU-TEAM**

**dc**

**AUTHORS:**

**NECHAEV SAMBA\_INTERNAL  
NAUMOV**

**192.168.1.2** (Здесь вводим значение вручную)

**123qweR%**

```
[root@br-srv ~]# samba-tool domain provision
Realm [AU-TEAM.IRPO]:
Domain [AU-TEAM]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]: 192.168.1.2
Administrator password:
```

После настройки должно появится такое в терминале, это значит, что всё настроено верно:

```
Applied Forest Update 140: a0a45aac-5550-42df-bb6a-3cc5c46b52f2
Applied Forest Update 141: 3e7645f3-3ea5-4567-b35a-87630449c70c
Applied Forest Update 142: e634067b-e2c4-4d79-b6e8-73c619324d5e
Skip Domain Update 75: 5e1574f6-55df-493e-a671-aaeffca6a100
Skip Domain Update 76: d262aae8-41f7-48ed-9f35-56bbb677573d
Skip Domain Update 77: 82112ba0-7e4c-4a44-89d9-d46c9612bf91
Applied Domain Update 78: c3c927a6-cc1d-47c0-966b-be8f9b63d991
Applied Domain Update 79: 54afc9b9-637a-4251-9f47-4d50e7021211
Applied Domain Update 80: f4728883-84dd-483c-9897-274f2ebcf11e
Applied Domain Update 81: ff4f9d27-7157-4cb0-80a9-5d6f2b14c8ff
Applied Domain Update 82: 83c53da7-427e-47a4-a07a-a324598b88f7
Applied Domain Update 83: c81fc9cc-0130-4fd1-b272-634d74818133
Applied Domain Update 84: e5f9e791-d96d-4fc9-93c9-d53e1dc439ba
Applied Domain Update 85: e6d5fd00-385d-4e65-b02d-9da3493ed850
Applied Domain Update 86: 3a6b3fbf-3168-4312-a10d-dd5b3393952d
Applied Domain Update 87: 7f950403-0ab3-47f9-9730-5d7b0269f9bd
Applied Domain Update 88: 434bb40d-dbc9-4fe7-81d4-d57229f7b080
Applied Domain Update 89: a0c238ba-9e30-4ee6-80a6-43f731e9a5cd
INFO 2024-10-25 12:01:29,371 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #24
32: A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
INFO 2024-10-25 12:01:29,372 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #24
34: Merge the contents of this file with your system krb5.conf or replace it with this one. Do not create a symlink!
INFO 2024-10-25 12:01:29,428 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #49
3: Once the above files are installed, your Samba AD server will be ready to use
INFO 2024-10-25 12:01:29,428 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #49
8: Server Role: active directory domain controller
INFO 2024-10-25 12:01:29,429 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #49
9: Hostname: br-srv
INFO 2024-10-25 12:01:29,429 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #50
0: NetBIOS Domain: AU-TEAM
INFO 2024-10-25 12:01:29,430 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #50
1: DNS Domain: au-team.irpo
INFO 2024-10-25 12:01:29,431 pid:27999 /usr/lib64/samba/dc/python3.9/samba/provision/_init__.py #50
2: DOMAIN SID: S-1-5-21-850490868-450961147-962401282
[root@br-srv ~]#
```

Перемещаем сгенерированный конфиг krb5.conf и включаем службу samba:

```
mv -f /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

```
systemctl enable samba
```

```
AUTHORS: NECHAEV NAUMOV NAGORNOV
[root@br-srv ~]# mv -f /var/lib/samba/private/krb5.conf /etc/krb5.conf
[root@br-srv ~]# systemctl enable samba
Synchronizing state of samba.service with SysV service script with /lib/systemd/systemd-sysv-install...
Executing: /lib/systemd/systemd-sysv-install enable samba
Created symlink /etc/systemd/system/multi-user.target.wants/samba.service → /lib/systemd/system/samba.service.
[root@br-srv ~]# _
```

Из-за того, что на Alt Linux могут пропадать IP-адреса после перезагрузки системы, добавим запись о перезапуске службы **network** и **samba** в **crontab** (именно в таком порядке), пишем в консоль:

```
export EDITOR=mcedit
```

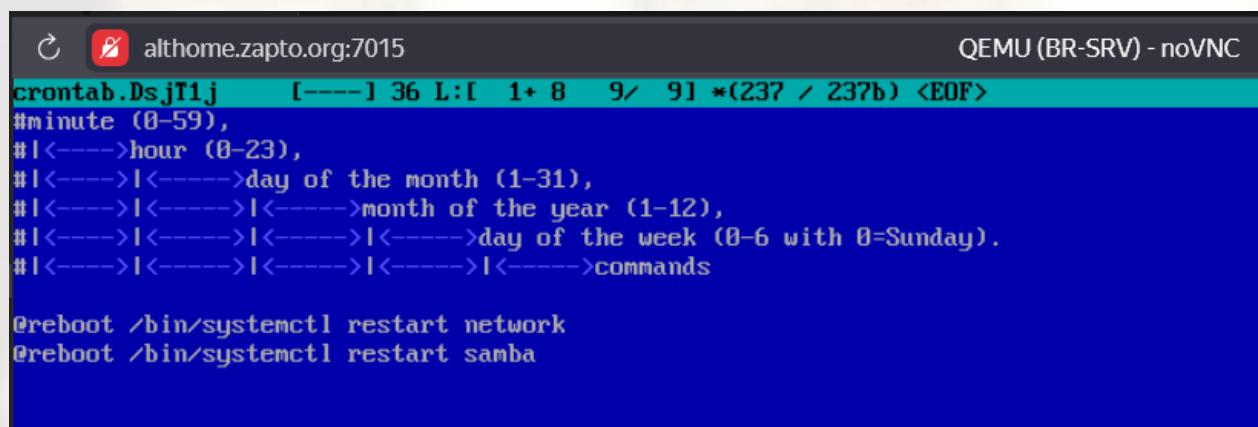
```
crontab -e
```

И вносим в конец файла следующие строки:

```
@reboot /bin/systemctl restart network
```

```
@reboot /bin/systemctl restart samba
```

**!ВАЖНО!** Оставляем ещё одну пустую строку снизу, иначе файл не станет сохраняться!



```
crontab.DsjT1j [----] 36 L:[ 1+ 8 9/ 9] *(237 / 237b) <EOF>
#minute (0-59),
#|<---->hour (0-23),
#|<---->|<---->day of the month (1-31),
#|<---->|<---->|<---->month of the year (1-12),
#|<---->|<---->|<---->|<---->day of the week (0-6 with 0=Sunday).
#|<---->|<---->|<---->|<---->|<---->commands

@reboot /bin/systemctl restart network
@reboot /bin/systemctl restart samba
```

Теперь ПЕРЕЗАПУСКАЕМ машину BR-SRV:

```
reboot
```

```
[root@br-srv ~]# reboot_
```

Проверяем работу домена:

```
samba-tool domain info 127.0.0.1
```

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
Welcome to ALT Server 10.2 (Mendelevium)!

Hostname: br-srv.au-team.irpo
IP: 192.168.4.2
br-srv login: root
Password:
Last login: Fri Oct 25 11:25:00 +07 2024 on tty2
[root@br-srv ~]# samba-tool domain info 127.0.0.1
Forest          : au-team.irpo
Domain         : au-team.irpo
Netbios domain : AU-TEAM
DC name        : br-srv.au-team.irpo
DC netbios name: BR-SRV
Server site    : Default-First-Site-Name
Client site   : Default-First-Site-Name
[root@br-srv ~]# -
```

Домен работает, у вас должно всё соответствовать картинке выше.

Теперь создадим 5 пользователей:

**samba-tool user add user1.hq 123qweR%**

**samba-tool user add user2.hq 123qweR%**

**samba-tool user add user3.hq 123qweR%**

**samba-tool user add user4.hq 123qweR%**

**samba-tool user add user5.hq 123qweR%**

```
[root@br-srv ~]# samba-tool user add user1.hq 123qweR%
User 'user1.hq' added successfully
[root@br-srv ~]# samba-tool user add user2.hq 123qweR%
^[[AUser 'user2.hq' added successfully
[root@br-srv ~]# samba-tool user add user3.hq 123qweR%
User 'user3.hq' added successfully
[root@br-srv ~]# samba-tool user add user4.hq 123qweR%
User 'user4.hq' added successfully
[root@br-srv ~]# samba-tool user add user5.hq 123qweR%
User 'user5.hq' added successfully
[root@br-srv ~]# -
```

AUTHORS:

NECHAEV

NAUMOV

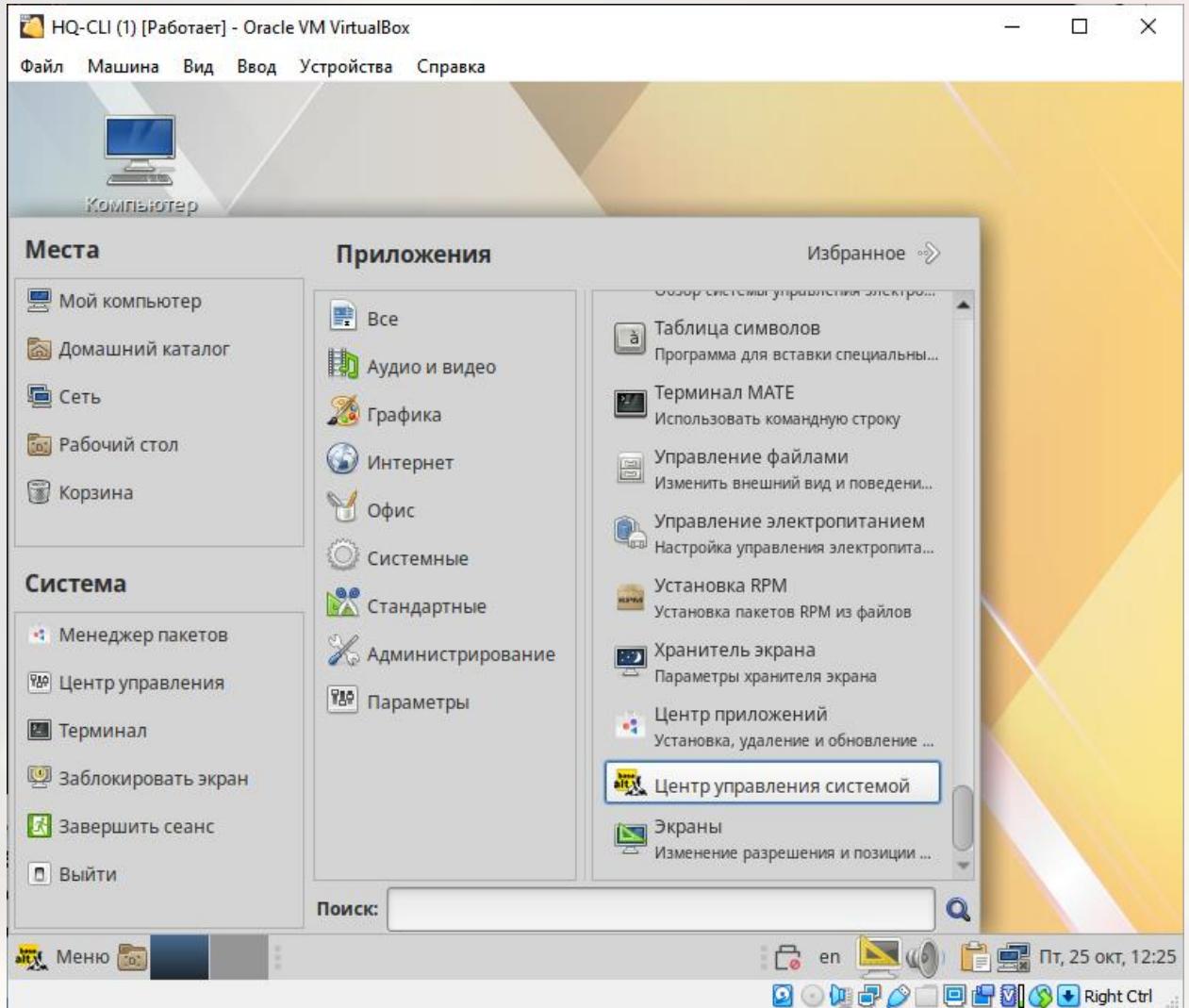
NAGORNOVA

**samba-tool group add hq**

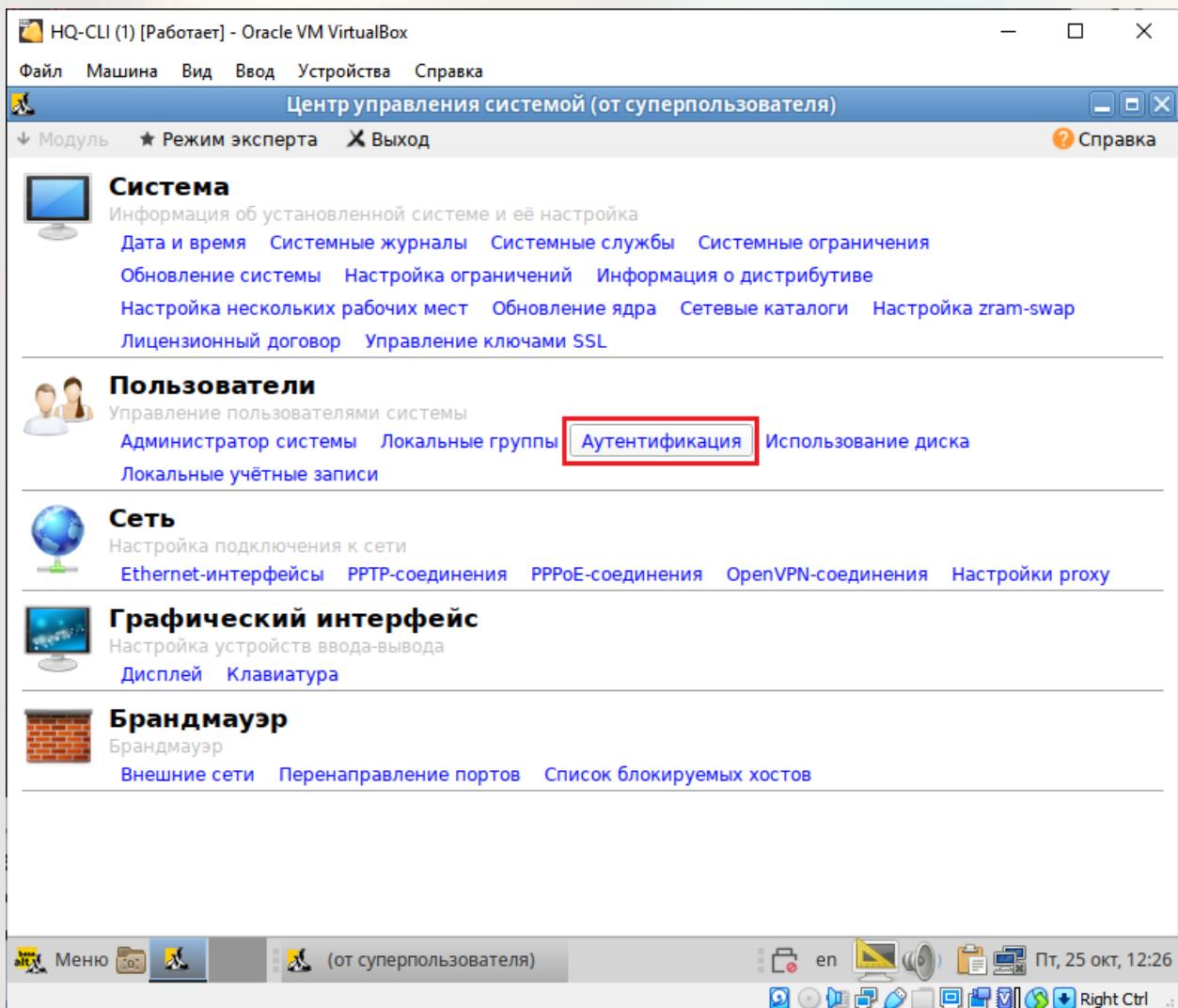
**samba-tool group addmembers hq user1.hq,user2.hq,user3.hq,user4.hq,user5.hq**

```
[root@br-srv ~]# samba-tool group add hq
Added group hq
[root@br-srv ~]# samba-tool group addmembers hq user1.hq,user2.hq,user3.hq,user4.hq,user5.hq
Added members to group hq
[root@br-srv ~]#
```

Теперь введём клиентскую машину в домен:

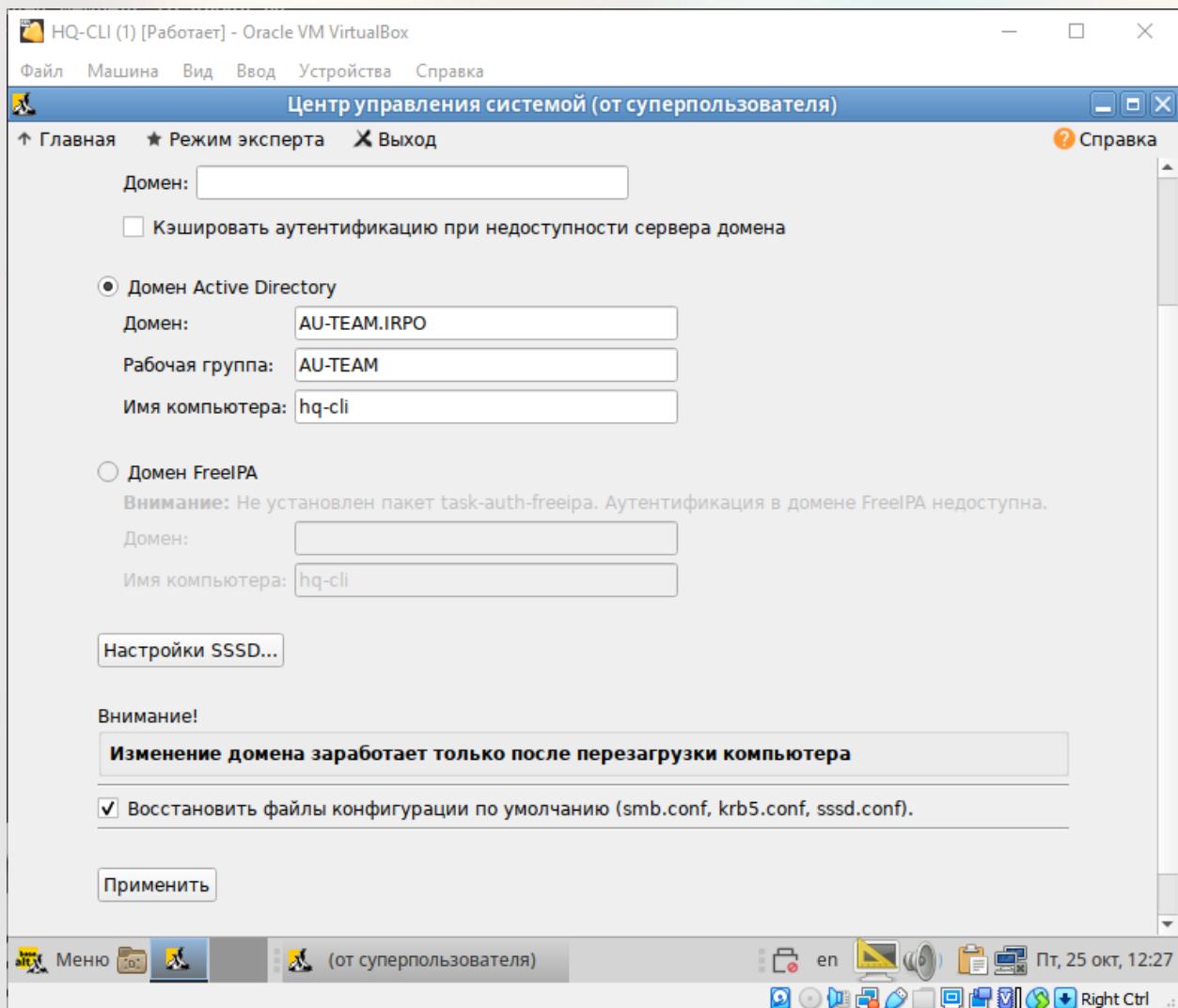


AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



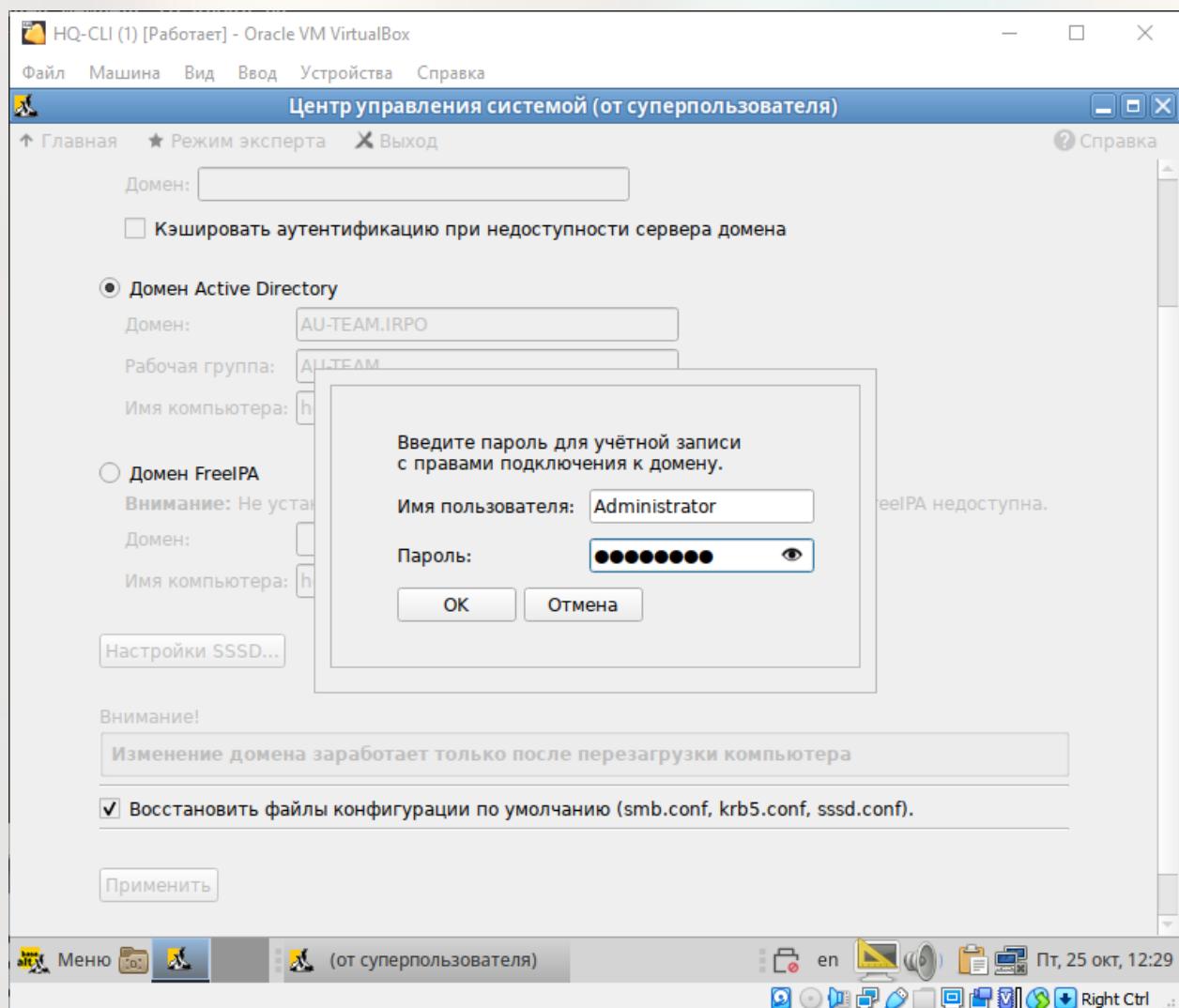
Заполняем так, как показано на скриншоте ниже:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



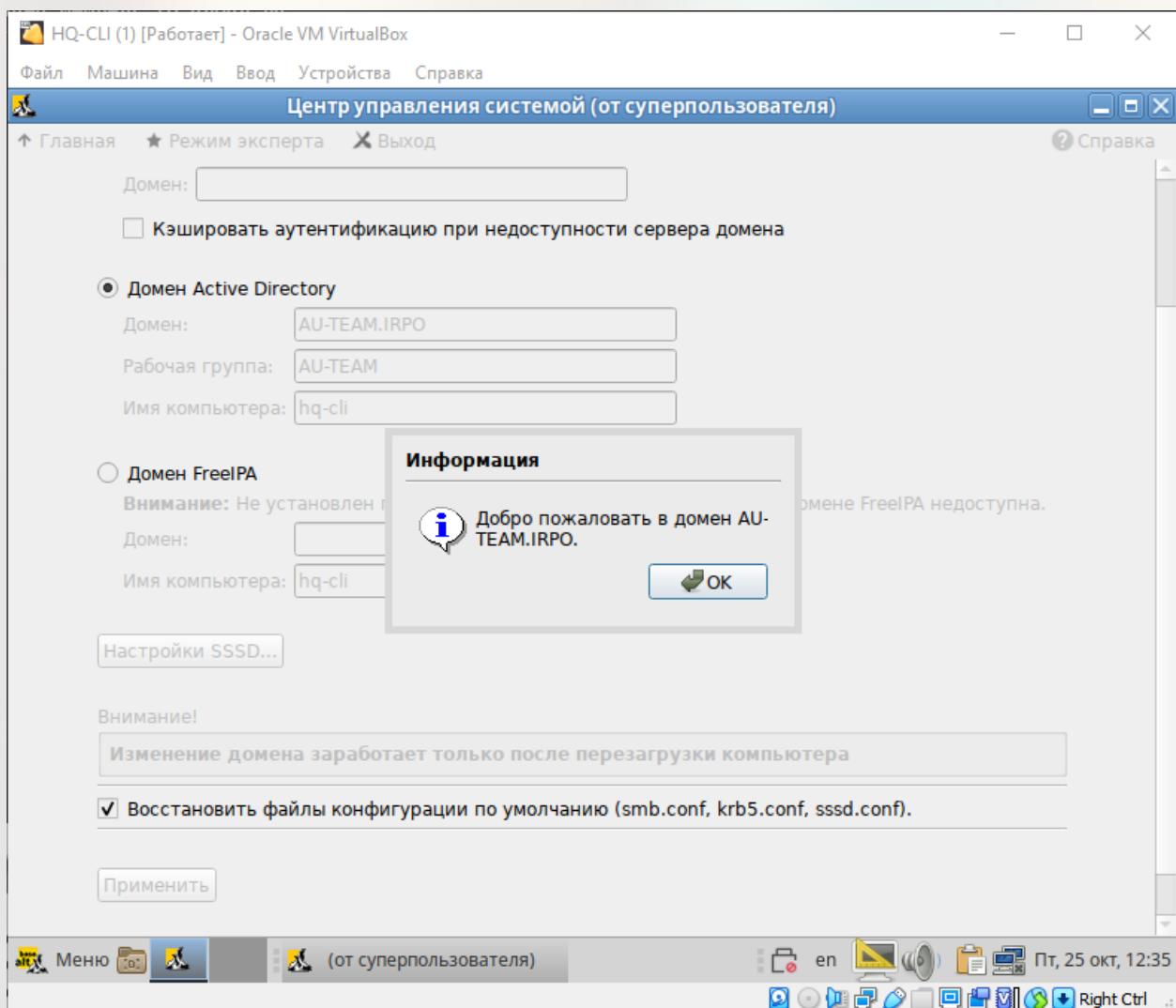
Вводим пароль, который вводили при настройке домена через samba-tool:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



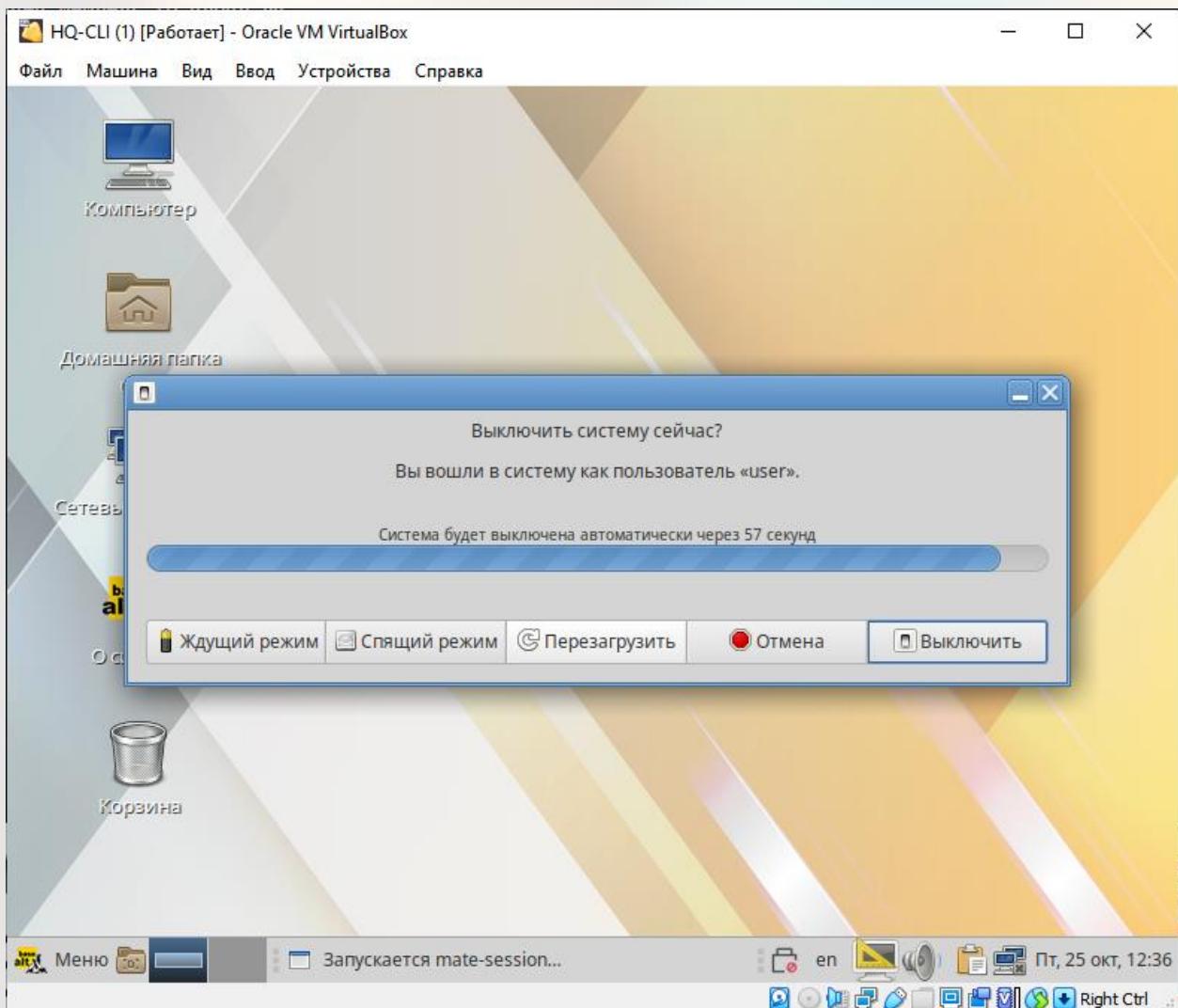
После ввода в домен должно появиться следующее сообщение на экране:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



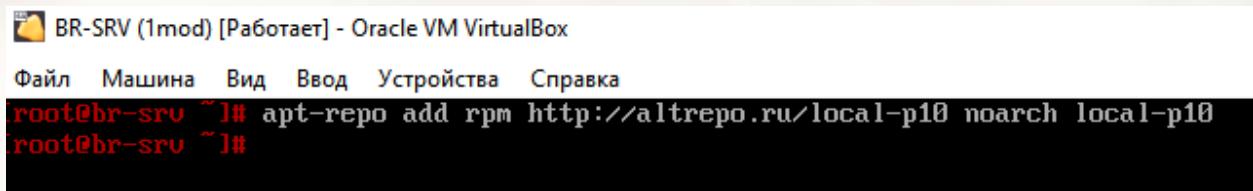
Перезагружаем машину **HQ-CLI**:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Чтобы настроить права созданных нами пользователей, нужно установить ещё один пакет на **BR-SRV**, но перед этим нужно подключить нужный репозиторий следующей командой:

```
apt-repo add rpm http://altrepo.ru/local-p10 noarch local-p10
```



Теперь обновляем список пакетов:

AUTHORS:

NECHAEV

NAUMOV

NAGORNOY

И можем устанавливать нужный нам пакет:

```
apt-get install sudo-samba-schema
```

BR-SRV (1mod) [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
[root@br-srv ~]# apt-repo add rpm http://altrepo.ru/local-p10 noarch local-p10
[root@br-srv ~]# apt-get update
Get:1 http://ftp.altlinux.org p10/branch/x86_64 release [4223B]
Get:2 http://altrepo.ru noarch release [1094B]
Get:3 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Get:4 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Fetched 9826B in 0s (45.7kB/s)
Hit http://ftp.altlinux.org p10/branch/x86_64/classic pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64/classic release
Hit http://ftp.altlinux.org p10/branch/x86_64/gostcrypto pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64/gostcrypto release
Hit http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64-i586/classic release
Hit http://ftp.altlinux.org p10/branch/noarch/classic pkglist
Hit http://ftp.altlinux.org p10/branch/noarch/classic release
Get:1 http://altrepo.ru noarch/local-p10 pkglist [87.6kB]
Get:2 http://altrepo.ru noarch/local-p10 release [128B]
Fetched 87.7kB in 0s (294kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done
[root@br-srv ~]# apt-get install sudo-samba-schema
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  dialog libdialog
The following NEW packages will be installed:
  dialog libdialog sudo-samba-schema
0 upgraded, 3 newly installed, 0 removed and 272 not upgraded.
Need to get 249kB of archives.
After unpacking 703kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

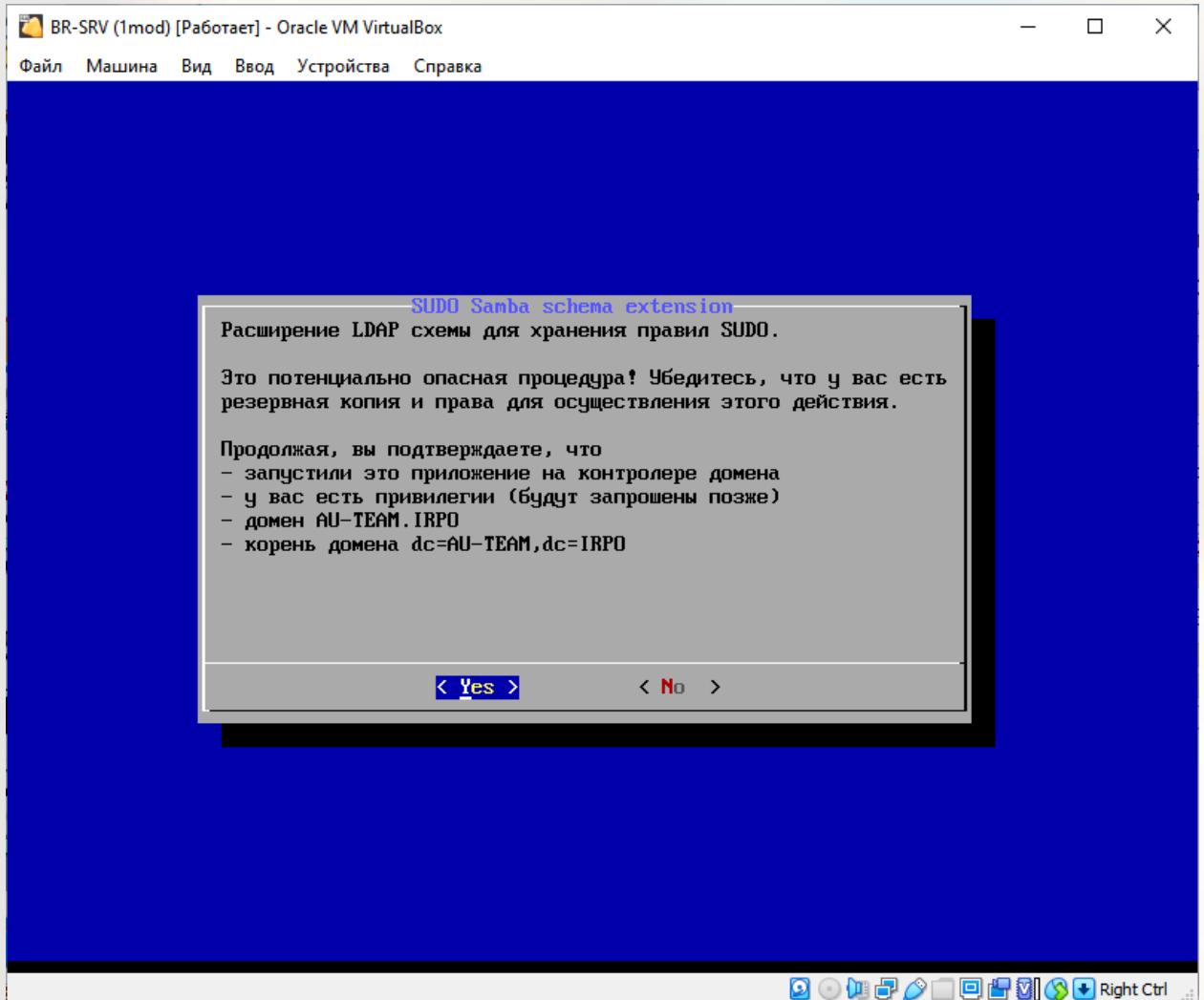
Далее добавляем новую схему следующей командой:

**sudo-schema-apply**

```
[root@br-srv ~]# sudo-schema-apply
```

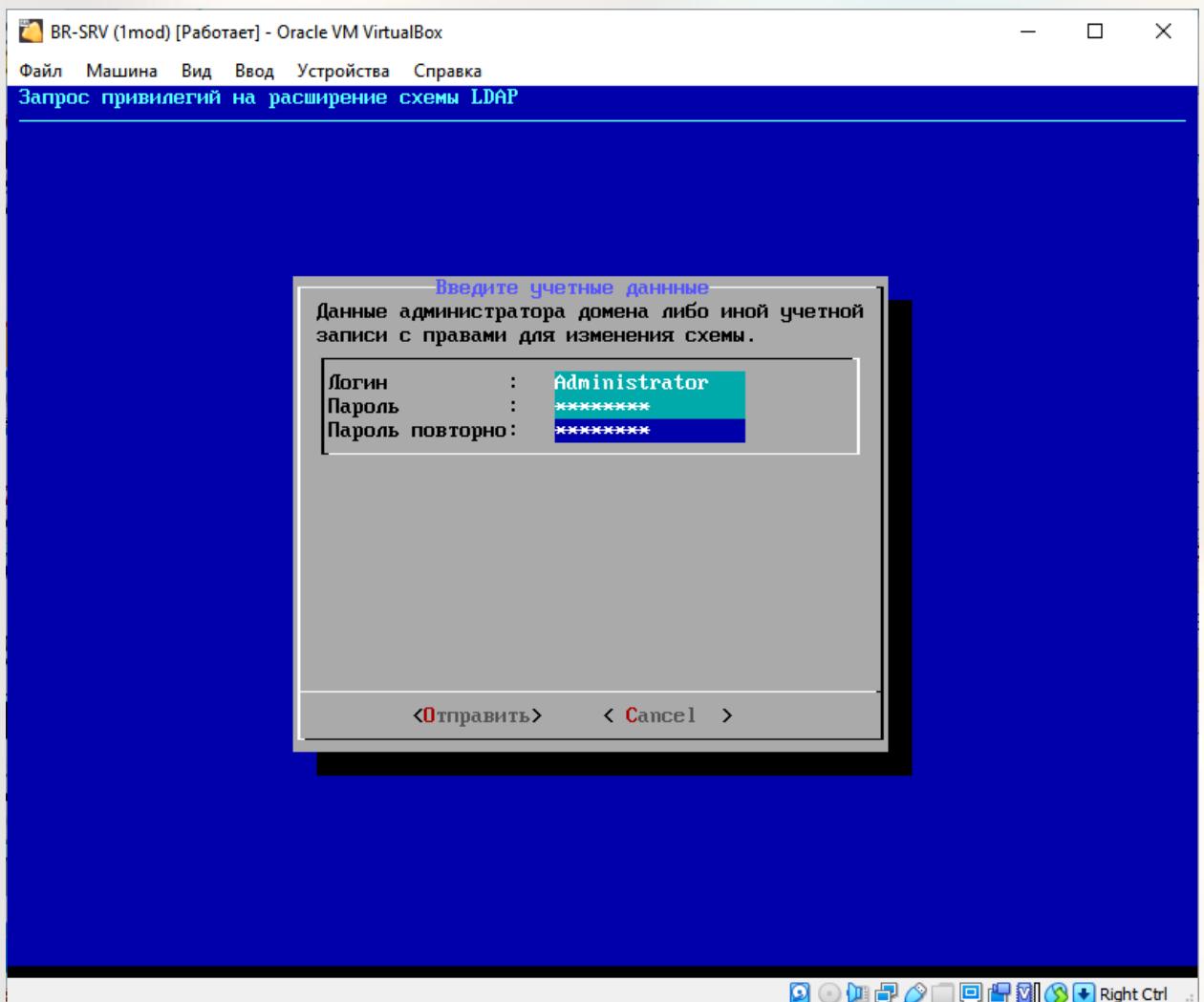
Откроется следующее диалоговое окно, нажимаем yes:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



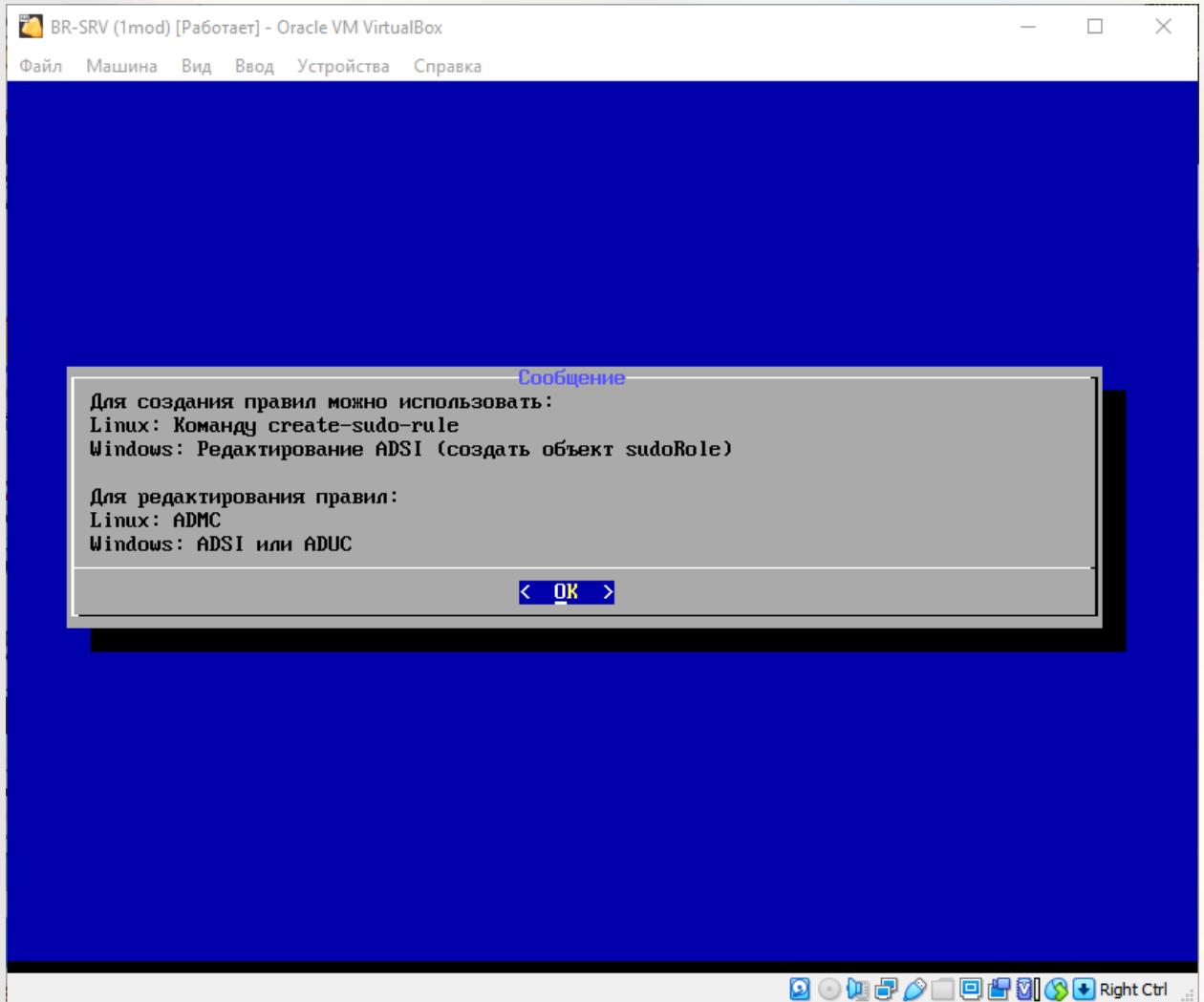
Затем у нас попросит пароль от доменного администратора:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



После этого должно появиться такое окно:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Далее мы создаём новое правило следующей командой (которую он сам предлагает в этом окне):

### **create-sudo-rule**

И вносим следующие изменения (имя правила можно любое):

Имя правила : **prava\_hq**

sudoCommand : **/bin/cat**

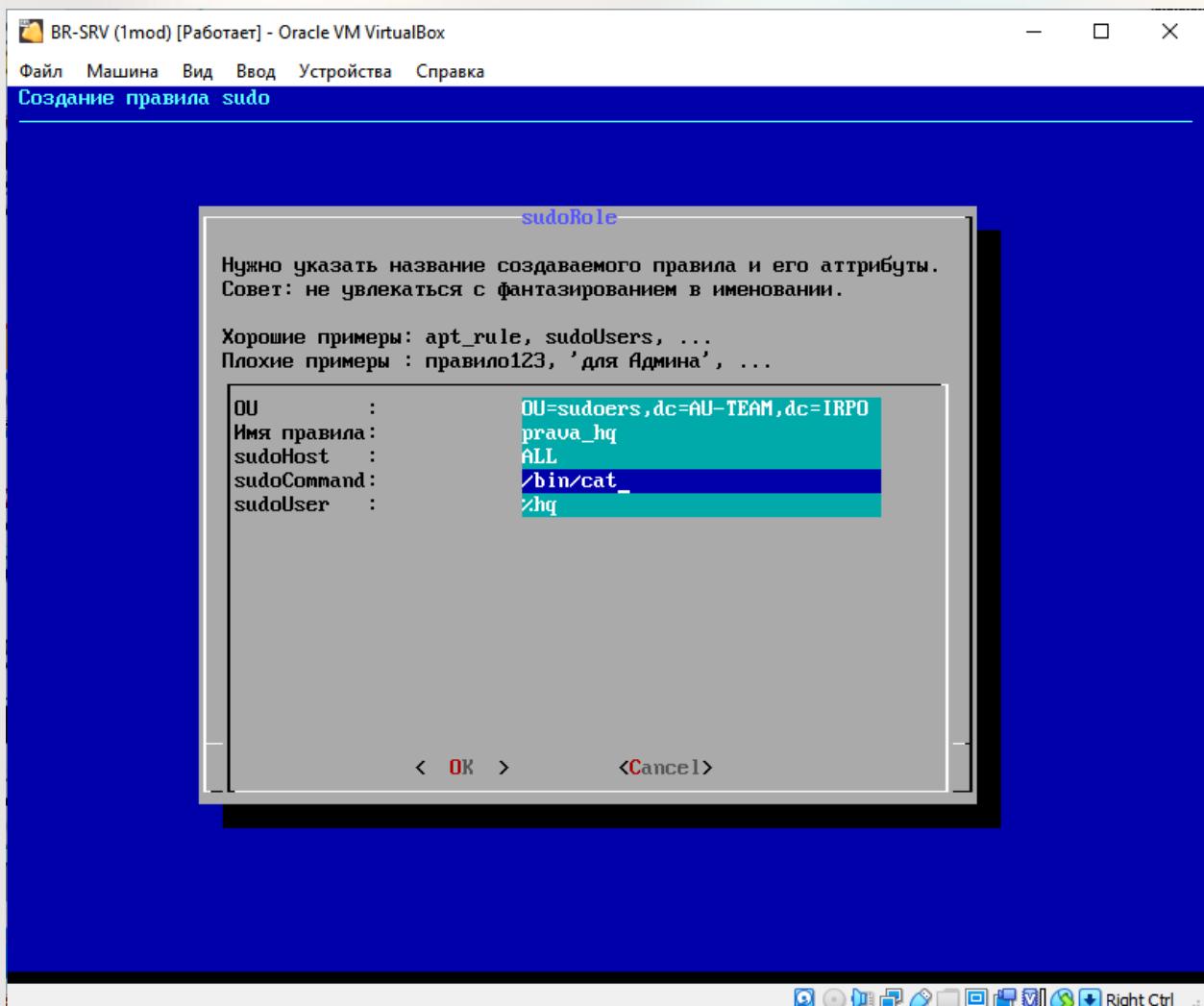
sudoUser : **%hq**

**AUTHORS:**

NECHAEV

NAUMOV

NAGORNOVA

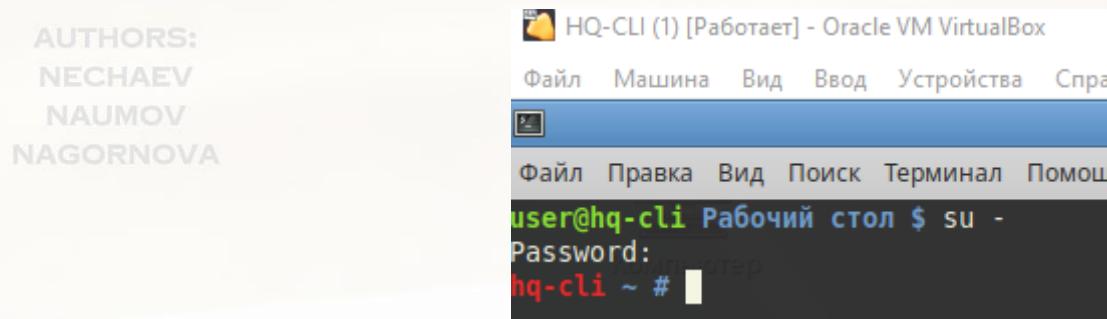


При успешном добавлении выведет следующие строки:

```
Added 1 records successfully
Modified CN=prava_hq,OU=sudoers,dc=AU-TEAM,dc=IRPO
Modified 1 records successfully
Операция прошла успешно
[root@br-srv ~]#
```

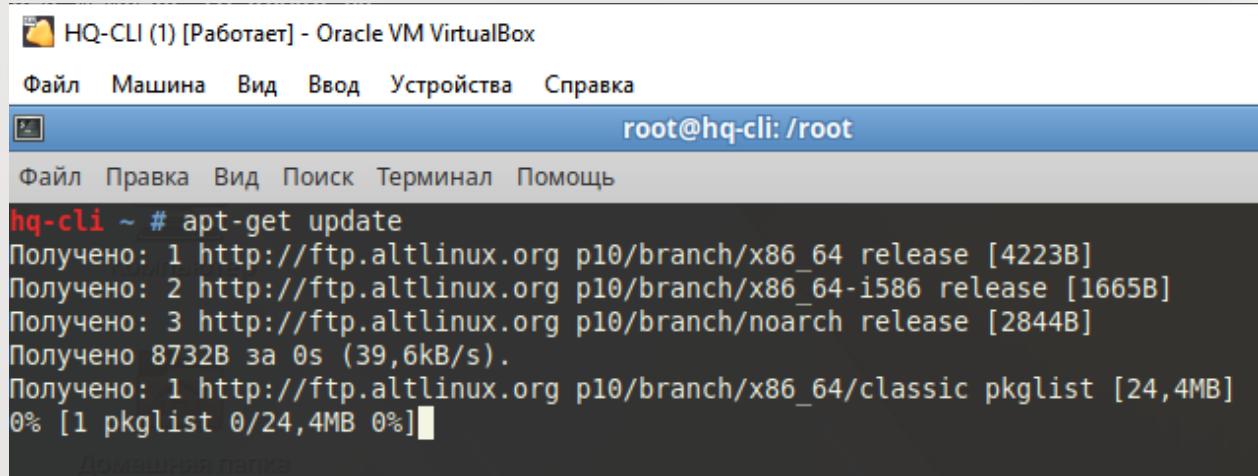
Заходим под локальным пользователем на клиентской машине **HQ-CLI** и получаем права root:

**sudo su**



Обновляем список пакетов:

**apt-get update**



```
hq-cli ~ # apt-get update
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64 release [4223B]
Получено: 2 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Получено: 3 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Получено 8732B за 0s (39,6kB/s).
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64/classic pkglist [24,4MB]
0% [1 pkglist 0/24,4MB 0%]
```

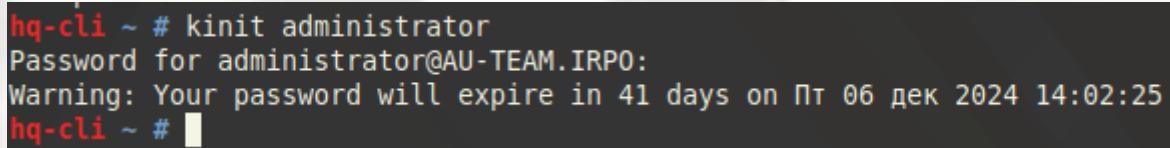
И поставим пакет admc:

**apt-get install admc**

Затем создаём тикет доменного администратора, чтобы получить права на редактирование правил на сервере:

**kinit administrator**

**123qweR%**

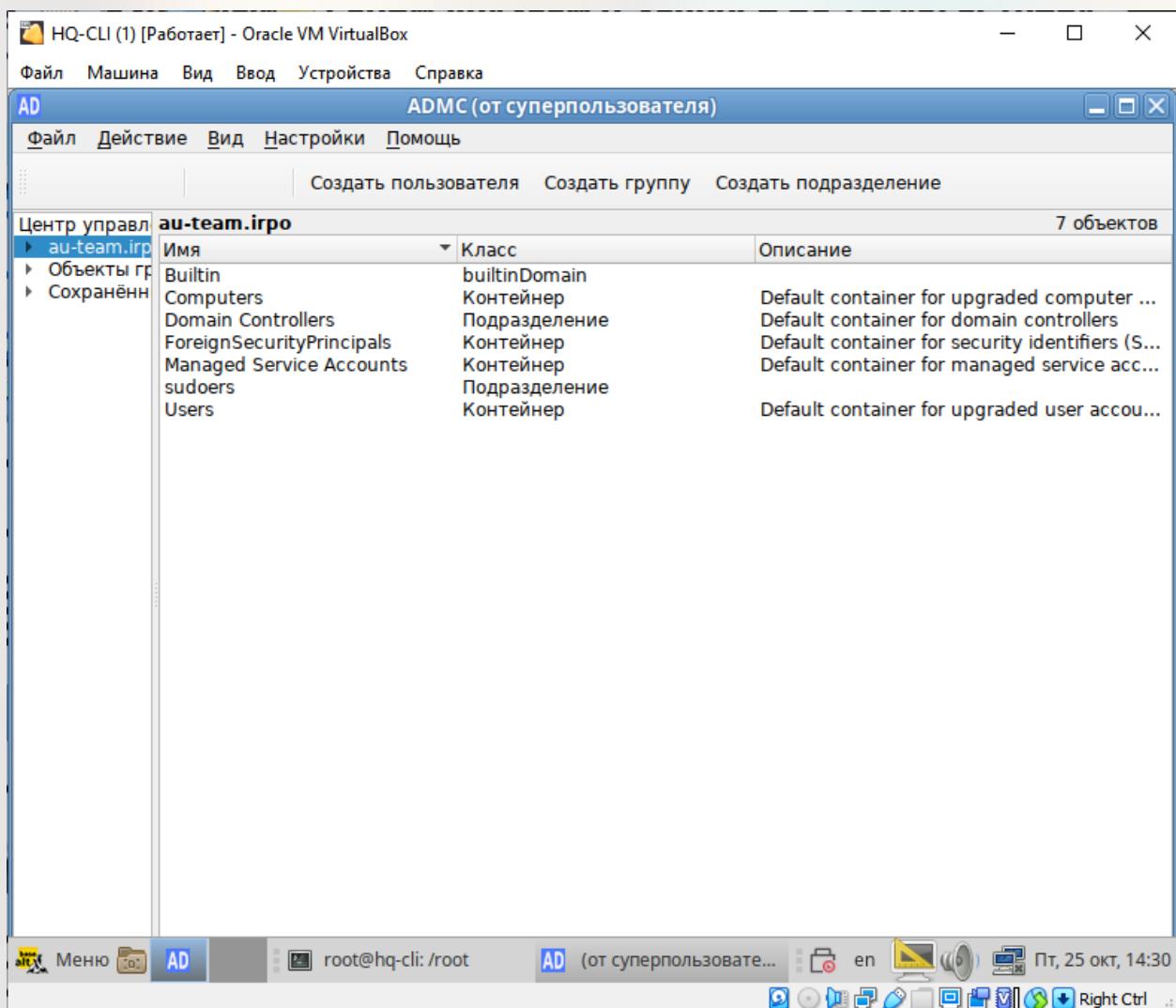


```
hq-cli ~ # kinit administrator
Password for administrator@AU-TEAM.IRPO:
Warning: Your password will expire in 41 days on Пт 06 дек 2024 14:02:25
hq-cli ~ #
```

И запускаем admc:

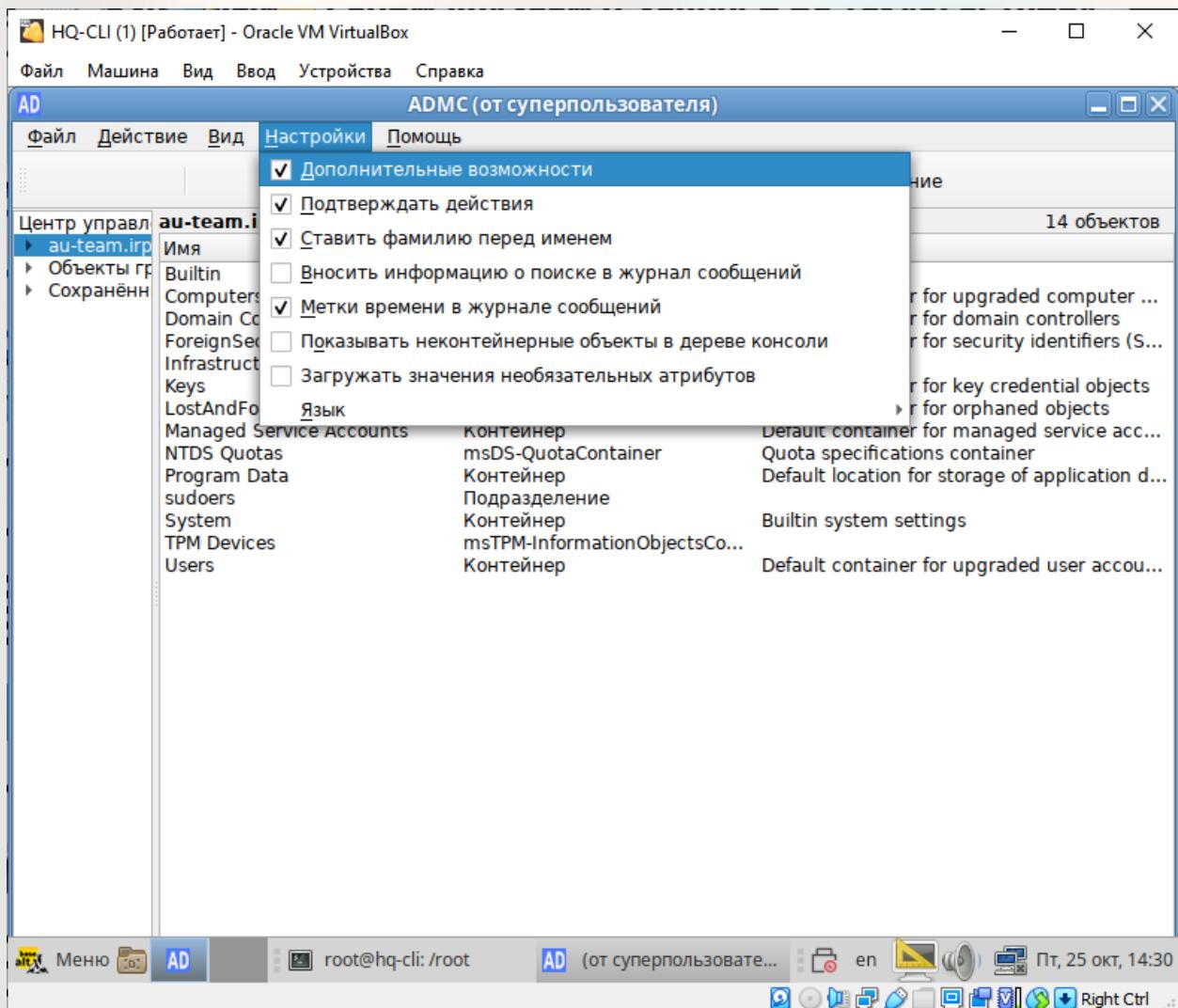
**admc**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



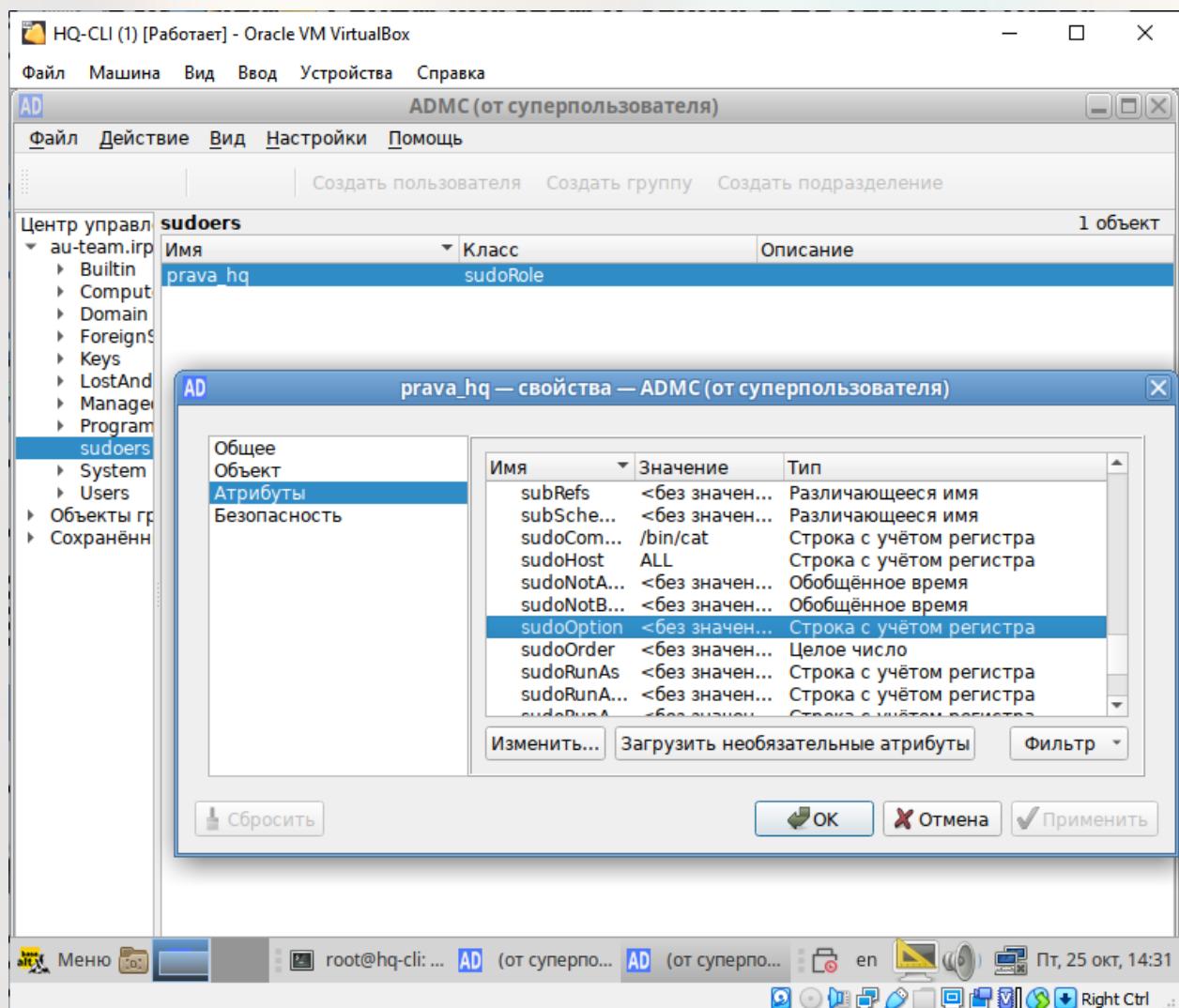
Включим дополнительные возможности через настройки:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Поменяем опцию **sudoOption** в созданном нами ранее правиле **prava\_hq** (правило всегда будет находиться в OU с названием **sudoers**):

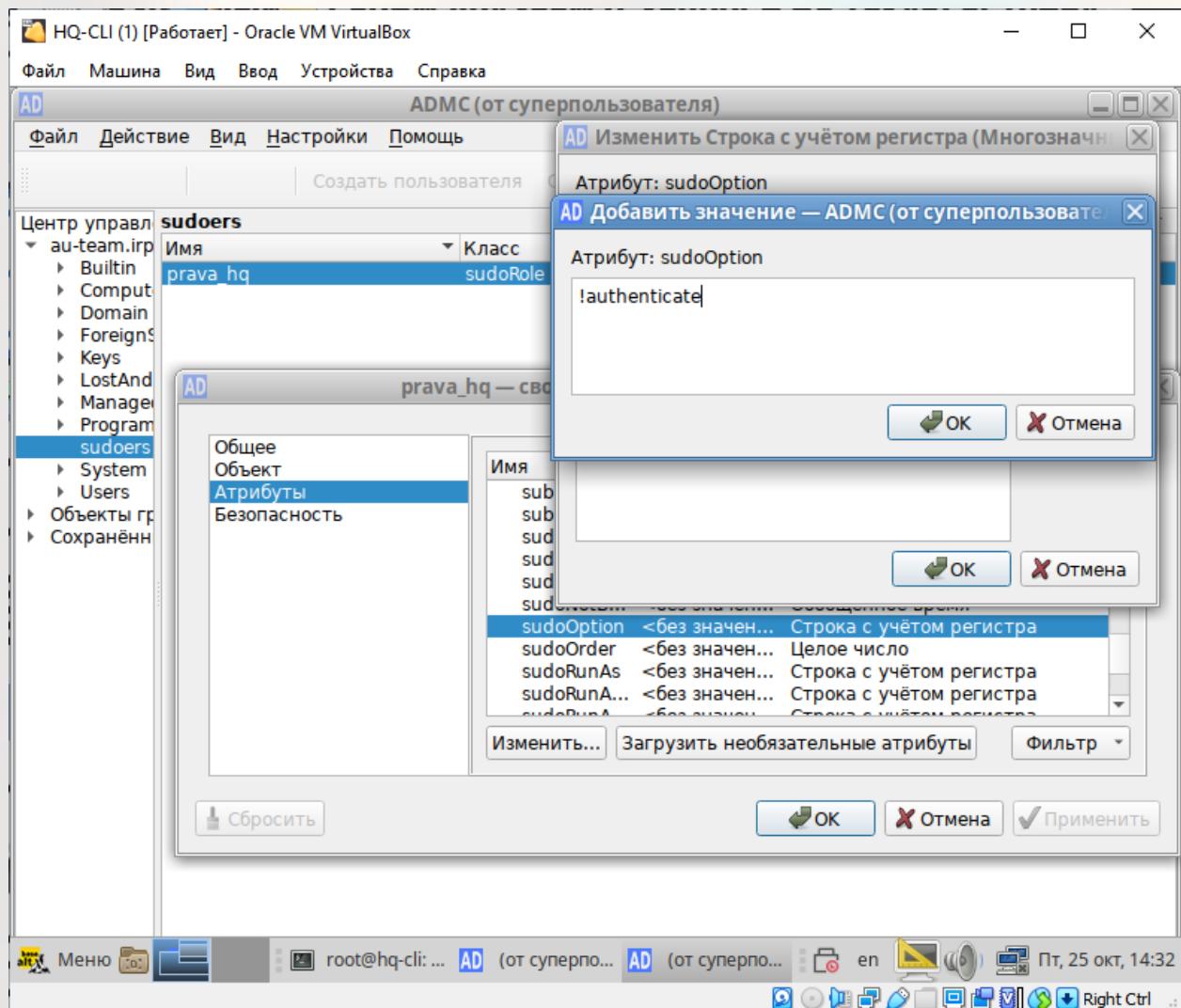
AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Новое значение будет:

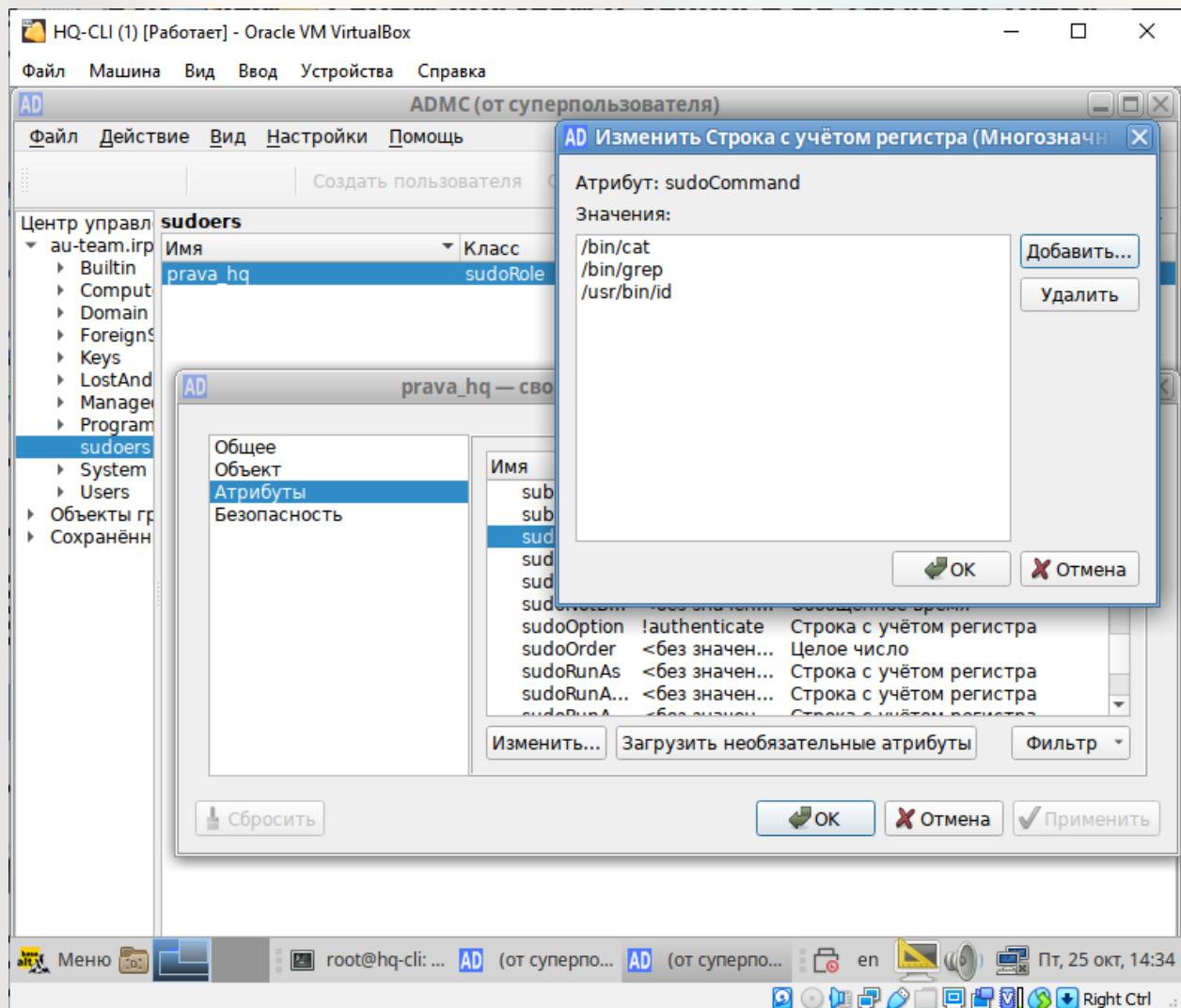
**!authenticate**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



И добавим ещё две команды в опцию **sudoCommand** (**grep** и **id**):

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



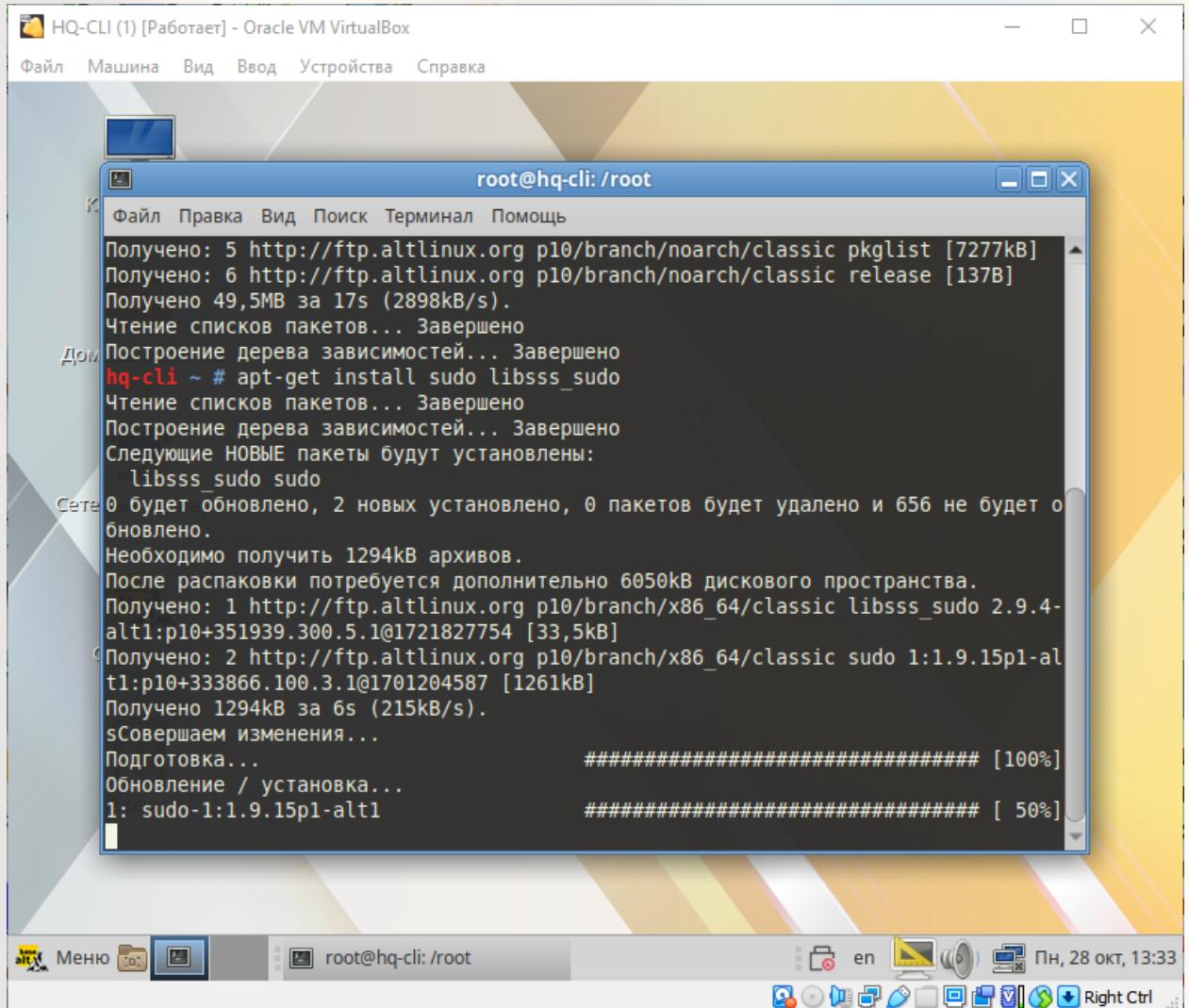
Обратите внимание, что путь до **id** отличается от других команд!

Теперь, чтобы работали все созданные нами правила, нужно зайти на **HQ-CLI** и установить дополнительные пакеты:

**apt-get update**

**apt-get install sudo libsss\_sudo**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Разрешаем использование sudo:

**control sudo public**

```
Завершено.
hq-cli ~ # control sudo public
hq-cli ~ #
```

Настроим конфиг **sssd.conf**:

**mcedit /etc/sssd/sssd.conf**

**services = nss, pam, sudo**

**sudo\_provider = ad**

AUTHORS  
NECHAEV  
NAUMOV  
NAGORNOVA

```
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
sssd.conf [-M--] 18 L:[ 1+16 17/ 28 ] *(327 / 605b) 0010 0x00A [*][X]
[sssd]
config_file_version = 2
services = nss, pam, sudo

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = _sssd

# SSSD will not start if you do not configure any domains.

domains = AU-TEAM.IRPO
[nss]

[pam]
[domain/AU-TEAM.IRPO]
id_provider = ad
sudo_provider = ad
autn_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
; cache_credentials = false
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true

1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Переить 7Поиск 8Удалить 9МенюМС 10Выход
Меню root@hq-cli: /root Пн, 28 окт, 13:35 Right Ctrl
```

Теперь отредактируем **nsswitch.conf**:

**mcedit /etc/nsswitch.conf**

**sudoers: files sss**

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
root@hq-cli: /root
File Edit View Insert Devices Help
File Edit View Search Terminal Help
nsswitch.conf [---] 18 L:[ 6+23 29/ 62 ] *(1026/1899b) 0010 0x00A [*][X]
#
# Specifying '[NOTFOUND=return]' means that the search for an entry
# should stop if the search with the previous service turned up nothing.
# Note that if the search failed due to some other reason (like no NIS
# server responding) then the search continues with the next service.
#
# Legal name services are:
#
#<---->files<-><---->Use local files
#<---->tcb<-><---->Use local tcb shadow files, see tcb(5)
#<---->db<-><---->Use local database files under /var/db
#<---->nis or yp<-><---->Use NIS (NIS version 2), also called YP
#<---->nisplus or nis+<-><---->Use NIS+ (NIS version 3)
#<---->dns<-><---->Use DNS (Domain Name Service)
#<---->compat<-><---->Use NIS in compatibility mode
#<---->hesiod<-><---->Use Hesiod for user lookups
#<---->[NOTFOUND=return]<---->Stop searching if not found so far
#
passwd: files sss
shadow: tcb files sss
group: files [SUCCESS=merge] sss role
gshadow: files
sudoers: files sss

hosts: files myhostname mdns4_minimal [NOTFOUND=return] dns fallback
# To use db, put the "db" in front of "files" for things you want to be
1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Пер~ить 7Поиск 8Удалить 9МенюМС 10Выход
```

Теперь перезагрузим нашу клиентскую машину **HQ-CLI**.

## reboot

На данном этапе мы можем проверить настроенные нами права и правильность настроек конфигурационных файлов. Сделать мы это можем под локальной учётной записью, у которой есть права администратора, в нашем случае это просто **root**. А ещё мы можем открыть вторую сессию нажав сочетание клавиш:

## Ctrl+Alt+F2

В дальнейшем мы можем переключаться между ними, т.к. нажатием тех же клавиш, но теперь уже с **F1** мы вернемся на первую нашу сессию с графической оболочкой.

## Ctrl+Alt+F1

После того как зашли на вторую сессию, логинимся под **root**

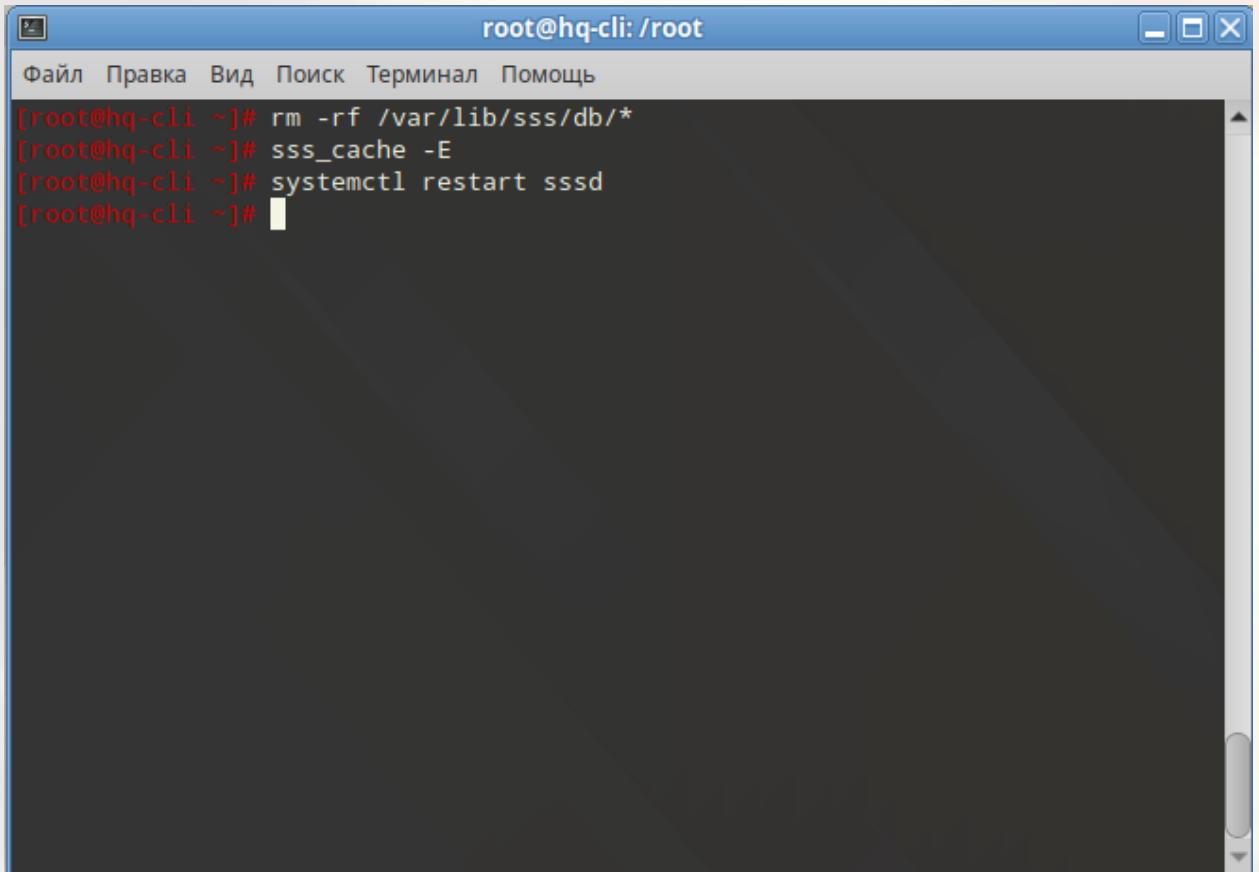
На всякий случай, нужно очистить кэш и удалить остаточные файлы, чтобы всё перезаписалось и применилось, для этого пишем следующие команды:

```
rm -rf /var/lib/sss/db/*
```

```
sss_cache -E
```

И перезагружаем службу **sssd**:

```
systemctl restart sssd
```



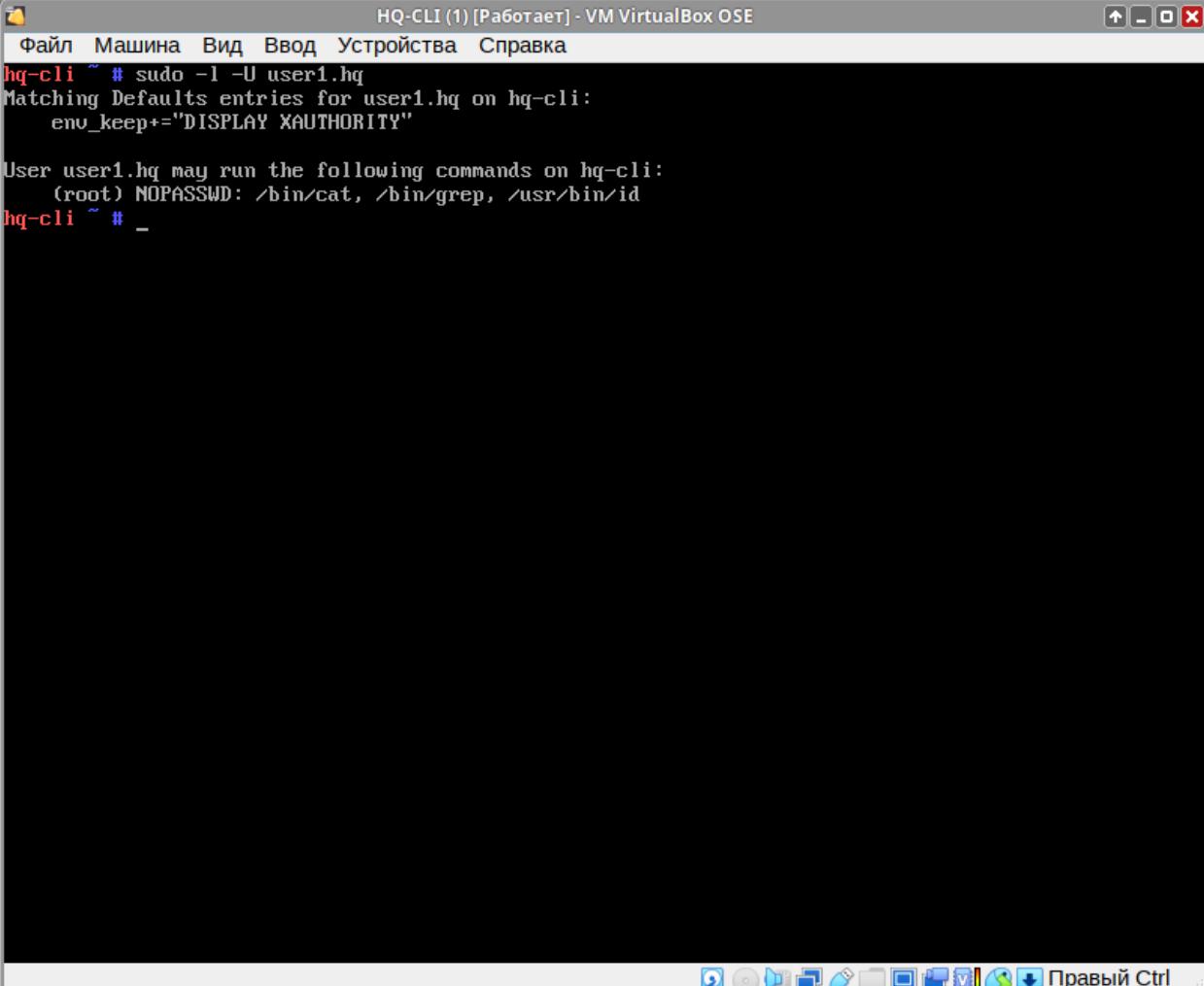
The screenshot shows a terminal window titled "root@hq-cli: /root". The menu bar includes "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Помощь". The command history at the top of the terminal window shows the following sequence of commands:

```
[root@hq-cli ~]# rm -rf /var/lib/sss/db/*
[root@hq-cli ~]# sss_cache -E
[root@hq-cli ~]# systemctl restart sssd
[root@hq-cli ~]#
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

Теперь проверим, какие правила для sudoers получил наш доменный пользователь:

**sudo -l -U user1.hq**



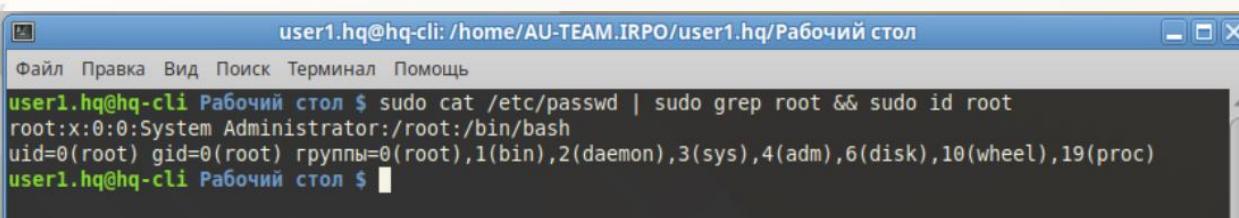
```
hq-cli ~ # sudo -l -U user1.hq
Matching Defaults entries for user1.hq on hq-cli:
    env_keep+="DISPLAY XAUTHORITY"

User user1.hq may run the following commands on hq-cli:
    (root) NOPASSWD: /bin/cat, /bin/grep, /usr/bin/id
hq-cli ~ # _
```

Вернёмся в первую сессию и залогинимся под нашим доменным пользователем **user1.hq** и проверить настроенные права наглядно:

**Ctrl+Alt+F1**

**sudo cat /etc/passwd | sudo grep root && sudo id root**



```
user1.hq@hq-cli Рабочий стол $ sudo cat /etc/passwd | sudo grep root && sudo id root
root:x:0:0:System Administrator:/root:/bin/bash
uid=0(root) gid=0(root) группы=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),19(proc)
user1.hq@hq-cli Рабочий стол $
```

Настройка прав для группы **hq** завершена!

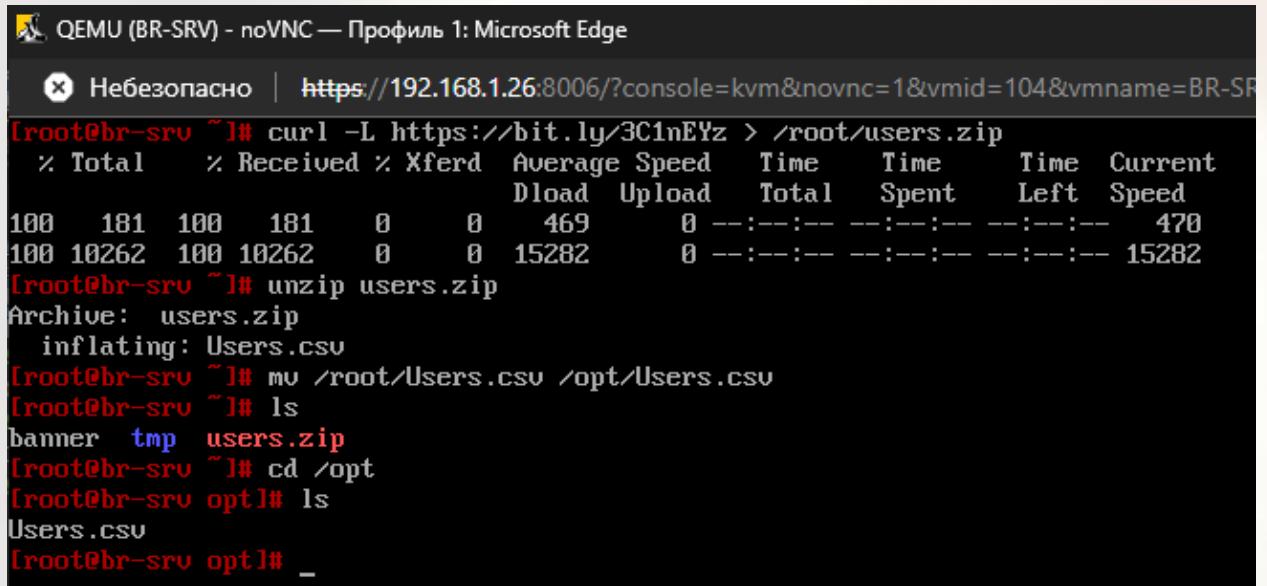
Приступаем к следующему этапу – **импортируем** пользователей из таблицы **Users.csv**.

Для этого нам нужно скачать файл Users.csv, но на ДЭ он уже будет скачан и лежать в каталоге /opt. Мы же, для обучения, скачиваем сейчас его сами и перемещаем его в /opt. Для этого пишем следующие команды:

```
curl -L https://bit.ly/3C1nEYz > /root/users.zip
```

```
unzip /root/users.zip
```

```
mv /root/Users.csv /opt/Users.csv
```



```
QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge
✖ Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1&vmid=104&vmname=BR-SR
[root@br-srv ~]# curl -L https://bit.ly/3C1nEYz > /root/users.zip
  % Total    % Received % Xferd  Average Speed   Time     Time      Current
               Dload  Upload   Total   Spent    Left  Speed
100  181  100  181    0     0  469      0 --:--:-- --:--:-- --:--:--  470
100 10262  100 10262    0     0 15282      0 --:--:-- --:--:-- --:--:-- 15282
[root@br-srv ~]# unzip users.zip
Archive:  users.zip
  inflating: Users.csv
[root@br-srv ~]# mv /root/Users.csv /opt/Users.csv
[root@br-srv ~]# ls
banner  tmp  users.zip
[root@br-srv ~]# cd /opt
[root@br-srv opt]# ls
Users.csv
[root@br-srv opt]# _
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

Создаём файл **import** и пишем туда следующий код:

```
mcedit import

#!/bin/bash

csv_file="/opt/Users.csv"

while IFS=";" read -r firstName lastName role phone ou street zip city country password; do

    if [ "$firstName" == "First Name" ]; then

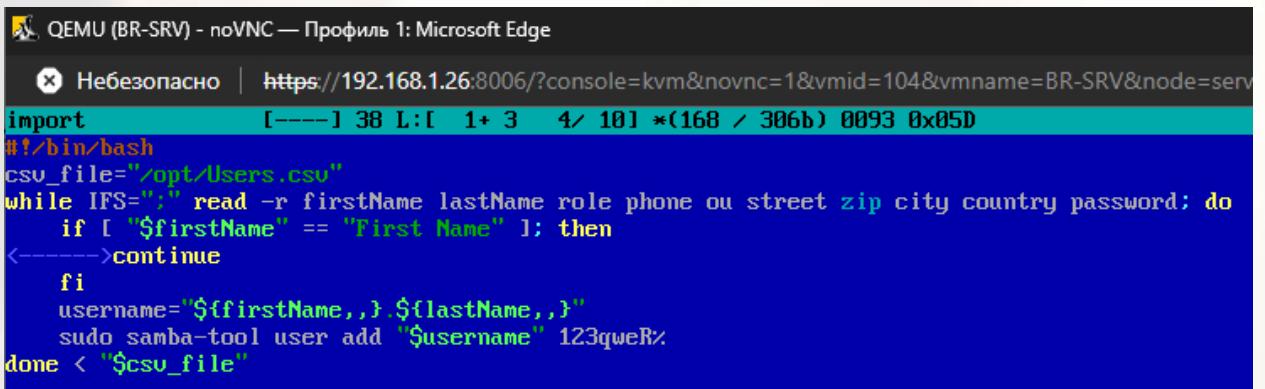
        continue

    fi

    username="${firstName,,}.${lastName,,}"

    sudo samba-tool user add "$username" 123qweR%

done < "$csv_file"
```



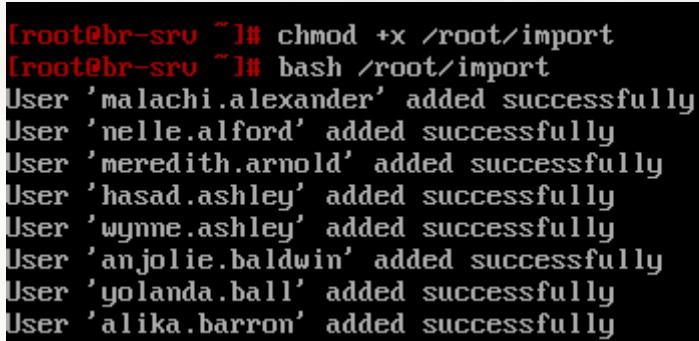
The screenshot shows a terminal window titled "QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge". The window displays the source code of the "import" shell script. The code reads from a CSV file named "Users.csv" and uses the "samba-tool user add" command to create users with a fixed password ("123qweR%"). It includes logic to skip rows where the first name is "First Name". The terminal window has a dark blue background with white text.

```
import          [---] 38 L:[ 1+ 3   4/ 10] *(168 / 306b) 0093 0x05D
#!/bin/bash
csv_file="/opt/Users.csv"
while IFS=";" read -r firstName lastName role phone ou street zip city country password; do
    if [ "$firstName" == "First Name" ]; then
        continue
    fi
    username="${firstName,,}.${lastName,,}"
    sudo samba-tool user add "$username" 123qweR%
done < "$csv_file"
```

Сохраняем этот файл и выдаём ему право на выполнение и запускаем его:

```
chmod +x /root/import
```

```
bash /root/import
```



The screenshot shows a terminal window with a black background and white text. It displays the command "chmod +x /root/import" followed by "bash /root/import". Below this, a list of users is shown, each ending with the message "added successfully". The users listed are: 'malachi.alexander', 'nelle.alford', 'meredith.arnold', 'hasad.ashley', 'wynne.ashley', 'anjolie.baldwin', 'yolanda.ball', and 'alika.barron'. The terminal window has a black background with white text.

```
[root@br-srv ~]# chmod +x /root/import
[root@br-srv ~]# bash /root/import
User 'malachi.alexander' added successfully
User 'nelle.alford' added successfully
User 'meredith.arnold' added successfully
User 'hasad.ashley' added successfully
User 'wynne.ashley' added successfully
User 'anjolie.baldwin' added successfully
User 'yolanda.ball' added successfully
User 'alika.barron' added successfully
```

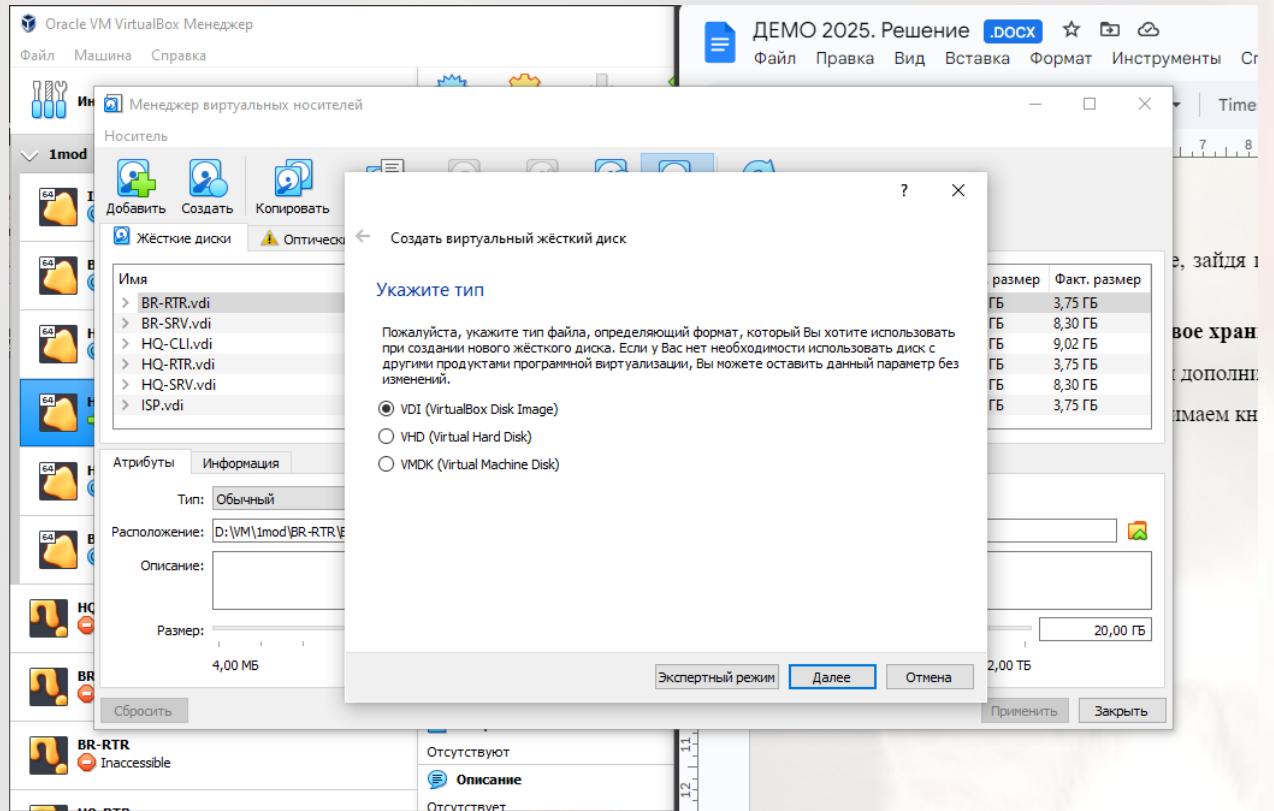
Добавляться они будут долго, но мы это сделали! Успех!

Если есть желание, проверьте, зайдя под одним из этих пользователей через клиентскую машину.

## 2. Конфигурация файлового хранилища на HQ-SRV.

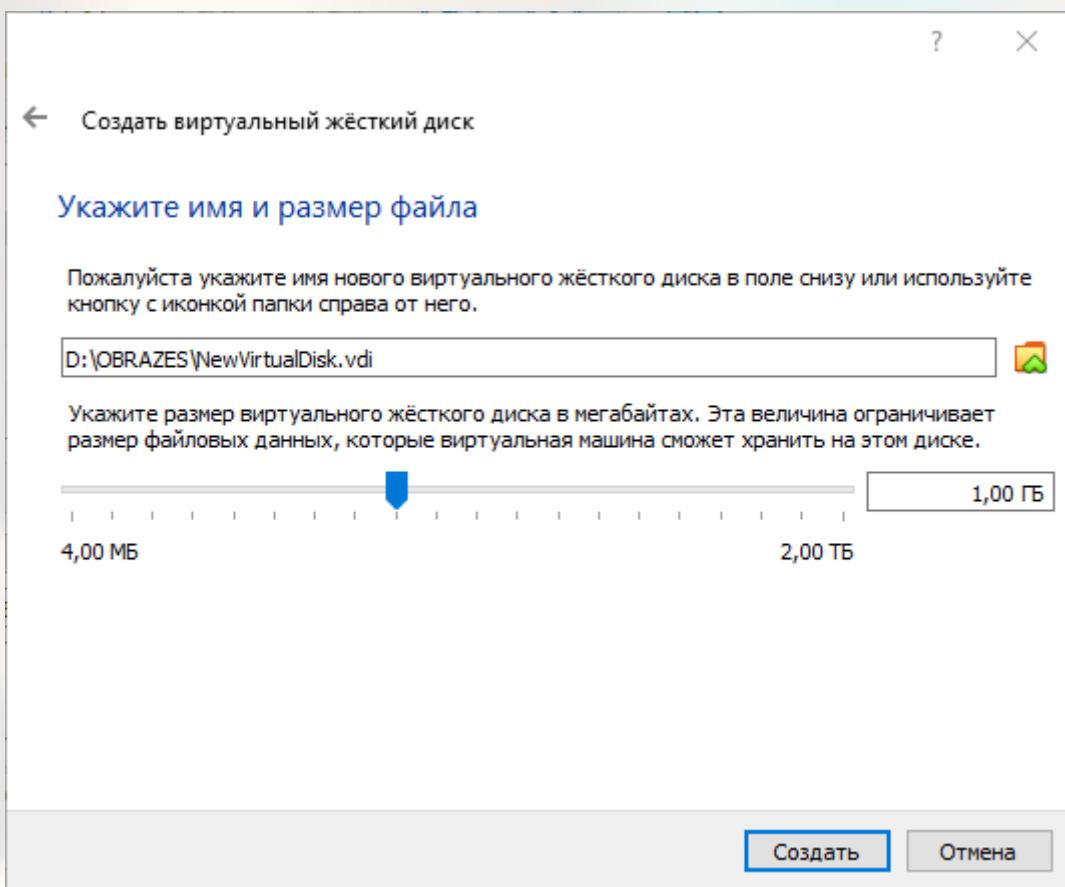
Для начала нужно создать три дополнительных диска размером 1 ГБ каждый.

Для этого жмём **Ctrl+D** и нажимаем кнопку создать.



Все значения выбираем по умолчанию за исключением размера, его выставляем в 1 ГБ.

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Создаём остальные два таким же образом.

В итоге должно получиться так:

Менеджер виртуальных носителей

Носитель

Добавить Создать Копировать Переместить Удалить Отключить Поиск Свойства Обновить

Жёсткие диски Оптические диски Гибкие диски

Имя	Вирт. размер	Факт. размер
HQ-RTR.vdi	20,00 ГБ	3,75 ГБ
HQ-SRV.vdi	60,00 ГБ	8,30 ГБ
ISP.vdi	20,00 ГБ	3,75 ГБ
NewVirtualDisk.vdi	1,00 ГБ	2,00 МБ
NewVirtualDisk_1.vdi	1,00 ГБ	2,00 МБ
NewVirtualDisk_2.vdi	1,00 ГБ	2,00 МБ

Атрибуты Информация

Тип: Обычный

Расположение: D:\OBRAZES\NewVirtualDisk.vdi

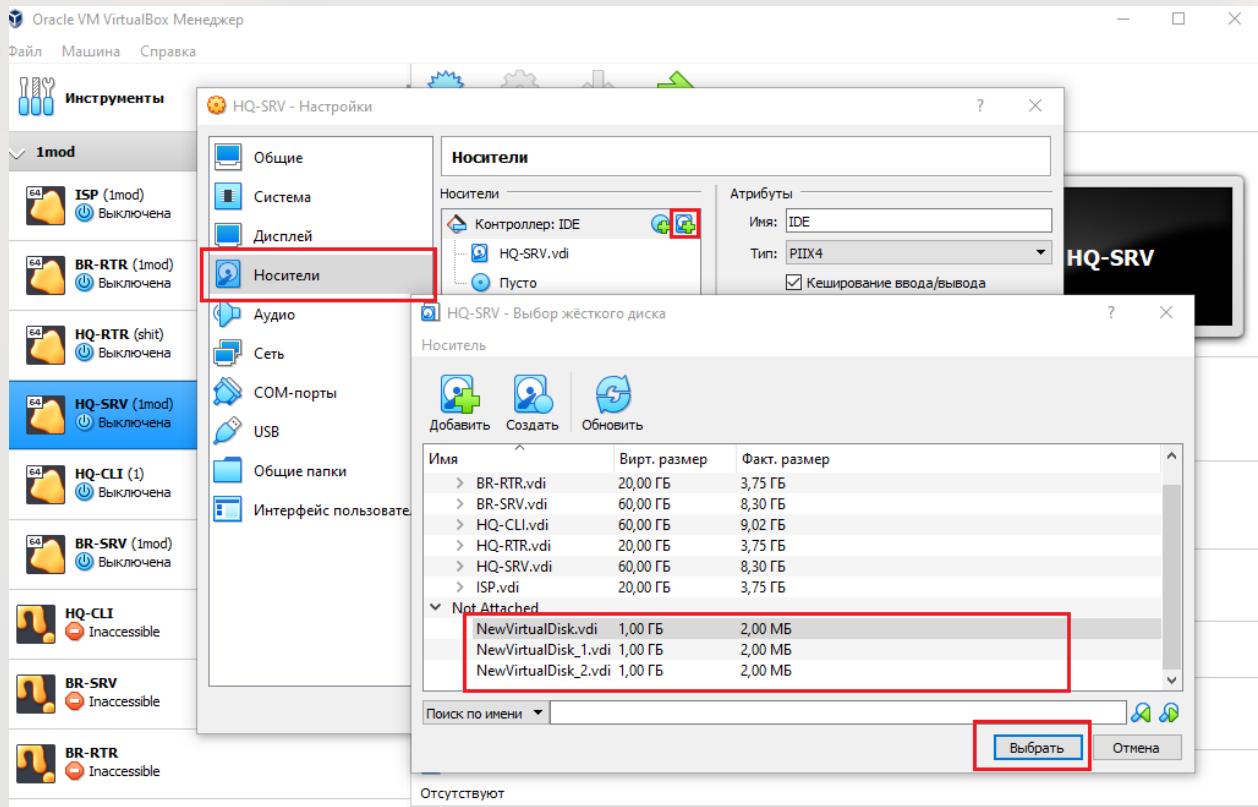
Описание:

Размер:

4,00 МБ 1,00 ГБ 2,00 ТБ

Сбросить Применить Закрыть

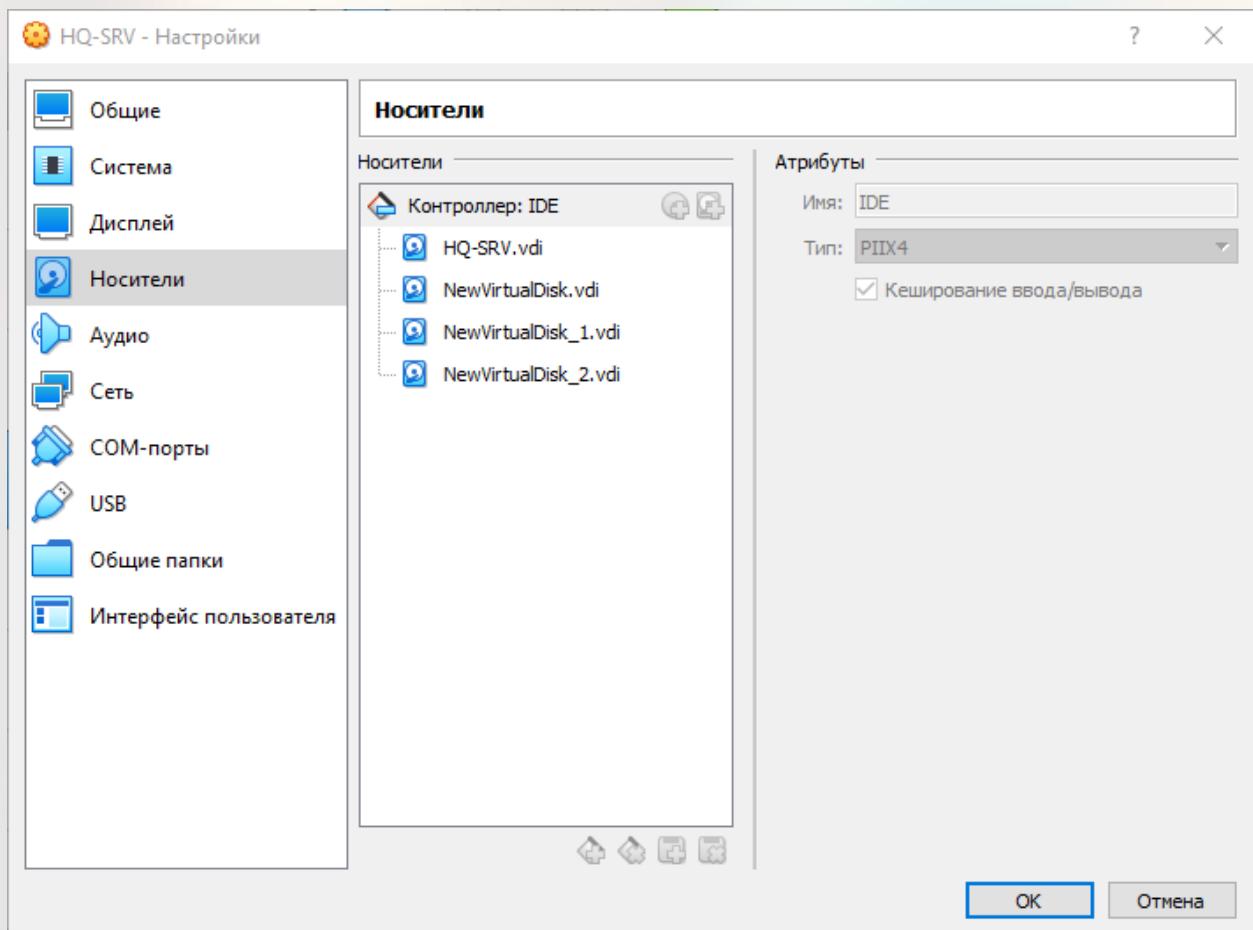
Теперь нам нужно их подключить к виртуальной машине **HQ-SRV**, для этого нужно зайти в настройки и в носителях нажать на значок жесткого диска, а затем подключим три созданных нами ранее диска.



Обратите внимание, что с контроллером, который стоит по умолчанию (**IDE**) не позволяет подключать больше четырех носителей, поэтому удаляем CD-привод и ставим ещё один диск.

В итоге должно получится так:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Теперь заходим в виртуальную машину и просматриваем все диски, которые мы подключили, следующей командой:

**lsblk**

```
[root@hq-srv ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda     8:0    0  32G  0 disk
└─sda1  8:1    0 490M  0 part [SWAP]
  └─sda2  8:2    0 31.5G  0 part /
sdb     8:16   0   1G  0 disk
sdc     8:32   0   1G  0 disk
sdd     8:48   0   1G  0 disk
[root@hq-srv ~]#
```

Обратите внимание, что у вас могут отличаться названия дисков, поэтому указываем при создании названия дисков, которые мы посмотрели ранее командой **lsblk**!

#### AUTHORS:

NECHAEV Теперь создадим дисковый массив уровня 5 из трёх дополнительных дисков  
NAUMOV следующей командой:

NAGORNOVA

**mdadm --create /dev/md0 --level=5 --raid-devices=3 /dev/sd[b-d]**

```
[root@hq-srv ~]# mdadm --create /dev/md0 --level=5 --raid-devices=3 /dev/sd[b-d]
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
[root@hq-srv ~]#
```

Посмотрим статус нашего raid-массива:

**cat /proc/mdstat**

```
[root@hq-srv ~]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid5 sdd[3] sdc[1] sdb[0]
      2093056 blocks super 1.2 level 5, 512k chunk, algorithm 2 [3/3] [UUU]

unused devices: <none>
[root@hq-srv ~]# _
```

Сохраним конфигурацию массива в файл **/etc/mdadm.conf** следующей командой:

**mdadm --detail -scan --verbose > /etc/mdadm.conf**

Теперь создаём раздел через **fdisk**.

Для этого пишем следующую команду:

**fdisk /dev/md0**

```
[root@hq-srv ~]# fdisk /dev/md0

Welcome to fdisk (util-linux 2.39.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS (MBR) disklabel with disk identifier 0x067eb73a.

Command (m for help): _
```

Затем пишем **n**, чтобы создать раздел, прокликаваем **Enter**, потому что он по дефолту предлагает то, что нам нужно, а в конце пишем **w**, чтобы записать изменения:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
[root@hq-srv ~]# fdisk /dev/md0
Welcome to fdisk (util-linux 2.39.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS (MBR) disklabel with disk identifier 0x067eb73a.

Command (m for help): n
Partition type
  p  primary (0 primary, 0 extended, 4 free)
  e  extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-4186111, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-4186111, default 4186111):

Created a new partition 1 of type 'Linux' and of size 2 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

[root@hq-srv ~]# _
```

Теперь создадим файловую систему, по заданию требуется ext4, создаём её следующей командой:

```
mkfs.ext4 /dev/md0p1
```

```
[root@hq-srv ~]# mkfs.ext4 /dev/md0p1
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 523008 4k blocks and 130816 inodes
Filesystem UUID: b0218cbd-ac35-4ba5-8e63-af2d9ed9f345
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

[root@hq-srv ~]# _
```

Теперь настроим автоматическое монтирование в /raid5. Добавляем

AUTHORS следующую строку в конец файла /etc/fstab:

NECHAEV  
NAUMOV  
NAGORNOVA

/dev/md0p1/raid5	ext4	defaults	0	0
------------------	------	----------	---	---

```
fstab [----] 57 L:[ 1+ 5 6/ 6] *(303 / 303б) <EOF>
proc<--><---->/proc<--><----><---->proc<-->nosuid,noexec,gid=proc<><---->0 0
devpts<--><---->/dev/pts<--><---->devpts<-->nosuid,noexec,gid=tty,mode=620<>0 0
tmpfs<--><---->/tmp<--><---->tmpfs<-->nosuid<><----><----><---->0 0
UUID=ddbd388d-496c-479c-8268-79942b19cb8b<---->/<---->ext4<-->relatime<---->1<---->1
UUID=31a3781b-74bb-4edf-9060-b7eb977e9978<---->swap<-->swap<-->defaults<---->0<---->0
/dev/md0p1<---->/raid5<-->defaults<---->0<---->0
```

Затем создаём каталог **/raid5** и монтируем ФС из **/etc/fstab**:

**mkdir /raid5**

**mount -a**

Заметьте, что команда не должна ничего выводить!

```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.1.26:8006/
[root@hq-srv ~]# mkdir /raid5
[root@hq-srv ~]# mount -a
[root@hq-srv ~]# _
```

Теперь настроим сервер файловой системы **NFS**, для этого обновляем список пакетов и устанавливаем службу **nfs-server** следующей командой:

**apt-get update**

**apt-get install nfs-server**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```

QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
✖ Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1&vmid=103&vmname=HQ-SRV&node=server3

[root@hq-srv ~]# apt-get update
Get:1 http://ftp.altlinux.org p10/branch/x86_64 release [4223B]
Get:2 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Get:3 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Fetched 8732B in 0s (41.4kB/s)
Hit http://ftp.altlinux.org p10/branch/x86_64/classic pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64/classic release
Hit http://ftp.altlinux.org p10/branch/x86_64/gostcrypto pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64/gostcrypto release
Hit http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64-i586/classic release
Hit http://ftp.altlinux.org p10/branch/noarch/classic pkglist
Hit http://ftp.altlinux.org p10/branch/noarch/classic release
Reading Package Lists... Done
Building Dependency Tree... Done
[root@hq-srv ~]# apt-get install nfs-server
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  keyutils libevent2.1 libnfsidmap nfs-clients
The following NEW packages will be installed:
  keyutils libevent2.1 libnfsidmap nfs-clients nfs-server
0 upgraded, 5 newly installed, 0 removed and 140 not upgraded.
Need to get 628kB of archives.
After unpacking 2324kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.altlinux.org p10/branch/x86_64/classic keyutils 1.6.3-alt1:sisyphus+266061.100.
Get:2 http://ftp.altlinux.org p10/branch/x86_64/classic libevent2.1 2.1.8-alt3:sisyphus+279511.1
Get:3 http://ftp.altlinux.org p10/branch/x86_64/classic libnfsidmap 1:2.5.4-alt1:sisyphus+279680
Get:4 http://ftp.altlinux.org p10/branch/x86_64/classic nfs-clients 1:2.5.4-alt1:sisyphus+279680
Get:5 http://ftp.altlinux.org p10/branch/x86_64/classic nfs-server 1:2.5.4-alt1:sisyphus+279680
Fetched 628kB in 0s (1233kB/s)
Committing changes...
Preparing...                                           #####
Updating / installing...
1: libnfsidmap-1:2.5.4-alt1                         #####
2: libevent2.1-2.1.8-alt3                           #####
3: keyutils-1.6.3-alt1                            #####
4: nfs-clients-1:2.5.4-alt1                         #####
5: nfs-server-1:2.5.4-alt1                          #####
Done.
[root@hq-srv ~]#

```

Приступаем к самой настройке, создадим каталог, назначим нового владельца и группу ему и выдадим новые права:

```

mkdir /raid5/nfs
chown 99:99 /raid5/nfs
chmod 777 /raid5/nfs

```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```

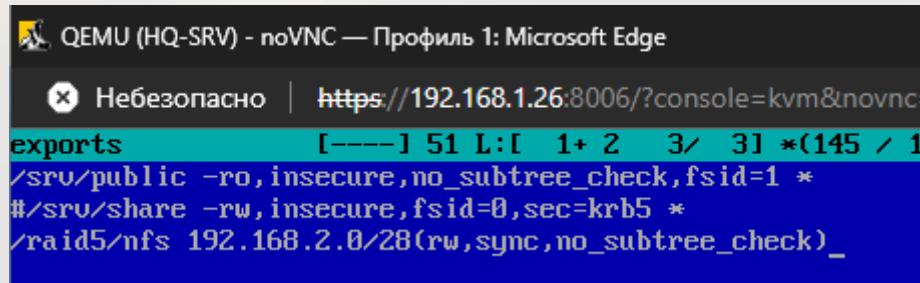
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
✖ Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1&vmid=103&vmname=HQ-SRV&node=server3

[root@hq-srv ~]# mkdir /raid5/nfs
[root@hq-srv ~]# chown 99:99 /raid5/nfs
[root@hq-srv ~]# chmod 777 /raid5/nfs
[root@hq-srv ~]#

```

Откроем каталог для общего доступа в сторону подсети, где находится **HQ-CLI**, для этого заходим в **/etc/exports** и пишем следующую строку в конец файла:

**/raid5/nfs 192.168.2.0/28(rw,sync,no\_subtree\_check)**



QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge  
Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1  
exports [----] 51 L:[ 1+ 2 3/ 31 \*(145 / 1  
/srv/public -ro,insecure,no\_subtree\_check,fsid=1 \*  
#/srv/share -rw,insecure,fsid=0,sec=krb5 \*  
/raid5/nfs 192.168.2.0/28(rw,sync,no\_subtree\_check)\_

После редактирования файла применяем изменения и смотрим, что она экспорттировалась:

**exportfs -a**

**exportfs -v**

```
[root@hq-srv ~]# mcedit /etc/exports  
[root@hq-srv ~]# exportfs -a  
[root@hq-srv ~]# exportfs -v  
/raid5/nfs 192.168.2.0/28(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squash)  
/srv/public <world>(sync,wdelay,hide,no_subtree_check,fsid=1,sec=sys,ro,insecure,root_squash,no_all_squash)  
[root@hq-srv ~]#
```

Включаем и перезапускаем службу NFS:

**systemctl enable nfs**

**systemctl restart nfs**

```
[root@hq-srv ~]# systemctl enable nfs  
Synchronizing state of nfs.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable nfs  
[root@hq-srv ~]# systemctl restart nfs  
[root@hq-srv ~]# -
```

Теперь идём монтировать этот каталог на клиенте **HQ-CLI**, для этого нужно:

**apt-get update**

**apt-get install nfs-clients**

AUTHORS:

NECHAEV  
NAUMOV  
NAGORNOVA

```

QEMU (HQ-CLI) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1&vmid=105&vmname=HQ-CLI&node=se
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
hq-cli ~ # apt-get update
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64 release [4223B]
Получено: 2 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Получено: 3 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Получено 8732B за 0s (35,1kB/s).
Найдено http://ftp.altlinux.org p10/branch/x86_64/classic pkglist
Найдено http://ftp.altlinux.org p10/branch/x86_64/classic release
Найдено http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist
Найдено http://ftp.altlinux.org p10/branch/x86_64-i586/classic release
Найдено http://ftp.altlinux.org p10/branch/noarch/classic pkglist
Найдено http://ftp.altlinux.org p10/branch/noarch/classic release
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
hq-cli ~ # apt-get install nfs-clients
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия nfs-clients уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 620 не будет обновлено.
hq-cli ~ #

```

Он может быть у вас уже установлен, но проверить нужно.

Теперь настроим автоматическое монтирование в каталог **/mnt/nfs**, но для начала создадим его:

**mkdir -p /mnt/nfs**

```

QEMU (HQ-CLI) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1&vmid=105&vmname=HQ-CLI&node=se
root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
hq-cli ~ # mkdir -p /mnt/nfs
hq-cli ~ #

```

Добавляем следующую строку в конец файла **/etc/fstab**:

**192.168.1.2:/raid5/nfs /mnt/nfs nfs intr,soft,\_netdev,x-systemd.automount 0 0**

```

root@hq-cli: /root
Файл Правка Вид Поиск Терминал Помощь
fstab [---] 91 L:[ 1+ 6 7/ 7] *(433 / 433b) <EOF> [*][X]
proc<-><---->/proc<-><----><---->proc<->nosuid,noexec,gid=proc<-><---->0 0
devpts<-><---->/dev/pts<-><---->devpts<->nosuid,noexec,gid=tty,mode=620<->0 0
tmpfs<-><---->/tmp<-><----><---->tmpfs<->nosuid<-><----><----><---->0 0
UUID=22ff23e4-f3da-489b-af27-bd6fc1c912e<-><---->ext4<->relatime<->1<---->1
UUID=a285232e-efcf-4738-b7a1-468324e7a671<-><---->swap<->swap<->defaults<->0<---->0
/dev/sr0<-><---->/media/ALTLinux>udf,iso9660<->ro,noauto,user,utf8,nofail,comment=x-gvfs-show<->0 0
192.168.1.2:/raid5/nfs<->/mnt/nfs<->nfs<->intr,soft,_netdev,x-systemd.automount<->0 0

```

Монтируем ФС из файла **/etc/fstab** и проверяем, что она появилась в списке:

```
mount -a
```

```
mount -v
```

```
user1.hq@hq-cli: /home/AU-TEAM.IRPO/user1.hq/Рабочий стол
Файл Правка Вид Поиск Терминал Помощь
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelega
te,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=28,pgroup=1,time
out=0,minproto=5,maxproto=5,direct,pipe_ino=12749)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatim
e)
tmpfs on /tmp type tmpfs (rw,nosuid,relatime)
tmpfs on /run/user/1083201103 type tmpfs (rw,nosuid,nodev,noexec,relatime,size=4
02328k,nr_inodes=100582,mode=700,uid=1083201103,gid=1083200513)
gvfsd-fuse on /run/user/1083201103/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,re
latime,user_id=1083201103,group_id=1083200513)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,noexec,relatime,size=402328k,nr_
inodes=100582,mode=700)
192.168.1.2:/raid5/nfs on /mnt/nfs type nfs4 (rw,relatime,vers=4.2,rsize=524288,
wsize=524288,namlen=255,soft,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=19
2.168.2.3,local_lock=none,addr=192.168.1.2, netdev)
user1.hq@hq-cli Рабочий стол $
```

Теперь проверим и создадим файл с клиентской машине в каталоге /mnt/nfs, затем посмотрим на сервере, создался ли он:

```
touch /mnt/nfs/cock
```

```
hq-cli ~ # touch /mnt/nfs/cock
hq-cli ~ #

[root@hq-srv ~]# cd /raid5/nfs
[root@hq-srv nfs]# ls
cock
[root@hq-srv nfs]#
```

### 3. Настройка службы сетевого времени на базе сервиса chrony

AUTHORS  
NECHAEV  
NAUMOV  
NAGORNOV  
Для его настройки на роутере HQ-RTR, обновим список пакетов и установим сам пакет:

```
apt update
```

```
apt install chrony
```

```
QEMU (HQ-RTR) - noVNC — Профиль 1: Microsoft Edge
× Небезопасно | https://192.168.1.26:8006/?console=kvm&novnc=1&vmid=101&vmname=HQ-RTR&node=server3&resize=off&cmd=

Astra Linux CE 2.12.46 (orel) hq-rtr.au-team.ipro tty1
hq-rtr login: root
Password:
Last login: Fri Nov  1 11:06:01 +07 2024 on tty1
root@hq-rtr:~# apt-get update
Сущ:1 https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository orel InRelease
Чтение списков пакетов... Готово
root@hq-rtr:~# apt-get install chrony
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующий пакет устанавливается автоматически и больше не требуется:
  libiptc25
Для его удаления используйте «apt autoremove».
Предлагаемые пакеты:
  dnsutils networkd-dispatcher
Пакеты, которые будут УДАЛЕНЫ:
  ntp
НОВЫЕ пакеты, которые будут установлены:
  chrony
обновлено 0, установлено 1 новых пакетов, для удаления отмечено 1 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 211 kB архивов.
После данной операции, объём занятого дискового пространства уменьшится на 1 636 kB.
Хотите продолжить? [Д/Н] у
Пол:1 https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository orel/main amd64 chrony amd64 3.4-4+deb10u2 [211 kB]
Получено 211 kB за 0с (337 kB/c).
(Чтение базы данных ... на данный момент установлено 71184 файла и каталога.)
Удаляется ntp (1:4.2.8p15+dfsg-1+ci202109031329+astra1) ...
Выбор ранее не выбранного пакета chrony.
(Чтение базы данных ... на данный момент установлено 71128 файлов и каталогов.)
Подготовка к распаковке .../chrony_3.4-4+deb10u2_amd64.deb ...
Распаковывается chrony (3.4-4+deb10u2) ...
Настраивается пакет chrony (3.4-4+deb10u2) ...
Creating '_chrony' system user/group for the chrony daemon...
Creating config file /etc/chrony/chrony.conf with new version
Creating config file /etc/chrony/chrony.keys with new version
Created symlink /etc/systemd/system/chronyd.service → /lib/systemd/system/chrony.service.
Created symlink /etc/systemd/system/multi-user.target.wants/chrony.service → /lib/systemd/system/chrony.service.
Обрабатываются триггеры для systemd (232-25+deb9u14astra.ce11) ...
Обрабатываются триггеры для man-db (2.7.6.1-2) ...
root@hq-rtr:~# _
```

Проверим работу службы **chrony** и **timedatectl**:

**systemctl status chrony**

**timedatectl**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
HQ-RTR (shit) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
libopts25
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 1 пакетов, и 0 пакетов не обновлено.
После данной операции, объём занятого дискового пространства уменьшится на 172 kB.
Хотите продолжить? [Д/н] у
(Чтение базы данных ... на данный момент установлено 66954 файла и каталога.)
Удаляется libopts25:amd64 (1:5.18.12-3) ...
Обрабатываются триггеры для libc-bin (2.28-10+deb10u1) ...
root@hq-rtr:~# systemctl status chrony
● chrony.service - chrony, an NTP client/server
   Loaded: loaded (/lib/systemd/system/chrony.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-11-13 11:11:54 +07; 21s ago
     Docs: man:chronyd(8)
           man:chronyc(1)
           man:chrony.conf(5)
 Main PID: 1618 (chrony)
    CGroup: /system.slice/chrony.service
            └─1618 /usr/sbin/chronyd -F -1
               ├─1619 /usr/sbin/chronyd -F -1

ноя 13 11:11:54 hq-rtr.au-team.irpo systemd[1]: Starting chrony, an NTP client/server...
ноя 13 11:11:54 hq-rtr.au-team.irpo chrony[1618]: chrony version 3.4 starting (+CMDMON +NTP +REFCLOCK)
ноя 13 11:11:54 hq-rtr.au-team.irpo chrony[1618]: Initial frequency 13.999 ppm
ноя 13 11:11:54 hq-rtr.au-team.irpo chrony[1618]: Loaded seccomp filter
ноя 13 11:11:54 hq-rtr.au-team.irpo chrony[1618]: Started chrony, an NTP client/server.
ноя 13 11:12:01 hq-rtr.au-team.irpo chrony[1618]: Selected source 162.159.200.1
ноя 13 11:12:01 hq-rtr.au-team.irpo chrony[1618]: System clock wrong by -4.453335 seconds, adjustment -4.453335
ноя 13 11:11:56 hq-rtr.au-team.irpo chrony[1618]: System clock was stepped by -4.453335 seconds
ноя 13 11:12:07 hq-rtr.au-team.irpo chrony[1618]: Source 2606:4700:f1::123 replaced with 2a00:ab00:
root@hq-rtr:~# timedatectl
          Local time: Ср 2024-11-13 11:12:28 +07
          Universal time: Ср 2024-11-13 04:12:28 UTC
                RTC time: Ср 2024-11-13 04:12:28
                  Time zone: Asia/Barnaul (+07, +0700)
      Network time on: no
NTP synchronized: yes
 RTC in local TZ: no
root@hq-rtr:~# s
```

Видим, что всё функционирует и синхронизация активна, которую мы позже уберём. Синхронизация нужна сейчас для того, чтобы мы получили самое точное время от серверов со статусом 0 и так далее. Позже мы будем пользоваться локальным временем, которое сохранится благодаря нашему chrony на роутере, и уже он будет выступать сервером для устройств клиентов.

Теперь приступим к настройке, редактируем файл `/etc/chrony/chrony.conf`, введем в начало файла следующие строки и в целом приводим файл к такому виду:

## local stratum 5

**allow 192.168.1.0/26**

AUTHORS

NECHAEV

NAUMOV

NAGORNOY

**allow 192.168.2.0/28**

**allow 172.16.5.0/28**

**allow 192.168.4.0/27**

```
QEMU (HQ-RTR) - noVNC — Профиль 1: Microsoft Edge
HTTPS://192.168.4.85:8006/?console=kvm&novnc=1&vmid=101&vmname=HQ-RTR
/etc/chrony/chrony.conf [----] 0 L:[ 1+ 3 4/ 33] *(58 /1027b) 0097 0x061
local stratum 5
allow 192.168.1.0/26
allow 192.168.2.0/28
allow 172.16.5.0/28
allow 192.168.4.0/27
# Welcome to the chrony configuration file. See chrony.conf(5) for more
# information about usable directives.
#pool 2.debian.pool.ntp.org iburst

# This directive specify the location of the file containing ID/key pairs for
# NTP authentication.
keyfile /etc/chrony/chrony.keys

# This directive specify the file into which chrony will store the rate
# information.
driftfile /var/lib/chrony/chrony.drift

# Uncomment the following line to turn logging on.
#log tracking measurements statistics

# Log files location.
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0

# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtcfile' directive.
#rtcsync

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 1 3
```

Файл должен выглядеть так, как на скрине, **закомментировав** ещё две строки, они нам нужны были только синхронизации с публичным сервером времени.

Включаем и перезапускаем службу **chrony**:

**systemctl enable --now chrony**

**systemctl restart chrony**

Выключаем теперь ту самую синхронизацию, оставляя, по сути, главным сервером NTP – наш роутер **HQ-RTR**, и проверяем ещё раз статус **timedatectl**:

AUTHORS:

NECHAEV

NAUMOV

NAGORNOY

**timedatectl set-ntp 0**

**timedatectl**

```
root@hq-rtr:~# timedatectl set-ntp 0
root@hq-rtr:~# timedatectl
      Local time: Пт 2024-11-15 10:18:50 +07
      Universal time: Пт 2024-11-15 03:18:50 UTC
            RTC time: Пт 2024-11-15 03:18:50
           Time zone: Asia/Barnaul (+07, +0700)
    Network time on: no
  NTP synchronized: no
    RTC in local TZ: no
root@hq-rtr:~#
```

Теперь переходим к настройке клиента, в качестве него возьмём **HQ-CLI**, но по заданию есть ещё, но о них позже.

Перед установкой новой службы выключим chrony на **HQ-CLI**:

```
systemctl disable --now chronyd
```

```
systemctl status chronyd
```

```
hq-cli ~ # systemctl disable --now chronyd
Synchronizing state of chronyd.service with SysV service script with /lib/systemd/systemd-sysv-in-
tall.
Executing: /lib/systemd/systemd-sysv-install disable chronyd
hq-cli ~ # systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/lib/systemd/system/chronyd.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
       Docs: man:chronyd(8)
              man:chrony.conf(5)

сен 11 05:33:52 HQ-Cli systemd[1]: Starting NTP client/server...
сен 11 05:33:53 HQ-CLI chronyd[2754]: chronyd version 4.3 starting (+CMDMON +NTP +REFCLOCK +RTC +F
сен 11 05:33:53 HQ-CLI systemd[1]: Started NTP client/server.
сен 11 06:07:42 hq-cli.au-team.irpo chronyd[2754]: chronyd exiting
сен 11 06:07:42 hq-cli.au-team.irpo systemd[1]: Stopping NTP client/server...
сен 11 06:07:42 hq-cli.au-team.irpo systemd[1]: chronyd.service: Deactivated successfully.
сен 11 06:07:42 hq-cli.au-team.irpo systemd[1]: Stopped NTP client/server.
hq-cli ~ #
```

Обновляем список пакетов на **HQ-CLI** и скачиваем службу **systemd-timesyncd**:

```
apt-get update
```

```
apt-get install systemd-timesyncd
```

AUTHORS:

NECHAEV

NAUMOV

NAGORNOVA

```
user@HQ-CLI: /home/user
[...]
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64 release [4223B]
Получено: 2 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Получено: 3 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Получено 8732B за 0s (18,3kB/s).
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64/classic pkglist [24,4MB]
Получено: 2 http://ftp.altlinux.org p10/branch/x86_64/classic release [137B]
Получено: 3 http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist [17,9MB]
Получено: 4 http://ftp.altlinux.org p10/branch/x86_64-i586/classic release [142B]
Получено: 5 http://ftp.altlinux.org p10/branch/noarch/classic pkglist [7281kB]
Получено: 6 http://ftp.altlinux.org p10/branch/noarch/classic release [137B]
Получено 49,5MB за 13s (3610kB/s).
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
HQ-CLI ~ # apt-get install systemd-timesyncd
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
 libnss-myhostname libnss-systemd pam systemd systemd-analyze systemd-boot-efi
 systemd-modules-common systemd-networkd systemd-sysctl-common systemd-sysvinit
 systemd-tmpfiles-common systemd-utils-filetriggers udev
Следующие пакеты будут ОБНОВЛЕНЫ:
 libnss-myhostname libnss-systemd pam systemd systemd-analyze systemd-boot-efi
 systemd-modules-common systemd-sysctl-common systemd-sysvinit systemd-tmpfiles-common
 systemd-utils-filetriggers udev
Следующие НОВЫЕ пакеты будут установлены:
 systemd-networkd systemd-timesyncd
12 будет обновлено, 2 новых установлено, 0 пакетов будет удалено и 685 не будет обновлено.
Необходимо получить 7833kB архивов.
После распаковки потребуется дополнительно 4580kB дискового пространства.
Продолжить? [Y/n] Y
Активация Windows
Чтобы активировать Windows, нажмите правую кнопку мыши на рабочем столе "Параметры
[...]
```

Теперь зайдём в конфиг **/etc/systemd/timesyncd.conf** и отредактируем только одну строку:

**NTP=192.168.1.1**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
timesyncd.conf      [-M--] 15 L:[ 1+15 16/ 21] *(659 / 744b) 0010 0x00A [*][X]
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it under the
# terms of the GNU Lesser General Public License as published by the Free
# Software Foundation; either version 2.1 of the License, or (at your option)
# any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file, or by creating "drop-ins" in
# the timesyncd.conf.d/ subdirectory. The latter is generally recommended.
# Defaults can be restored by simply deleting this file and all drop-ins.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=192.168.1.1
#FallbackNTP=
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

Теперь включим службу **systemd-timesyncd** и посмотрим её статус работы:

**systemctl enable --now systemd-timesyncd**

**timedatectl timesync-status**

```
HQ-CLi ~ # systemctl enable --now systemd-timesyncd
HQ-CLi ~ # timedatectl timesync-status
          Server: 192.168.1.1 (192.168.1.1)
          Poll interval: 4min 16s (min: 32s; max 34min 8s)
            Leap: normal
          Version: 4
        Stratum: 5
      Reference: 7F7F0101
      Precision: 1us (-25)
    Root distance: 0 (max: 5s)
        Offset: -1.407ms
        Delay: 672us
        Jitter: 759us
   Packet count: 4
      Frequency: -6,038ppm
HQ-CLi ~ #
```

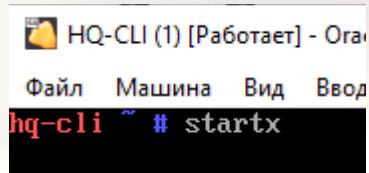
Актив

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

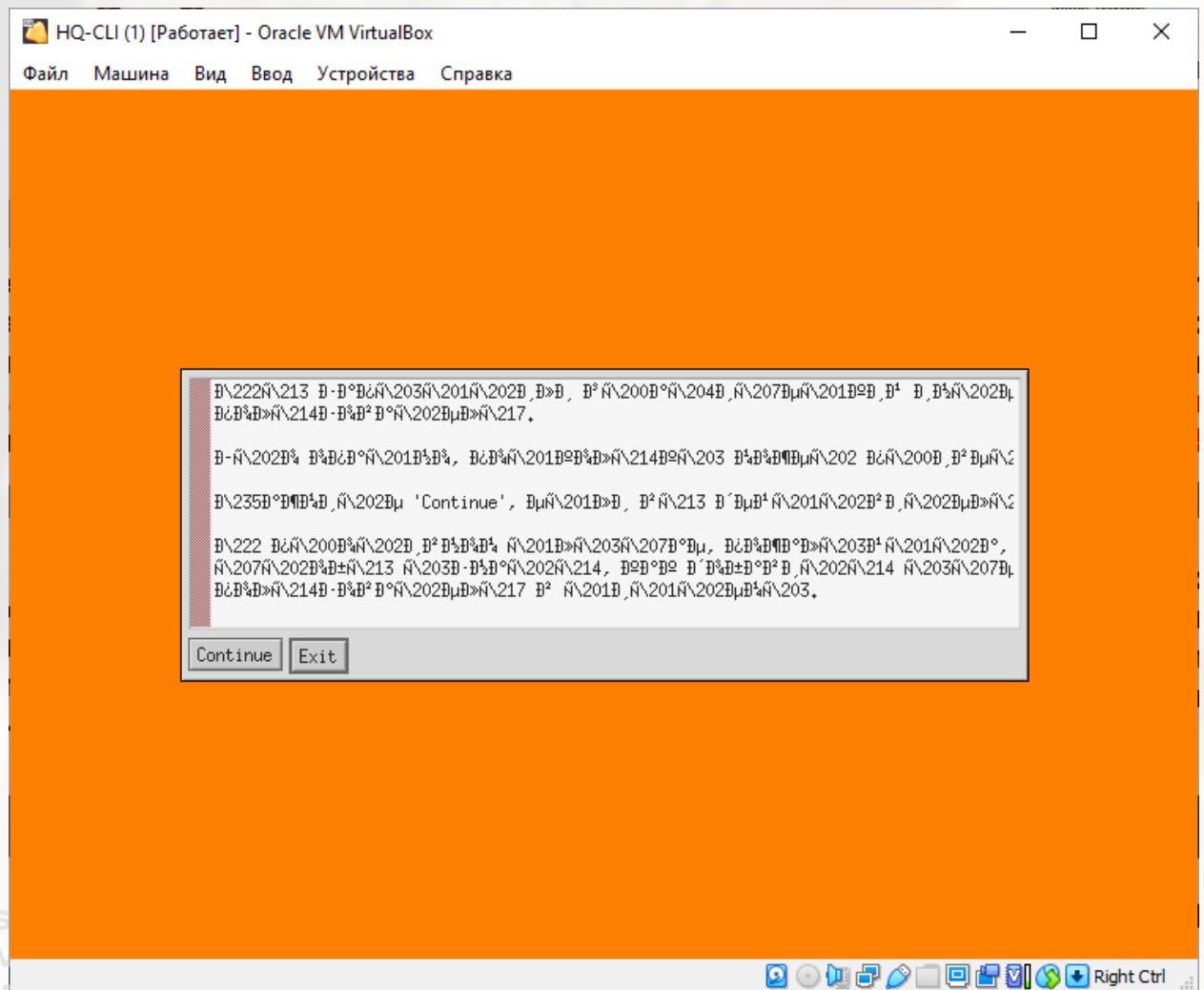
Видим, что стратум совпадает по заданию и всё работает. Задание выполнено.

Но есть одно НО! После перезагрузки клиентской машины **HQ-CLI** и вход в пользователя у вас может не появиться рабочий стол. Для этого мы заходим снова через **Ctrl+Alt+F2** во второе окно и прописываем команду **startx**. Это заставит запуститься графическую среду.

**ДЕЛАЕМ ЭТО ТОЛЬКО В СЛУЧАЕ ПОЛОМКИ ГРАФИЧЕСКОЙ СРЕДЫ!**



Далее мы увидим следующий бред на скриншоте, на нём мы прожигаем **continue**:

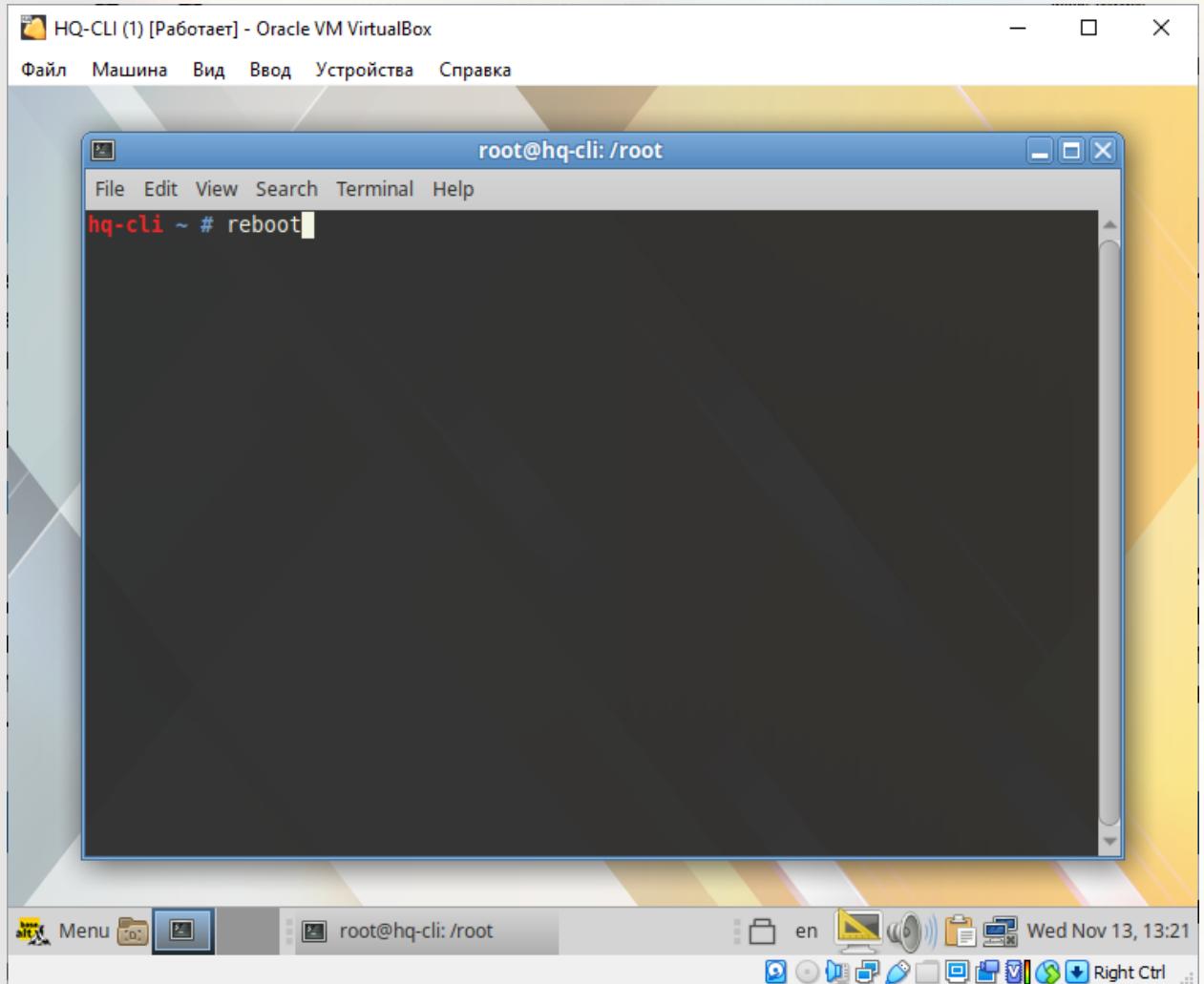


AUTHORS  
NECHAEV  
NAUMOV

NAGORNO

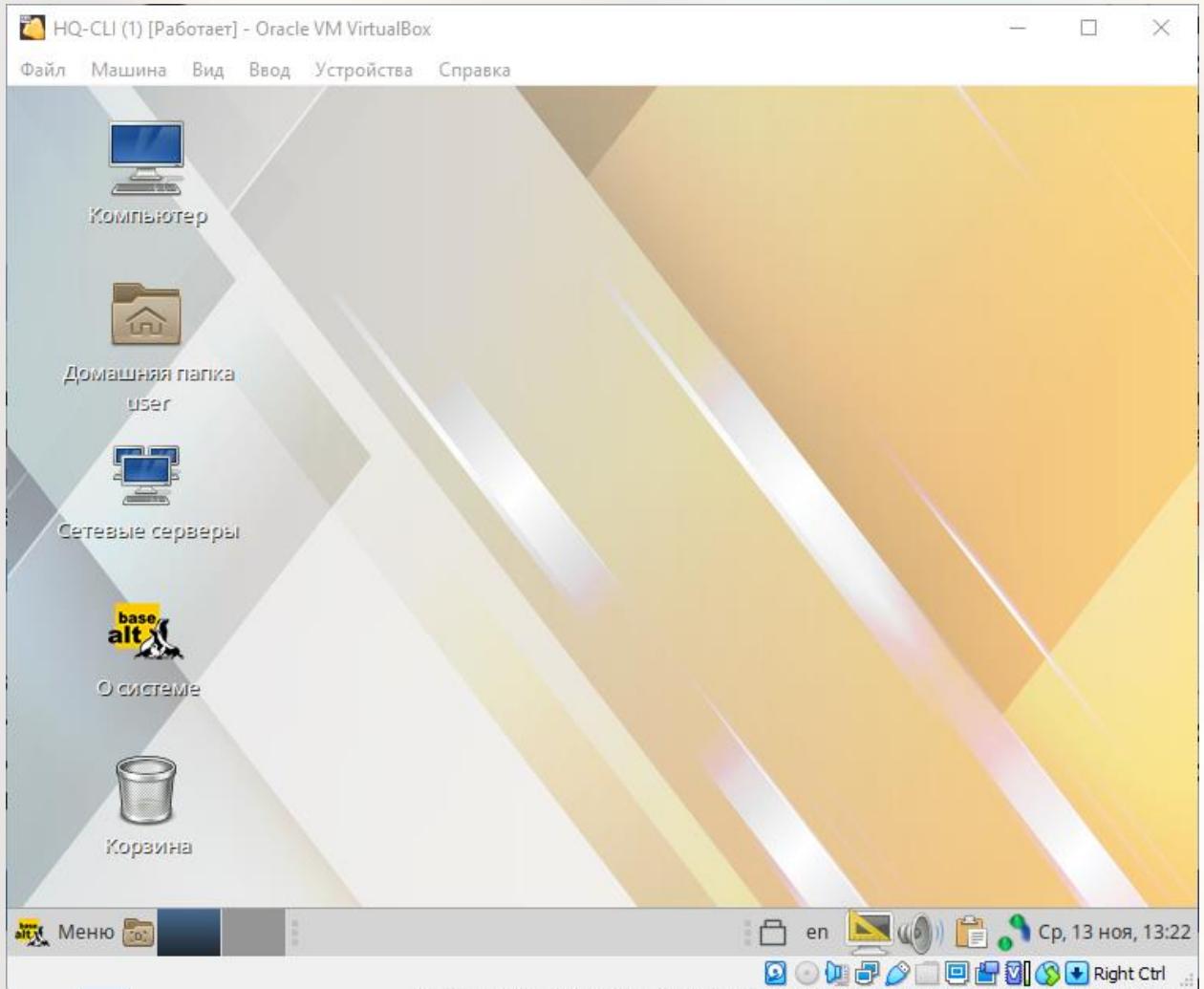
После этого она начнёт потихоньку запускаться, но мы ещё раз перезагружаем систему через **reboot** и система должна вновь нормально запуститься:

Right Ctrl



Вуаля, всё успешно, и дата на месте, и графическая среда!

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Настроим теперь **BR-RTR**, удаляем пакеты **ntp**, **chrony**, если они есть:

**apt purge ntp**

**apt purge chrony**

```
QEMU (BR-RTR) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=102&vmname=BR-RTR&node=server&resize=1000x600
root@br-rtr:~# apt purge ntp
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Пакет «ntp» не установлен, поэтому не может быть удалён
Следующий пакет устанавливался автоматически и больше не требуется:
  libopts25
Для его удаления используйте «apt autoremove».
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
root@br-rtr:~# apt purge chrony
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Пакет «chrony» не установлен, поэтому не может быть удалён
Следующий пакет устанавливался автоматически и больше не требуется:
  libopts25
Для его удаления используйте «apt autoremove».
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
root@br-rtr:~# _
```

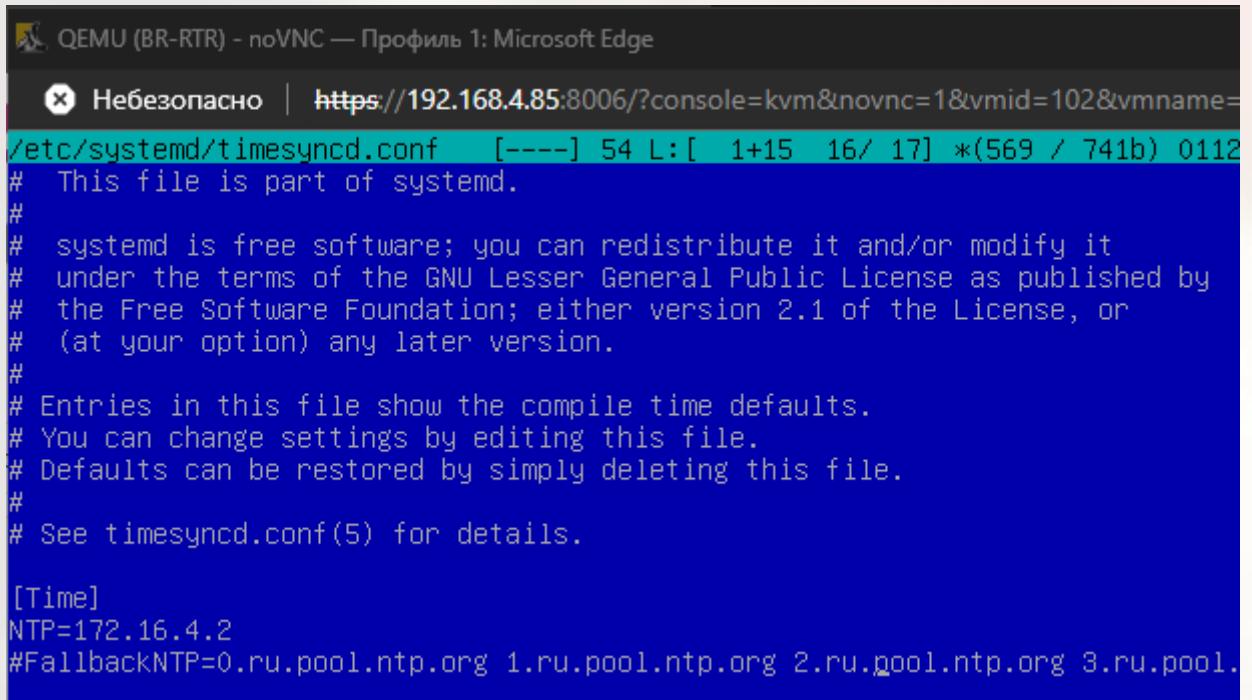
На Астре по умолчанию должна быть установлена служба **systemd-timesyncd**, но если её нет, то установите:

**apt update**

**apt install systemd-timesyncd**

Настроим также его конфиг в **/etc/systemd/timesyncd.conf**:

**NTP=172.16.4.2**



```
QEMU (BR-RTR) - noVNC — Профиль 1: Microsoft Edge
HTTPS://192.168.4.85:8006/?console=kvm&novnc=1&vmid=102&vmname=BR-RTR

/etc/systemd/timesyncd.conf [----] 54 L:[ 1+15 16/ 17] *(569 / 741b) 0112
# This file is part of systemd.
#
# systemd is free software; you can redistribute it and/or modify it
# under the terms of the GNU Lesser General Public License as published by
# the Free Software Foundation; either version 2.1 of the License, or
# (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=172.16.4.2
#FallbackNTP=0.ru.pool.ntp.org 1.ru.pool.ntp.org 2.ru.pool.ntp.org 3.ru.pool.
```

Теперь включим службу **systemd-timesyncd** и готово:

**systemctl enable --now systemd-timesyncd**

На остальных клиентах нужно проделать тоже самое, исходя из документа остались - **HQ-SRV**, **BR-SRV** (настройка идентична клиенту **HQ-CLI**, поэтому [клику](#)).

Но помните, что **NTP** для **BR-SRV** – это внешний IP-адрес **HQ-RTR**, то-есть **172.16.4.2**.

#### 4. Сконфигурируйте ansible на сервере BR-SRV

AUTHORS Для начала проверим, обновлены ли у нас списки пакетов и затем попробуем  
NECHAEV установить **ansible**:  
NAUMOV

**NAGORNO apt-get update**

**apt-get install ansible**

```

python3-module-resuelib python3-module-yaml
The following NEW packages will be installed:
  ansible libsodium23 python3-module-bcrypt python3-module-paramiko python3-module-pynacl
  python3-module-resuelib python3-module-yaml
0 upgraded, 7 newly installed, 0 removed and 289 not upgraded.
Need to get 19.3MB of archives.
After unpacking 126MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.altlinux.org p10/branch/x86_64/classic python3-module-yaml 6.0.1-alt1.1:p10+340092.
554.16.1e1709018089 [167kB]
Get:2 http://ftp.altlinux.org p10/branch/x86_64/classic python3-module-bcrypt 3.2.0-alt2:sisyphus+27.
9385.100.1.2e1626528254 [34.0kB]
Get:3 http://ftp.altlinux.org p10/branch/x86_64/classic libsodium23 1.0.18-alt1:sisyphus+279527.100.
1.1e162655762 [147kB]
Get:4 http://ftp.altlinux.org p10/branch/x86_64/classic python3-module-pynacl 1.3.0-alt1:sisyphus+27.
9125.100.1.1e1626380493 [86.1kB]
Get:5 http://ftp.altlinux.org p10/branch/noarch/classic python3-module-paramiko 2.11.0-alt1:p10+3082.
71.100.1.1e1665571428 [289kB]
Get:6 http://ftp.altlinux.org p10/branch/noarch/classic python3-module-resuelib 0.5.5-alt1:p10+288.
299.100.1.1e1635428468 [27.0kB]
Get:7 http://ftp.altlinux.org p10/branch/noarch/classic ansible 2.9.27-alt3.p10.2:p10+338955.200.6.1
e1711953698 [18.6MB]
Fetched 19.3MB in 6s (2949kB/s)
Committing changes...
Preparing...                                           #####[100%]
Updating / installing...
1: python3-module-resuelib-0.5.5-alt1 #####[14%]
2: libsodium23-1.0.18-alt1 #####[29%]
3: python3-module-pynacl-1.3.0-alt1 #####[43%]
4: python3-module-bcrypt-3.2.0-alt2 #####[57%]
5: python3-module-paramiko-2.11.0-alt1 #####[71%]
6: python3-module-yaml-6.0.1-alt1.1 #####[86%]
7: ansible-2.9.27-alt3.p10.2 #####[100%]
Done

```

Далее нам нужен рабочий каталог для нашего ansible, который может быть уже создан, НО если нет, то создадим его следующей командой:

**mkdir /etc/ansible**

У нас он уже создан, и там же находится нужный нам файл **hosts**, тоже уже созданный, НО в случае его отсутствия, нужно также его создать:

**mcedit /etc/ansible/hosts**

```

[root@br-srv ~]# cd /etc/ansible/
[root@br-srv ansible]# ls
ansible.cfg  hosts
[root@br-srv ansible]# 

```

AUTHORS:  
NECHAEV

Теперь нам нужно написать следующие строки в файл **hosts**:

NAUMOV  
NAGORNOVA

**hq-srv ansible\_host=sshuser@192.168.1.2 ansible\_port=2024**  
**hq-cli ansible\_host=sshuser@192.168.2.5 ansible\_port=2024** (у вас может быть другой адрес)

**hq-rtr ansible\_host=net\_admin@192.168.1.1 ansible\_port=22**

**br-rtr ansible\_host=net\_admin@192.168.4.1 ansible\_port=22**

```
hosts [----] 57 L:[ 1+ 3 4/ 4] *(231 / 231)
hq-srv ansible_host=sshuser@192.168.1.2 ansible_port=2024
hq-cli ansible_host=sshuser@192.168.2.8 ansible_port=2024
hq-rtr ansible_host=net_admin@192.168.1.1 ansible_port=22
br-rtr ansible_host=net_admin@192.168.4.1 ansible_port=22_
```

И настроим в каталоге `/etc/ansible` файл `ansible.cfg`:

**mcedit /etc/ansible/ansible.cfg**

Добавим под строку `[defaults]` ещё одну:

`ansible_python_interpreter=/usr/bin/python3`

```
ansible.cfg [-M--] 43 L:[ 1+10 11/493] *(423 /20030b) 0010 0x00A
# config file for ansible -- https://ansible.com/
# =====

# nearly all parameters can be overridden in ansible-playbook
# or with command line flags. ansible will read ANSIBLE_CONFIG,
# ansible.cfg in the current working directory, .ansible.cfg in
# the home directory or /etc/ansible/ansible.cfg, whichever it
# finds first

[defaults]
ansible_python_interpreter=/usr/bin/python3_
```

Но, возникает другая проблема, в первом модуле мы настраивали SSH на серверах, однако маршрутизаторы **HQ-RTR**, **BR-RTR** и клиент **HQ-CLI** не входили в пункт по настройке. Теперь его нужно настроить сейчас, на этих устройствах, поэтому приступаем к их настройке, чтобы мы могли выполнить задание по **ansible**.

Первым делом настроим **HQ-RTR**, в ней немного отличается пакет и путь к конфигу, но в остальном всё тоже самое, сейчас увидите:

**AUTHORS:**

**NECHAEV**

**NAUMOV**

**apt install ssh-server**

```
 HQ-RTR (shit2) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@hq-rtr:~# apt update
Пол:1 http://deb.debian.org/debian buster InRelease [122 kB]
Игн:1 http://deb.debian.org/debian buster InRelease
Получено 122 kB за 0с (273 kB/c)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состояниях... Готово
Может быть обновлено 274 пакета. Запустите «apt list --upgradable» для их показа.
W: Ошибка GPG: http://deb.debian.org/debian buster InRelease: Следующие подписи не могут быть проверены, так как недоступен открытый ключ: NO_PUBKEY 648ACFD622F3D138 NO_PUBKEY 0E98404D386FA1D9 NO_PUBKEY DCC9EFBF77E11517
root@hq-rtr:~# apt install openssh-server
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состояниях... Готово
Будут установлены следующие дополнительные пакеты:
 libargon2-1 libcomerr2 libcryptsetup12 libgcrypt20 libgnutls30 libgssapi-krb5-2
 libhogweed4 libk5crypto3 libkrb5-3 libkrb5support0 libmount1 libnettle6 libp11-kit0
 libpam-systemd libsystemd0 libtasn1-6 libunistring2 libx11-6 libx11-data libxau6 libxcb1
 libxdmcp6 libxext6 libxmuu1 openssh-client openssh-sftp-server systemd xauth
Предлагаемые пакеты:
 rng-tools gnutls-bin krb5-doc krb5-user keychain libpam-ssh monkeysphere ssh-askpass molly-guard
 rssh systemd-containerr policykit-1
Рекомендуемые пакеты:
 krb5-locales
Новые пакеты, которые будут установлены:
 libargon2-1 libcomerr2 libcryptsetup12 libpam-systemd libunistring2 libx11-6 libx11-data
 libxau6 libxcb1 libxdmcp6 libxext6 libxmuu1 openssh-server openssh-sftp-server xauth
Пакеты, которые будут обновлены:
 libcomerr2 libgcrypt20 libgnutls30 libgssapi-krb5-2 libhogweed4 libk5crypto3 libkrb5-3
 libkrb5support0 libmount1 libnettle6 libp11-kit0 libsystemd0 libtasn1-6 openssh-client systemd
 обновлено 15, установлено 15 новых пакетов, для удаления отмечено 0 пакетов, и 259 пакетов не обновлено.
Необходимо скачать 10,6 МБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 12,0 МВ.
Хотите продолжить? [Д/Н] у
```

Теперь заходим в конфигурационный файл **/etc/ssh/sshd\_config** и вносим в него следующие строки:

**Port 22**

**MaxAuthTries 2**

**AllowUsers net\_admin**

**PermitRootLogin no**

**AUTHORS:**

NECHAEV  
NAUMOV  
NAGORNOVA

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

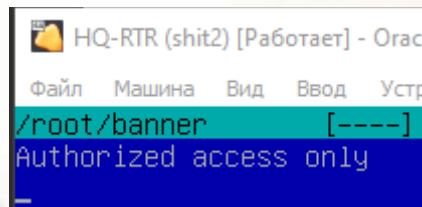
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 22
AllowUsers net_admin
MaxAuthTries 2
PermitRootLogin no
```

Ну и также можно создать баннер в **/root/banner**, как тогда у серверов:

**Authorized access only** (не забываем ENTER после этого предложения)



Ну и вернёмся в конфиг, внесем в строку с баннером путь до нашего файла:

**Banner /root/banner**

```
# no default banner path
Banner /root/banner
```

**systemctl enable --now sshd**

**systemctl restart sshd**

Так как [пользователей](#) на роутерах мы создавали ещё в первом модуле, то можно переходить к следующему этапу.

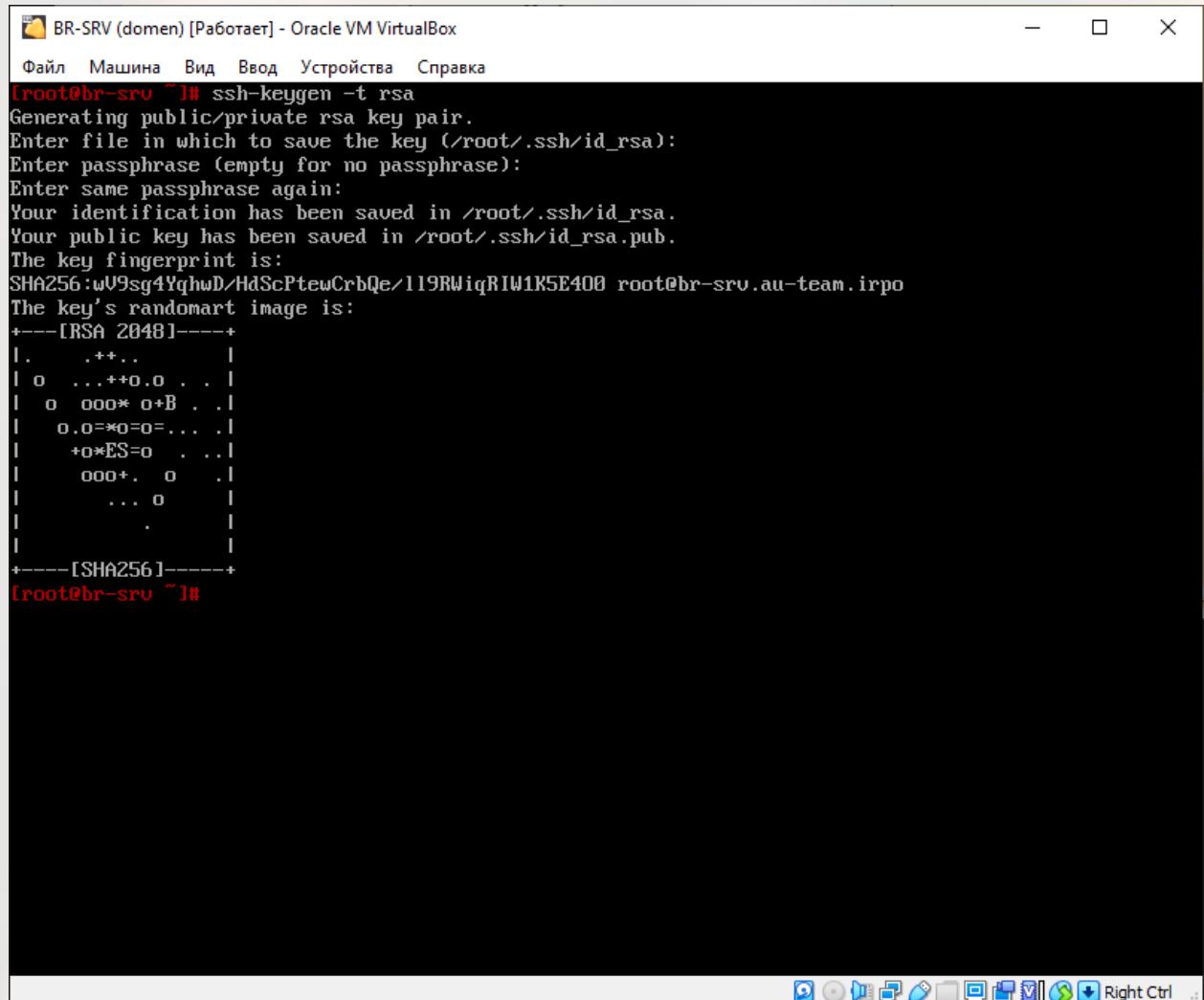
Проделываем тоже самое с [\*\*BR-RTR\*\*](#).

**AUTHORS:**  
NECHAEV  
NAUMOV  
NAGORNOУточните что и на серверах в первом модуле. ([клик](#))

А также настраиваем на нём саму службу **ssh**, как на серверах. ([клик](#))

Теперь на **BR-SRV** генерируем ключи **RSA**, чтобы экспортировать их на машины клиенты, строку с путём и **passphrase** оставляем пустой:

## ssh-keygen -t rsa



```
BR-SRV (domen) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
[root@br-srv ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:wU9sg4YqhwD/HdScPtewCrbQe/119RWiqRIW1K5E400 root@br-srv.au-team.irpo
The key's randomart image is:
+---[RSA 2048]---+
| . .++.. |
| o ...++o.o . . |
| o 000* o+B . . |
| o.o=*=o=o=... . |
| +o*ES=o . . . |
| 000+. o . . |
| ... o . . |
| . . . . |
+---[SHA256]---+
[root@br-srv ~]#
```

Копируем публичный ключ на клиентские машины, первая из них будет **BR-RTR**:

**ssh-copy-id -p 22 net\_admin@192.168.4.1**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```

alhome.zapto.org:7015 QEMU (BR-SRV) - noVNC
[root@br-srv apt]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:WUyF1b0/ZItJaX+XoBo0eCQhsj9ZF3EC76XX6Yj1Yg root@br-srv.au-team.ipro
The key's randomart image is:
+---[RSA 2048]---+
| . o . +*** |
| o o 0.+o. |
| = * +o. |
| + +.o |
| S o +o. |
| E o ***+. |
| . .o+*ooo! |
| . .ooo+.o! |
| ..+ . .! |
+---[SHA256]---+
[root@br-srv apt]# ssh-copy-id -p 22 net_admin@192.168.4.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.4.1 (192.168.4.1)' can't be established.
ED25519 key fingerprint is SHA256:TXHuuy3VJZ3CPae4YueRLkFhk8e+E1ucPfiY8Z0sWHRc.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
Authorized acces only!
net_admin@192.168.4.1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p '22' 'net_admin@192.168.4.1'"
and check to make sure that only the key(s) you wanted were added.

[root@br-srv apt]# -

```

Проделываем для остальных клиентов (**HQ-CLI**, **HQ-SRV**, **HQ-RTR**):

**ssh-copy-id -p 2024 sshuser@192.168.2.5** (Но у вас может быть другой IP, т.к. адрес он получает по DHCP)

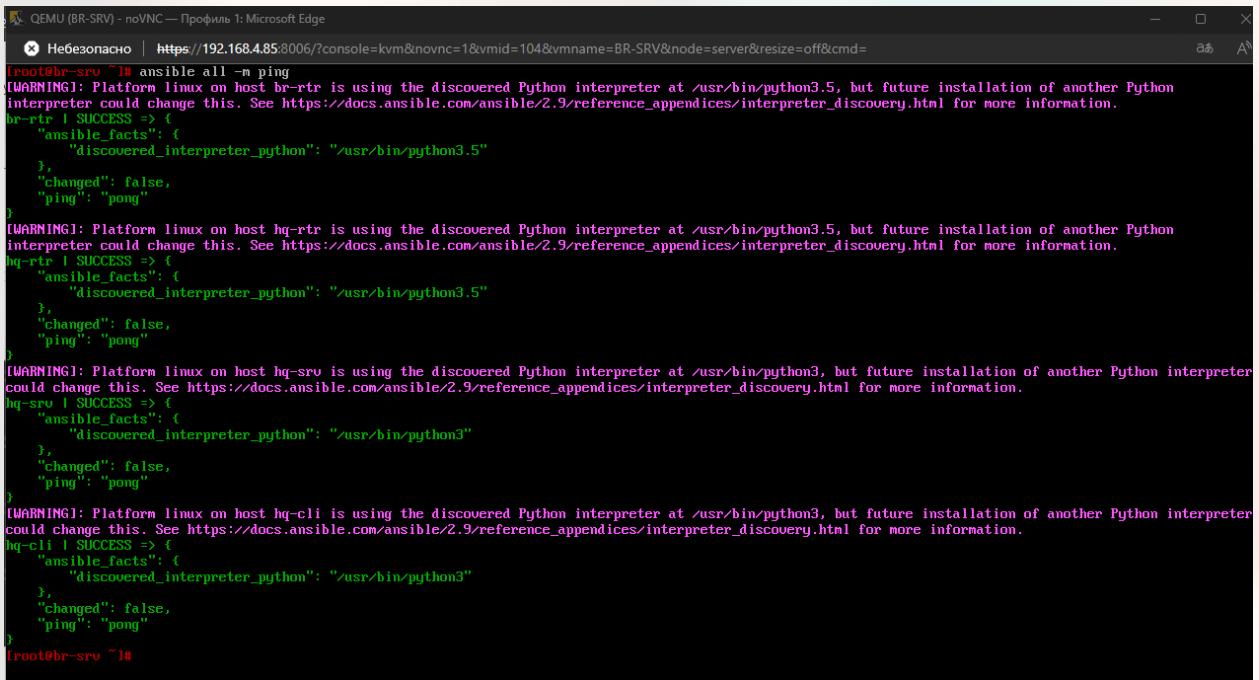
**ssh-copy-id -p 2024 sshuser@192.168.1.2**

**ssh-copy-id -p 22 net\_admin@192.168.1.1**

После этого мы можем проверить связь. Машины должны без предупреждений и ошибок отвечать **pong** на команду **ping** в **ansible** посланную с **BR-SRV**:

**ansible all -m ping**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge  
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=104&vmname=BR-SRV&node=server&resize=off&cmd=  
[root@br-srv ~]# ansible all -m ping  
[WARNING]: Platform linux on host br-rtr is using the discovered Python interpreter at /usr/bin/python3.5, but future installation of another Python interpreter could change this. See https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information.  
br-rtr | SUCCESS => {  
 "ansible\_facts": {  
 "discovered\_interpreter\_python": "/usr/bin/python3.5"  
 },  
 "changed": false,  
 "ping": "pong"  
}  
[WARNING]: Platform linux on host hq-rtr is using the discovered Python interpreter at /usr/bin/python3.5, but future installation of another Python interpreter could change this. See https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information.  
hq-rtr | SUCCESS => {  
 "ansible\_facts": {  
 "discovered\_interpreter\_python": "/usr/bin/python3.5"  
 },  
 "changed": false,  
 "ping": "pong"  
}  
[WARNING]: Platform linux on host hq-srv is using the discovered Python interpreter at /usr/bin/python3, but future installation of another Python interpreter could change this. See https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information.  
hq-srv | SUCCESS => {  
 "ansible\_facts": {  
 "discovered\_interpreter\_python": "/usr/bin/python3"  
 },  
 "changed": false,  
 "ping": "pong"  
}  
[WARNING]: Platform linux on host hq-cli is using the discovered Python interpreter at /usr/bin/python3, but future installation of another Python interpreter could change this. See https://docs.ansible.com/ansible/2.9/reference\_appendices/interpreter\_discovery.html for more information.  
hq-cli | SUCCESS => {  
 "ansible\_facts": {  
 "discovered\_interpreter\_python": "/usr/bin/python3"  
 },  
 "changed": false,  
 "ping": "pong"  
}  
[root@br-srv ~]#

Задание выполнено.

## 5. Развёртывание приложений в Docker на сервере BR-SRV.

Перед настройкой нам необходимо обновить список пакетов и установить docker-engine и docker-compose:

**apt-get update**

**apt-get install docker-engine docker-compose**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

QEMU (BR-SRV) - noVNC — Профиль 1: Microsoft Edge

Небезопасно | <https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=104&vmname=BR-SRV&node=server>

```
[root@br-srv ~]# apt-get update
Get:1 http://ftp.altlinux.org p10/branch/x86_64 release [4223B]
Get:2 http://altrepo.ru noarch release [1094B]
Get:3 http://ftp.altlinux.org p10/branch/x86_64-i586 release [1665B]
Get:4 http://ftp.altlinux.org p10/branch/noarch release [2844B]
Fetched 9826B in 0s (25.9kB/s)
Hit http://altrepo.ru noarch/local-p10 pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64/classic pkglist
Hit http://altrepo.ru noarch/local-p10 release
Hit http://ftp.altlinux.org p10/branch/x86_64/classic release
Hit http://ftp.altlinux.org p10/branch/x86_64/gostcrypto pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64/gostcrypto release
Hit http://ftp.altlinux.org p10/branch/x86_64-i586/classic pkglist
Hit http://ftp.altlinux.org p10/branch/x86_64-i586/classic release
Hit http://ftp.altlinux.org p10/branch/noarch/classic pkglist
Hit http://ftp.altlinux.org p10/branch/noarch/classic release
Reading Package Lists... Done
Building Dependency Tree... Done
[root@br-srv ~]# apt-get install docker-engine docker-compose
Reading Package Lists... Done
Building Dependency Tree... Done
Selecting docker-compose-v2 for 'docker-compose'
The following extra packages will be installed:
  containerd docker-buildx docker-cli docker-compose-v2 docker-proxy runc tini
The following NEW packages will be installed:
  containerd docker-buildx docker-cli docker-compose-v2 docker-engine docker-proxy runc tini
0 upgraded, 8 newly installed, 0 removed and 131 not upgraded.
Need to get 109MB of archives.
After unpacking 428MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

И запустим службу docker:

**systemctl enable --now docker**

**systemctl status docker**

```
[root@br-srv ~]# systemctl enable --now docker
Synchronizing state of docker.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.
[root@br-srv ~]# systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-11-18 12:18:40 +07; 6s ago
     TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
    Main PID: 17364 (dockerd)
      Tasks: 9
     Memory: 25.7M
        CPU: 638ms
      CGroup: /system.slice/docker.service
              └─ 17364 /usr/bin/dockerd --containerd /run/containerd/containerd.sock --exec-opt native.cgo

Nov 18 12:18:35 br-srv.au-team.irpo systemd[1]: Starting Docker Application Container Engine...
Nov 18 12:18:35 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:35.588472740+07:00" level=info
Nov 18 12:18:35 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:35.937867021+07:00" level=info
Nov 18 12:18:37 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:37.475534884+07:00" level=info
Nov 18 12:18:39 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:39.041118865+07:00" level=info
Nov 18 12:18:39 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:39.853622086+07:00" level=warning
Nov 18 12:18:39 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:39.854529335+07:00" level=info
Nov 18 12:18:39 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:39.855273000+07:00" level=info
Nov 18 12:18:40 br-srv.au-team.irpo dockerd[17364]: time="2024-11-18T12:18:40.873702660+07:00" level=info
Nov 18 12:18:40 br-srv.au-team.irpo systemd[1]: Started Docker Application Container Engine.
```

Активация Windows

Загружаем образы следующей командой:

```
docker pull mediawiki
```

```
docker pull mariadb
```

```
[root@br-srv ~]# docker pull mediawiki
Using default tag: latest
latest: Pulling from library/mediawiki
2d429b9e73a6: Pull complete
b6bdded20f71: Pull complete
1597d7096267: Pull complete
43ab2d6ba4d8: Pull complete
accc5831bae2: Pull complete
40aee99de06f: Pull complete
9dbb6269a533: Pull complete
5437219f2ae2: Pull complete
ef68bb5b2da8: Pull complete
925ee9570811: Pull complete
70b140214414: Pull complete
5ef09f350653: Pull complete
3b3b0ecbf64c: Pull complete
4f4fb700ef54: Pull complete
cf0714095e17: Pull complete
55c066b61e8a: Pull complete
273583bebef5: Pull complete
ce16e9bdd3fe: Pull complete
9aa3bf771837: Pull complete
c7a30b96f8b1: Pull complete
562559a8fe68: Pull complete
Digest: sha256:eda2934a768a89903d0e9698bd1c1e0c48af52e8484a53d153e70d077f304ae1
Status: Downloaded newer image for mediawiki:latest
docker.io/library/mediawiki:latest
```

```
[root@br-srv ~]# docker pull mariadb
Using default tag: latest
latest: Pulling from library/mariadb
afad30e59d72: Pull complete
51dd17487841: Pull complete
2c73bf457d06: Pull complete
e45aad49aaa1: Pull complete
1c10d4792e4a: Pull complete
c4fe613b36f7: Pull complete
dc087a037fc5: Pull complete
325ea7d8633e: Pull complete
Digest: sha256:2d50fe0f77dac919396091e527e5e148a9de690e58f32875f113bef6506a17f5
Status: Downloaded newer image for mariadb:latest
docker.io/library/mariadb:latest
[root@br-srv ~]# _
```

Создаем в домашней директории пользователя файл, в качестве пользователя,

AUTHORS, которого мы создавали при установке ОС, у нас – **user**, а его домашний каталог

NECHAEV – **/home/user**, файл называется – **wiki.yml**, для приложения MediaWiki:

NAUMOV

NAGORNOVA

```
mcedit /home/user/wiki.yml
```

И заполняем его следующими строками, обратите внимание, что в строках ПРОБЕЛЫ, А НЕ ТАБУЛЯЦИЯ:

services:

**mariadb:**

**image: mariadb**

**container\_name: mariadb**

**restart: always**

**environment:**

**MYSQL\_ROOT\_PASSWORD: 123qweR%**

**MYSQL\_DATABASE: mediawiki**

**MYSQL\_USER: wiki**

**MYSQL\_PASSWORD: WikiP@ssw0rd**

**volumes: [ mariadb\_data:/var/lib/mysql ]**

**wiki:**

**image: mediawiki**

**container\_name: wiki**

**restart: always**

**environment:**

**MEDIAWIKI\_DB\_HOST: mariadb**

**MEDIAWIKI\_DB\_USER: wiki**

**MEDIAWIKI\_DB\_PASSWORD: WikiP@ssw0rd**

**MEDIAWIKI\_DB\_NAME: mediawiki**

**ports:**

**- "8080:80"**

**#volumes: [ /home/user/mediawiki/LocalSettings.php:/var/www/html/LocalSettings.php ]**

**volumes:**

**mariadb\_data:**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```

althome.zapto.org:7015 QEMU (BR-SRV) - noVNC
wiki.yml [-M--] 36 L:I 1+22 23/ 251 *(572 / 649b) 0047 0x02F
services:
  mariadb:
    image: mariadb
    container_name: mariadb
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: 123queRz
      MYSQL_DATABASE: mediawiki
      MYSQL_USER: wiki
      MYSQL_PASSWORD: WikiP@ssw0rd
    volumes: [ mariadb_data:/var/lib/mysql ]
  wiki:
    image: mediawiki
    container_name: wiki
    restart: always
    environment:
      MEDIAWIKI_DB_HOST: mariadb
      MEDIAWIKI_DB_USER: wiki
      MEDIAWIKI_DB_PASSWORD: WikiP@ssw0rd
      MEDIAWIKI_DB_NAME: mediawiki
    ports:
      - "8080:80"
    #volumes: [ /home/user/mediawiki/_LocalSettings.php:/var/www/html/_LocalSettings.php ]
  volumes:
    mariadb_data:

```

После всех настроек строку **volumes..** мы обратно раскомментируем, убрав символ #!

Приступаем к запуску контейнера **wiki.yml**, в зависимости от версии compose, существует ещё одна запись, она для второй его версии:

Обычная версия:

**docker-compose -f /home/user/wiki.yml up -d**

Вторая версия:

**docker compose -f /home/user/wiki.yml up -d**

```

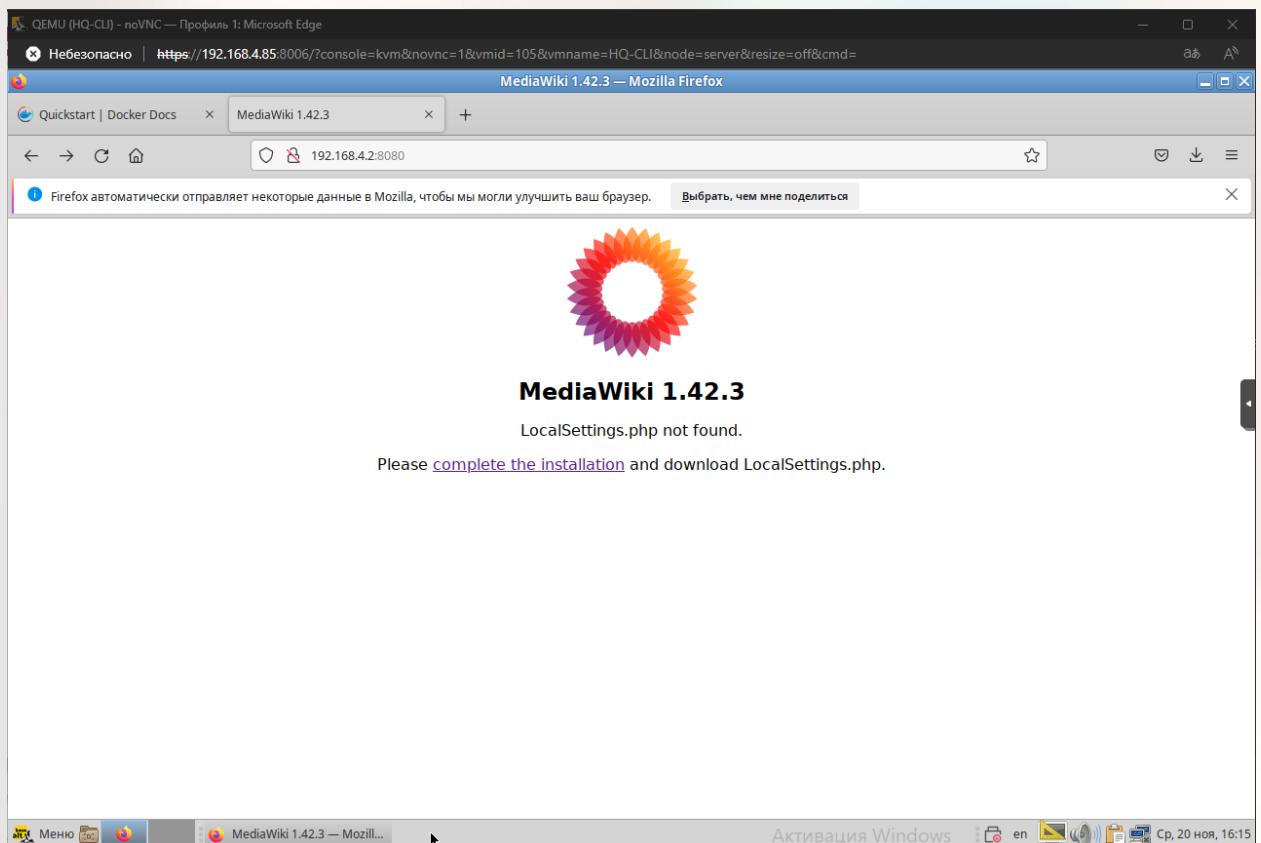
[root@br-srv ~]# docker compose -f /home/user/wiki.yml up -d
[+] Running 4/4
 ? Network user_default      Created
 ? Volume "user_mariadb_data" Created
 ? Container wiki             Started
 ? Container mariadb          Started

```

AUTHORS  
NECHAEV

NAUMOV  
NAGORNOVA

Заходим с клиента **HQ-CLI** на сайт после запуска контейнера:



Видим, что файл **LocalSettings.php** не найден, и нажимаем на **complete the installation** или **set up the wiki**.

Выбираем удобный для вас язык:

Установка MediaWiki 1.42.3

**Язык**

Ваш язык:  
справка  
ru - русский

Язык, который будет использовать вики:  
справка  
ru - русский

[Далее →](#)

**• Язык**  
• Существующая вики  
• Добро пожаловать в MediaWiki!  
• Подключение к базе данных  
• Обновление существующей установки  
• Настройки базы данных  
• Название  
• Настройки  
• Установка  
• Готово!

Здесь просто идём далее:

The screenshot shows a Firefox browser window with the URL <https://192.168.4.2:8080/mw-config/index.php?page=Welcome>. The page title is "Установка MediaWiki 1.42.3". The main content area displays the "Добро пожаловать в MediaWiki!" (Welcome to MediaWiki!) message. Below it, the "Проверка окружения" (Environment check) section lists three items: "Установленная версия PHP: 8.1.30.", "ICU 72.1 установлен (поддерживает Unicode 15.0.0.)", and "Обнаружен ImageMagick: /usr/bin/convert". To the right, a sidebar titled "Добро пожаловать в MediaWiki!" contains a list of setup steps: Язык, Существующая вики, Подключение к базе данных, Обновление существующей установки, Настройки базы данных, Название, Настройки, Установка, and Готово!. At the bottom of the sidebar is a link to "Начать установку заново". The browser's address bar shows "192.168.4.2:8080/mw-config/index.php?page=Welcome". The taskbar at the bottom includes icons for "Меню", "Файл", "Firefox", and "Установка MediaWiki 1.42...".

Видим строки, которые нужно заполнить:

Хост базы данных:

**mariadb**

Имя базы данных (без дефисов):

**mediawiki**

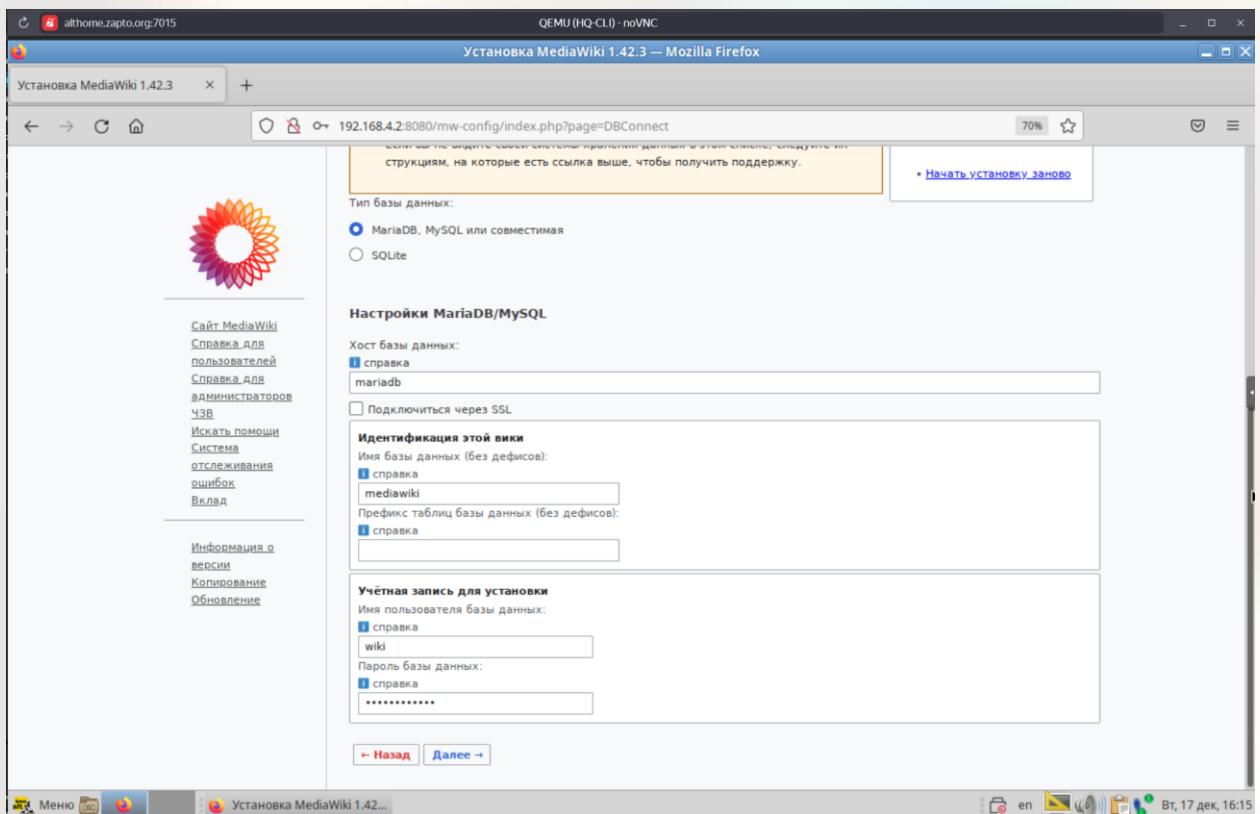
Имя пользователя базы данных:

**wiki**

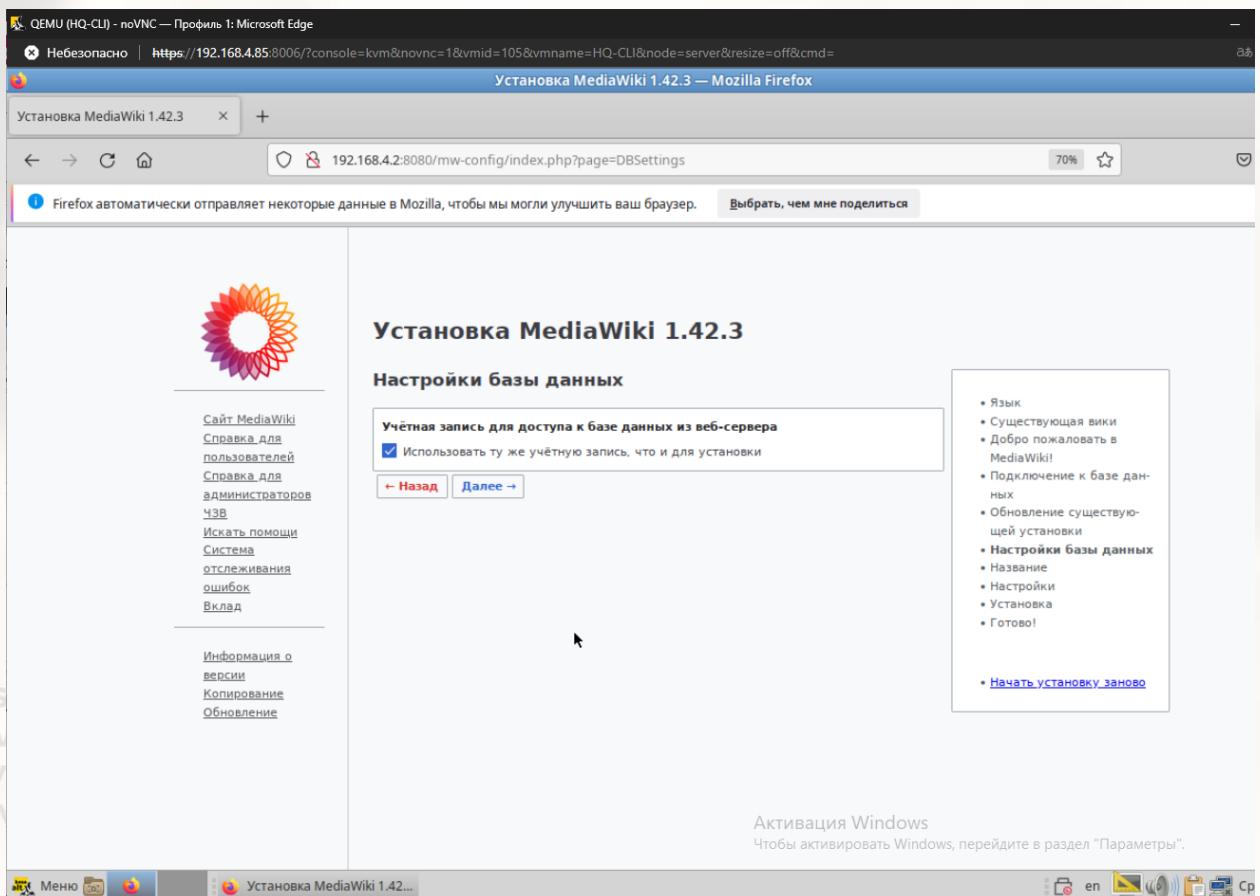
Пароль базы данных:

**WikiP@ssw0rd**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Прожимаем Далее, оставляя всё как есть:



Пишем в строках следующее и выбираем пункты, как на скрине:

Название вики:

link community - <https://t.me/sysdemocommunity>

**cock** (можно своё название)

Ваше имя участника:

**wiki**

Пароль:

**WikiP@ssw0rd**

QEMU (HQ-CLI) - noVNC — Профиль 1: Microsoft Edge

Небезопасно | <https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=105&vname=HQ-CLI&node=server&resize=off&cmd=>

Установка MediaWiki 1.42.3 — Mozilla Firefox

Установка MediaWiki 1.42.3

Firefox автоматически отправляет некоторые данные в Mozilla, чтобы мы могли улучшить ваш браузер. Выбрать, чем мне поделиться

Название вики:  
справка  
cock

Пространство имён проекта:  
справка  
То же, что и имя вики: Cock

Проект  
Другое (указать)

Учётная запись администратора

Ваше имя участника:  
справка  
wiki

Пароль:  
Пароль: Пароль ещё раз:

Адрес электронной почты:  
справка

Подписаться на рассылку новостей о появлении новых версий MediaWiki.

Поделиться сведениями об этой установке с разработчиками MediaWiki.

Информация  
Вы почти у цели! Остальные настройки можно пропустить и приступить к установке вики.

Произвести тонкую настройку  
Хватит уже, просто установите вики.

Назад Далее >

Активация Windows  
Чтобы активировать Windows, перейдите в раздел «Активация»

Нажимаем **Далее**:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

The screenshot shows the MediaWiki 1.42.3 installation page. At the top, there's a navigation bar with links for 'Установка MediaWiki 1.42.3' and 'Вы chọn, чем мне поделиться'. Below the navigation bar, a message from Mozilla states: 'Firefox автоматически отправляет некоторые данные в Mozilla, чтобы мы могли улучшить ваш браузер.' A link 'Выбрать, чем мне поделиться' is also present.

The main content area has a title 'Установка MediaWiki 1.42.3' and a sub-section 'Установка'. It contains an information box with a warning icon: 'Информация' and the text: 'Нажав «Далее >», вы начнёте установку MediaWiki. Если вы хотите внести изменения, нажмите «← Назад».' Below this are two buttons: '← Назад' and 'Далее >'. To the right of the main content is a sidebar with a list of steps:

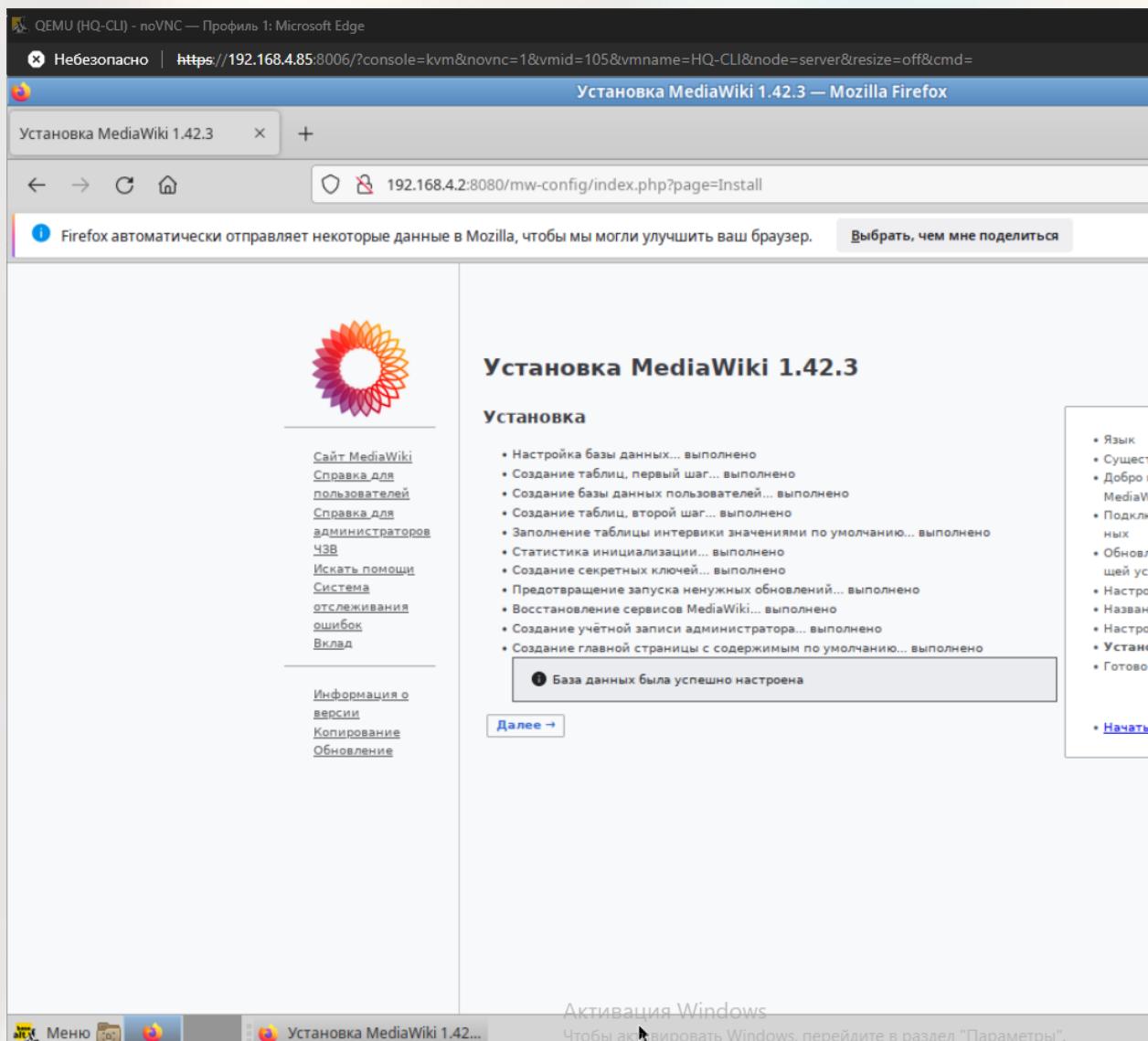
- Язык
- Существующая вики
- Добро пожаловать в MediaWiki!
- Подключение к базе данных
- Обновление существующей установки
- Настройки базы данных
- Название
- Настройки
- Установка
- Готово!

At the bottom of the sidebar is a link: 'Начать установку заново'.

The browser status bar at the bottom shows: 'Меню' (Menu), 'Установка MediaWiki 1.42...', 'Активация Windows' (Windows Activation), and 'ru' (Russian).

И вот мы успешно создали базу данных:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Далее автоматически скачивается файл **LocalSettings.php**, который нужно переместить теперь на сервер с **mediawiki**, а именно на **BR-SRV** с **HQ-CLI**:

**scp -P 2024 /home/user/**(смотрите под каким пользователем вы авторизовались до настройки)**/Загрузки/LocalSettings.php**  
**sshuser@192.168.4.2:/home/sshuser/**

```
user@hq-cli ~ $ scp -P 2024 /home/user/Загрузки/LocalSettings.php sshuser@192.168.4.2:/home/sshuser/
Authorized access only
sshuser@192.168.4.2's password:
```

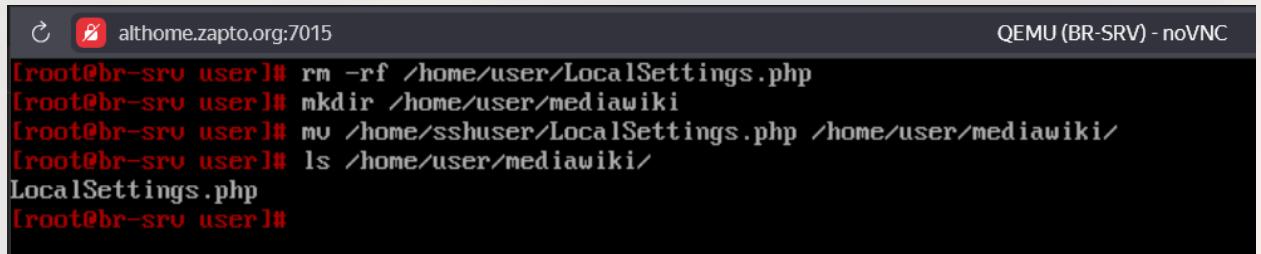
Теперь заходим на сервер **BR-SRV** и перемещаем скачанный файл в **/root**, но перед этим удаляем то, что создалось в **/root** (могло и не создаваться, так даже лучше):

**rm -rf /home/user/LocalSettings.php**

```
mkdir /home/user/mediawiki
```

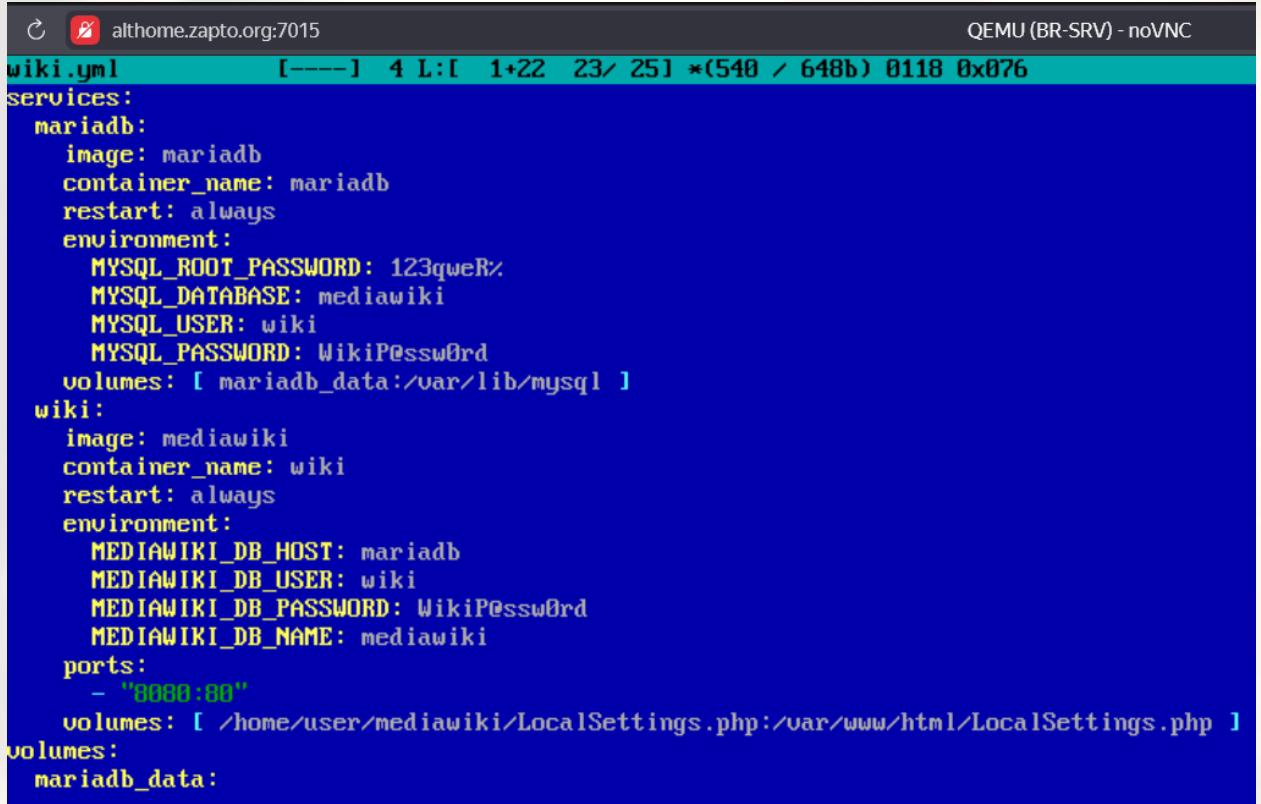
```
mv /home/sshuser/LocalSettings.php /home/mediawiki/
```

```
ls /home/user/mediawiki/
```



```
[root@br-srv user]# rm -rf /home/user/LocalSettings.php
[root@br-srv user]# mkdir /home/user/mediawiki
[root@br-srv user]# mv /home/sshuser/LocalSettings.php /home/user/mediawiki/
[root@br-srv user]# ls /home/user/mediawiki/
LocalSettings.php
[root@br-srv user]#
```

Раскомментируем, как и говорили ранее, строку **volumes**...:



```
wiki.yml      [----] 4 L:[ 1+22 23/ 25] *(540 / 648b) 0118 0x076
services:
  mariadb:
    image: mariadb
    container_name: mariadb
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: 123qweR%
      MYSQL_DATABASE: mediawiki
      MYSQL_USER: wiki
      MYSQL_PASSWORD: WikiP@ssw0rd
    volumes: [ mariadb_data:/var/lib/mysql ]
  wiki:
    image: mediawiki
    container_name: wiki
    restart: always
    environment:
      MEDIAWIKI_DB_HOST: mariadb
      MEDIAWIKI_DB_USER: wiki
      MEDIAWIKI_DB_PASSWORD: WikiP@ssw0rd
      MEDIAWIKI_DB_NAME: mediawiki
    ports:
      - "8080:80"
    volumes: [ /home/user/mediawiki/LocalSettings.php:/var/www/html/LocalSettings.php ]
volumes:
  mariadb_data:
```

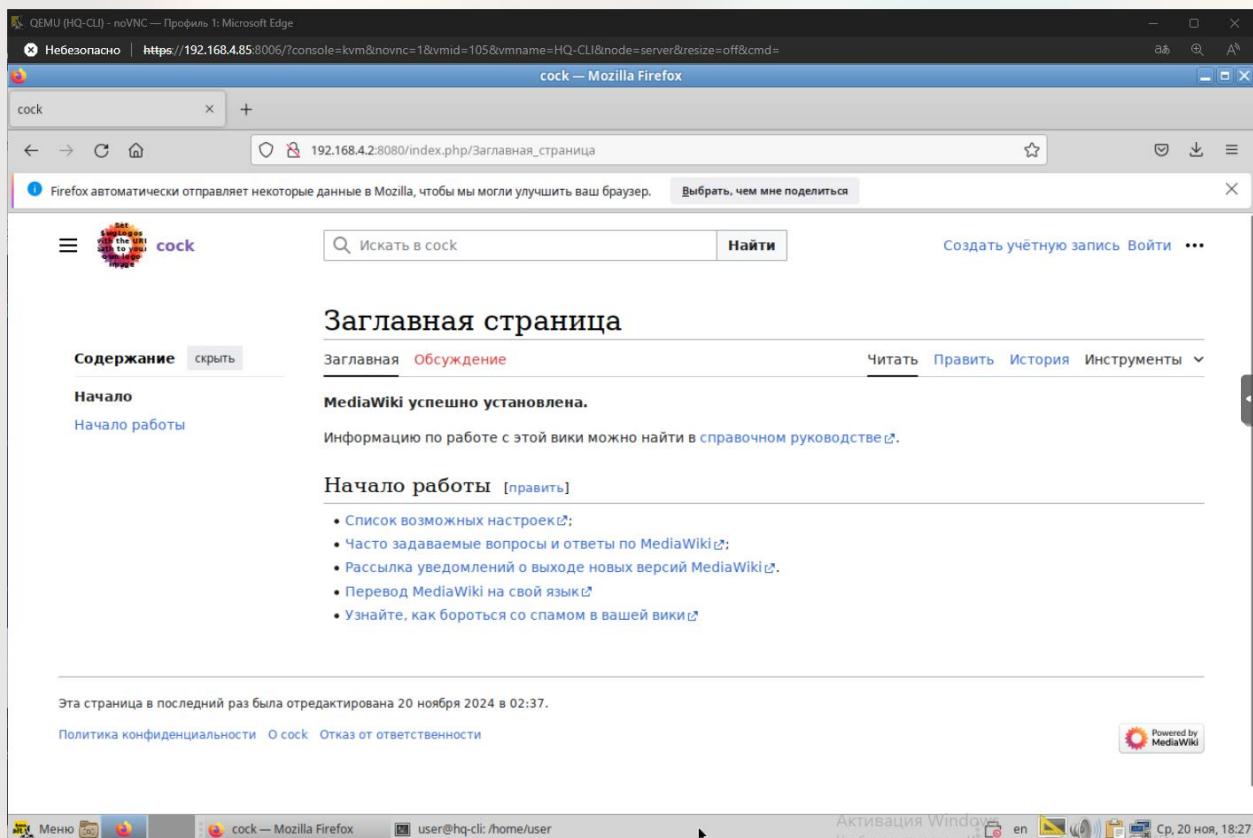
Теперь перезапускаем контейнеры путём запуска контейнера ещё раз:

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



```
[root@br-srv user]# docker compose -f wiki.yml up -d
AUTHORS
[+] Running 2/2
NECHAEV
NAUMOV
NAGORNOY
? Container mariadb  Running
? Container wiki    Started
[root@br-srv user]#
```

Проверим работу сайта, зайдем вновь через клиента **HQ-CLI** и увидим домашнюю страницу сайта:



## 6. На маршрутизаторах сконфигурируйте статическую трансляцию портов

Пробросим порт **80** в порт **8080** и порт **2024** в порт **2024** на **BR-SRV** на маршрутизаторе **BR-RTR**, для обеспечения работы сервиса **mediawiki** и **ssh**, правила прописываем через консоль:

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.4.1 --dport 80 -j DNAT --to-destination 192.168.4.2:8080
iptables -t nat -A PREROUTING -p tcp -d 192.168.4.1 --dport 2024 -j DNAT --to-destination 192.168.4.2:2024
```

```
althome.zapto.org:7015 QEMU (BR-RTR) - noVNC
root@br-rtr:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.4.1 --dport 80 -j DNAT --to-destination 192.168.4.2:8080
root@br-rtr:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.4.1 --dport 2024 -j DNAT --to-destination 192.168.4.2:2024
root@br-rtr:~# _
```

Сохраняем правила, не забывайте, что у вас уже есть правила, которые мы писали ещё в первом модуле, проверьте, чтобы в этом файле сохранялись и прошлые, и новые (которые мы сейчас ввели):

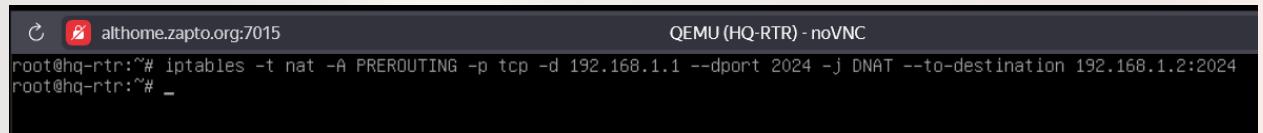
**iptables-save > /root/rules**

```
althome.zapto.org:7015 QEMU (BR-RTR) - noVNC
root@br-rtr:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.4.1 --dport 80 -j DNAT --to-destination 192.168.4.2:8080
root@br-rtr:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.4.1 --dport 2024 -j DNAT --to-destination 192.168.4.2:2024
root@br-rtr:~# iptables-save > /root/rules
root@br-rtr:~# _
```

Запись в **crontab** делать заново не нужно, т.к. правила и так там выгружаются через **iptables-restore**, который мы делали ещё в первом модуле.

Пробросим порт **2024** в порт **2024** на **HQ-SRV** на маршрутизаторе **HQ-RTR**, для обеспечения работы сервиса ssh, правило прописываем через консоль:

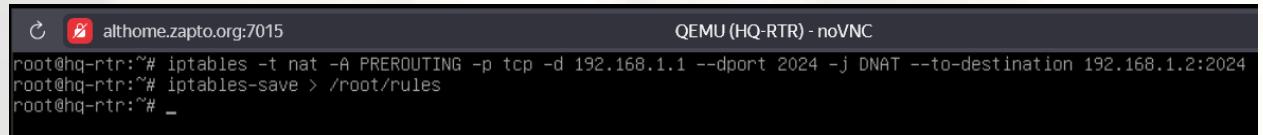
```
iptables -t nat -A PREROUTING -p tcp -d 192.168.1.1 --dport 2024 -j DNAT -  
-to-destination 192.168.1.2:2024
```



```
alithome.zapto.org:7015 QEMU (HQ-RTR) - noVNC  
root@hq-rtr:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.1.1 --dport 2024 -j DNAT --to-destination 192.168.1.2:2024  
root@hq-rtr:~# _
```

Сохраняем правила, не забывайте, что у вас уже есть правила, которые мы писали ещё в первом модуле, проверьте, чтобы в этом файле сохранялись и прошлые, и новое (которое мы сейчас ввели):

```
iptables-save > /root/rules
```



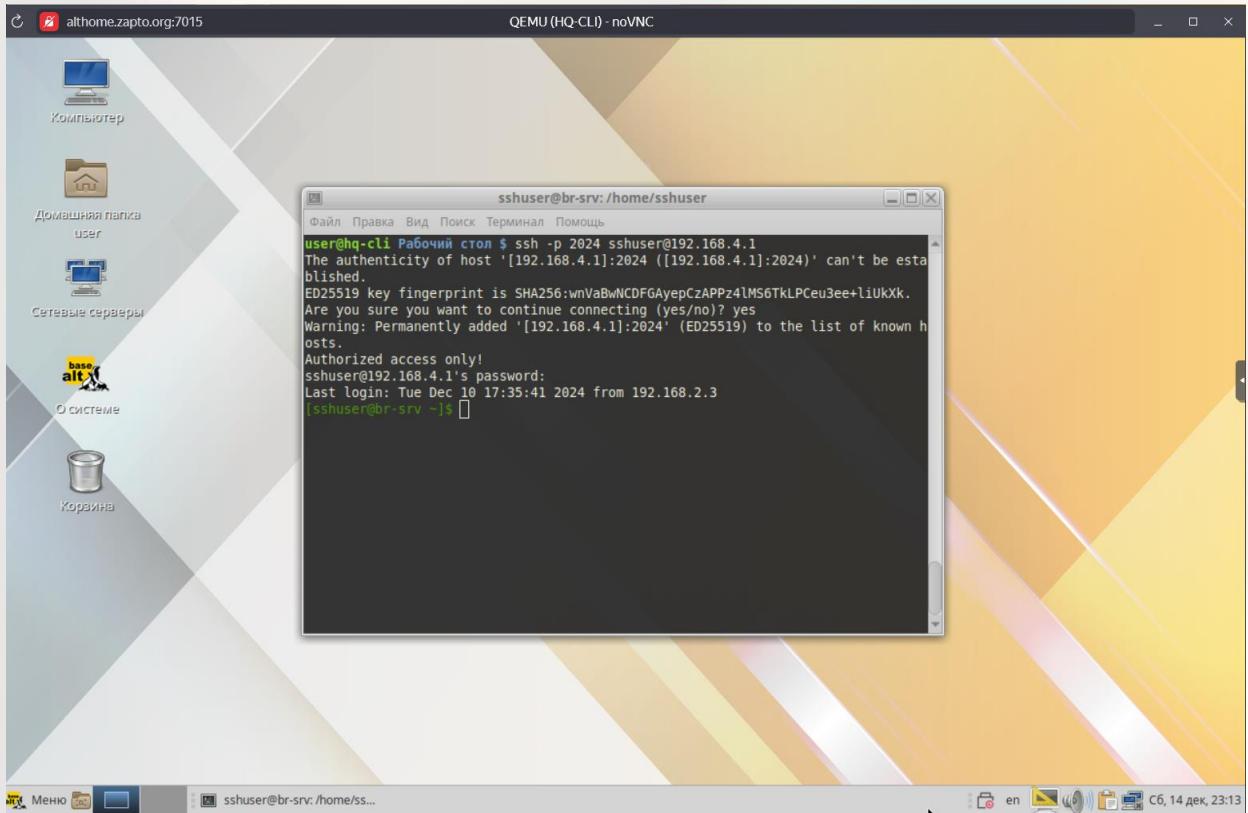
```
alithome.zapto.org:7015 QEMU (HQ-RTR) - noVNC  
root@hq-rtr:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.1.1 --dport 2024 -j DNAT --to-destination 192.168.1.2:2024  
root@hq-rtr:~# iptables-save > /root/rules  
root@hq-rtr:~# _
```

Запись в **crontab** делать заново не нужно, т.к. правила и так там выгружаются через **iptables-restore**, который мы делали ещё в первом модуле.

Теперь перезагружаем ОБА роутера и проверим правила путём подключения с клиента **HQ-CLI** по **ssh** к серверу **BR-SRV** через IP-адрес роутера **BR-RTR**:

```
ssh -p 2024 sshuser@192.168.4.1
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



Вуаля, всё успешно!

## 7. Запустите сервис moodle на сервере HQ-SRV

Устанавливаем для ряд пакетов, которые будут нам нужны для работы:

**apt-get update**

```
apt-get install apache2 php8.2 apache2-mod_php8.2 mariadb-server php8.2-  
opcache php8.2-curl php8.2-gd php8.2-intl php8.2-mysqli php8.2-xml php8.2-  
xmlrpc php8.2-ldap php8.2-zip php8.2-soap php8.2-mbstring php8.2-json  
php8.2-xmlreader php8.2-fileinfo php8.2-sodium
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```
[root@hq-srv ~]# apt-get install apache2 php8.2 apache2-mod_php8.2 mariadb-server php8.2-opcache php8.2-curl php8.2-gd php8.2-intl php8.2-mysqli php8.2-xml php8.2-xmlrpc php8.2-ldap php8.2-zip php8.2-soap php8.2-mbstring php8.2-json php8.2-xmlreader php8.2-fileinfo php8.2-sodium
Reading Package Lists... Done
Building Dependency Tree... Done
Selecting php8.2-mysqlnd-mysqli for 'php8.2-mysqli'
Selecting php8.2-libs for 'php8.2-xml'
Selecting php8.2-libs for 'php8.2-json'
The following extra packages will be installed:
apache2-ab apache2-base apache2-cgi apache2-cgi-bin-printenv apache2-cgi-bin-test-cgi
apache2-datalists apache2-htcacheclean apache2-htcacheclean-control apache2-html apache2-htpasswd
apache2-httpd-prefork apache2-httpd-worker apache2-icons apache2-mod_cache_disk apache2-mods
condstopstart-common condstopstart-web curl libapr1 libaprutil1 libcurl libdb4.8 libmariadb3
libmm liboniguruma5 libsodium23 libzip5 mariadb-client mariadb-common mariadb-server-control
numactl perl-DBM php-base php8.2-libs php8.2-mysqlnd php8.2-mysqlnd-mysqli php8.2-openssl
webserver-cgi-bin-control webserver-common webserver-common-control
The following packages will be upgraded
curl libcurl
The following NEW packages will be installed:
apache2 apache2-ab apache2-base apache2-cgi apache2-cgi-bin apache2-cgi-bin-printenv
apache2-cgi-bin-test-cgi apache2-datalists apache2-htcacheclean apache2-htcacheclean-control
apache2-html apache2-htpasswd apache2-httpd-prefork apache2-httpd-worker apache2-icons
apache2-mod_cache_disk apache2-mod_php8.2 apache2-mods condstopstart-common condstopstart-web
libapr1 libaprutil1 libdb4.8 libmariadb3 libmm liboniguruma5 libsodium23 libzip5 mariadb-client
mariadb-common mariadb-server mariadb-server-control numactl perl-DBM php-base php8.2
php8.2-curl php8.2-fileinfo php8.2-gd php8.2-intl php8.2-ldap php8.2-libs php8.2-mbstring
php8.2-mysqlnd php8.2-mysqlnd-mysqli php8.2-opcache php8.2-openssl php8.2-soap php8.2-sodium
php8.2-xmlreader php8.2-xmlrpc php8.2-zip webserver-cgi-bin-control webserver-common
webserver-common-control
2 upgraded, 54 newly installed, 0 removed and 289 not upgraded.
Need to get 24.6MB of archives.
After unpacking 219MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Включаем службы **httpd2** и **mysqld** для дальнейшей работы с ними следующей командой:

**systemctl enable –now httpd2 mysqld**

```
[root@hq-srv ~]# systemctl enable --now httpd2 mysqld
Synchronizing state of httpd2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable httpd2
Synchronizing state of mysqld.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mysqld
Created symlink /etc/systemd/system/multi-user.target.wants/httpd2.service → /lib/systemd/system/httpd2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mysqld.service → /lib/systemd/system/mysqld.service.
[root@hq-srv ~]#
```

Теперь настроим безопасный доступ к нашей будущей базе данных с помощью команды:

**mysql\_secure\_installation**

Прожимаем просто **enter**, т.к. сейчас **root** без пароля:

**Enter**

Прожимаем **у** для задания пароля:

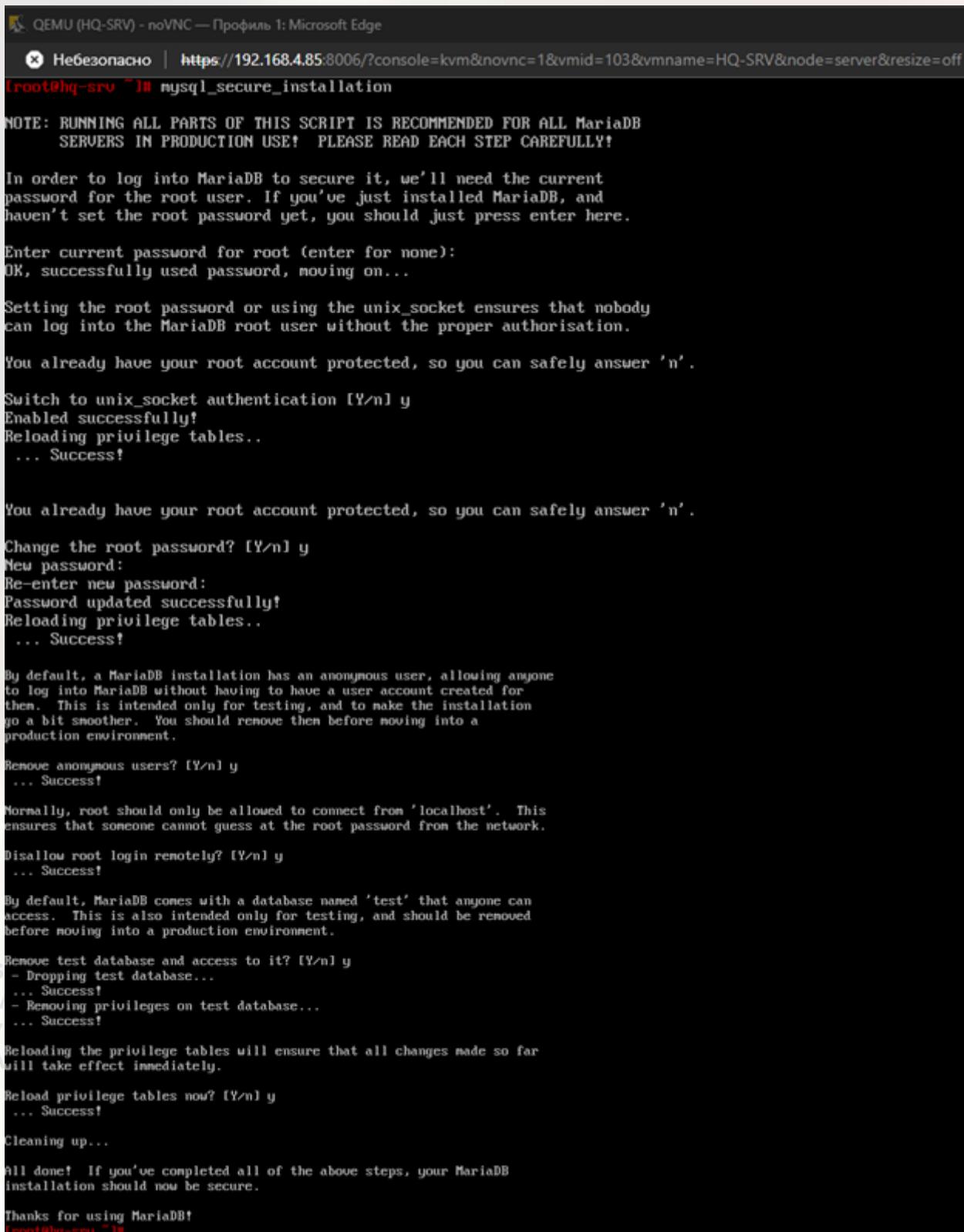
**Y**

Задаем пароль к нашему **root**, желательно стандартный:

**123qweR%**

Далее нажимаем на всё **y**, как на скриншоте:

**Y**



```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=103&vmname=HQ-SRV&node=server&resize=off
root@hq-srv ~]# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] y
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
(root@hq-srv ~]#
```

Теперь заходим в СУБД для создания и настройки базы данных:

```
mariadb -u root -p
```

```
CREATE DATABASE moodledb;
```

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

```
GRANT ALL PRIVILEGES ON moodledb.* TO moodle;
```

```
FLUSH PRIVILEGES;
```

```
exit
```

```
[root@hq-srv nfs]# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 14
Server version: 10.6.20-MariaDB-alt1 (ALT p10)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE moodledb;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> CREATE USER moodle IDENTIFIED BY 'P@ssw0rd';
Query OK, 0 rows affected (0.022 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON moodledb.* TO moodle;
Query OK, 0 rows affected (0.023 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> exit
Bye
[root@hq-srv nfs]#
```

Теперь скачаем сам модуль стабильной версии:

```
curl -L https://github.com/moodle/moodle/archive/refs/tags/v4.5.0.zip >
/root/moodle.zip
```

```
AUTHORS:
NECHAEV
NAUMOV
NAGORNOV
[root@hq-srv ~]# curl -L https://github.com/moodle/moodle/archive/refs/tags/v4.5.0.zip > /root/moodle.zip
  % Total    % Received  % Xferd  Average Speed   Time     Time      Current
               Dload  Upload Total   Spent    Left Speed
  0    0    0    0    0    0    0    0 --:--:-- --:--:-- --:--:--   0
100 92.0M  0 92.0M    0    0  6486k      0 --:--:--  0:00:14 --:--:-- 7044k
[root@hq-srv ~]# ls
banner moodle.zip tmp
[root@hq-srv ~]#
```

Разархивируем его в **/var/www/html/** для дальнейшей настройки:

```
unzip /root/moodle.zip -d /var/www/html
```

```
mv /var/www/html/moodle-4.5.0/* /var/www/html/
```

```
ls /var/www/html
```

```
inflating: /var/www/html/moodle-4.5.0/webservice/tests/behat/siteadmin_webservice_token_breadcrumbs.feature
inflating: /var/www/html/moodle-4.5.0/webservice/tests/behat/webservice_users.feature
creating: /var/www/html/moodle-4.5.0/webservice/tests/event/
inflating: /var/www/html/moodle-4.5.0/webservice/tests/event/events_test.php
inflating: /var/www/html/moodle-4.5.0/webservice/tests/externallib_test.php
    creating: /var/www/html/moodle-4.5.0/webservice/tests/generator/
inflating: /var/www/html/moodle-4.5.0/webservice/tests/generator/behat_core_webservice_generator.php
inflating: /var/www/html/moodle-4.5.0/webservice/tests/generator/lib.php
inflating: /var/www/html/moodle-4.5.0/webservice/tests/helpers.php
inflating: /var/www/html/moodle-4.5.0/webservice/tests/lib_test.php
inflating: /var/www/html/moodle-4.5.0/webservice/upgrade.txt
inflating: /var/www/html/moodle-4.5.0/webservice/upload.php
inflating: /var/www/html/moodle-4.5.0/webservice/wsdoc.php
[root@hq-srv ~]# ls /var/www/html
addon-modules index.html moodle-4.5.0
[root@hq-srv ~]# mv /var/www/html/moodle-4.5.0/* /var/www/html/
[root@hq-srv ~]# ls /var/www/html
CONTRIBUTING.md analytics calendar course filter iplookup moodlenet pluginfile.php search
COPYING.txt auth cohort customfield grade lang my portfolio security.txt
Grunfile.js availability comment dataformat group lib notes privacy sms
INSTaLL.txt backup communication draftfile.php h5p local npm-shrinkwrap.json question tag
README.md badges competency editmode.php heIp.php login package.json r.php theme
TRADEMARK.txt behat.yml.dist completion enrol heIp_ajax.php media payment rating
UPGRADING.md blocks composer.json error index.html message phpcs.xml.dist report tokenpluginfile.php
addon-modules blog composer.lock favourites index.php mnet phpunit.xml.dist reportbuilder user
admin brokenfile.php config-dist.php file.php install mod pix repository userpix
ai cache contentbank files install.php moodle-4.5.0 plagiarism rss version.php
[root@hq-srv ~]#
```

Создадим новый каталог **moodledata**, там будут храниться данные и изменим владельца на каталогах **html** и **moodledata**:

```
mkdir /var/www/moodledata
```

```
chown apache2:apache2 /var/www/html
```

```
chown apache2:apache2 /var/www/moodledata
```

```
[root@hq-srv ~]# mkdir /var/www/moodledata
[root@hq-srv ~]# chown apache2:apache2 /var/www/html
[root@hq-srv ~]# chown apache2:apache2 /var/www/moodledata
[root@hq-srv ~]#
```

Поменяем значение параметра **max\_input\_vars** в файле **php.ini**:

```
mcedit /etc/php/8.2/apache2-mod_php/php.ini
```

Жмём F7 для поиска нужной нам строки и пишем туда:

```
max_input_vars
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge

Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=103&vname=HQ-SRV&node=server&resize=off

php.ini [---] 0 L: [ 1+ 1 2/12361 \*(6 /47643b) 0010 0x00A [TOP]

```
#####
; About php.ini :
#####
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable. (as of PHP 5.2.0)
; 3. A number of predefined registry keys on Windows (as of PHP 5.2.0)
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path
; Windows directory (C:\windows or C:\wintnt)
; See the PHP docs for more specific information.
; http://php.net/configuration-file

; The syntax of the file is extremely simple. Whitespace
; beginning with a semicolon are silently ignored.
; Section headers (e.g., [FOOB]) are also silently ignored
; they might mean something in the future.

; Directives following the section heading [PATH=www]
; apply to PHP files in the /www/msysite directory.
; following the section heading [HOST=www.example.com]
; PHP files served from www.example.com. Directives set in these
; special sections cannot be overridden by user-defined INI files or
; at runtime. Currently, [PATH=] and [HOST=] sections only work under
; CGI/FastCGI.
; http://php.net/ini.sections

; Directives are specified using the following syntax:
; directive = value
; Directive names are case sensitive - foo=bar is different from FOO=bar.
; Directives are variables used to configure PHP or PHP extensions.
; There is no name validation. If PHP can't find an expected
; directive because it is not set or is mistyped, a default value will be used.

; The value can be a string, a number, a PHP constant (e.g., E_ALL or M_PI), one
; of the INI constants (On, Off, True, False, Yes, No and None) or an expression
; (e.g., E_ALL & ~E_NOTICE), a quoted string ("bar"), or a reference to a
; previously set variable or directive (e.g., ${foo})

; Expressions in the INI file are limited to bitwise operators and parentheses:

```

Search  
Enter search string:  
max\_input\_vars  
(\* ) Normal [ ] Case sensitive  
( ) Regular expression [ ] Backwards  
( ) Hexadecimal [ ] In selection  
( ) Wildcard search [ ] Whole words  
[ ] All charsets  
OK Find all Cancel

Help Save Mark Replace Copy Move Search Delete PullDn Quit

Раскомментируем и пишем новое значение:

**max\_input\_vars = 5000**

QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge

Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=103&vname=HQ-SRV&node=server&resize=off

php.ini [-M--1 21 L:1354+35 389/12361 \*(14940/47641b) 0010 0x00A [TOP]

```
#####
; Miscellaneous :
#####

; Decides whether PHP may expose the fact that it is installed on the server
; (e.g., by adding its signature to the Web server header). It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; http://php.net/expose-php
expose_php = On

#####
; Resource Limits :
#####

; Maximum execution time of each script, in seconds
; http://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 240

; Maximum amount of time each script may spend parsing request data. It's a good
; idea to limit this time on production servers in order to eliminate unexpectedly
; long running scripts.
; Note: This directive is hardcoded to -1 for the CLI SAPI
; Default Value: -1 (Unlimited)
; Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)
; http://php.net/max-input-time
max_input_time = 240

; Maximum Input variable nesting level
; http://php.net/max-input-nesting-level
max_input_nesting_level = 64

; How many GET/POST/COOKIE input variables may be accepted
max_input_vars = 5000

; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit = 128M

#####
; Error handling and logging :
#####

; This directive informs PHP of which errors, warnings and notices you would like
; it to take action for. The recommended way of setting values for this
; directive is through the use of the error level constants and bitwise

```

Help Save Mark Replace Copy Move Search Delete PullDn Quit

Удаляем стандартную страницу apache:

```
cd /var/www/html
```

```
ls
```

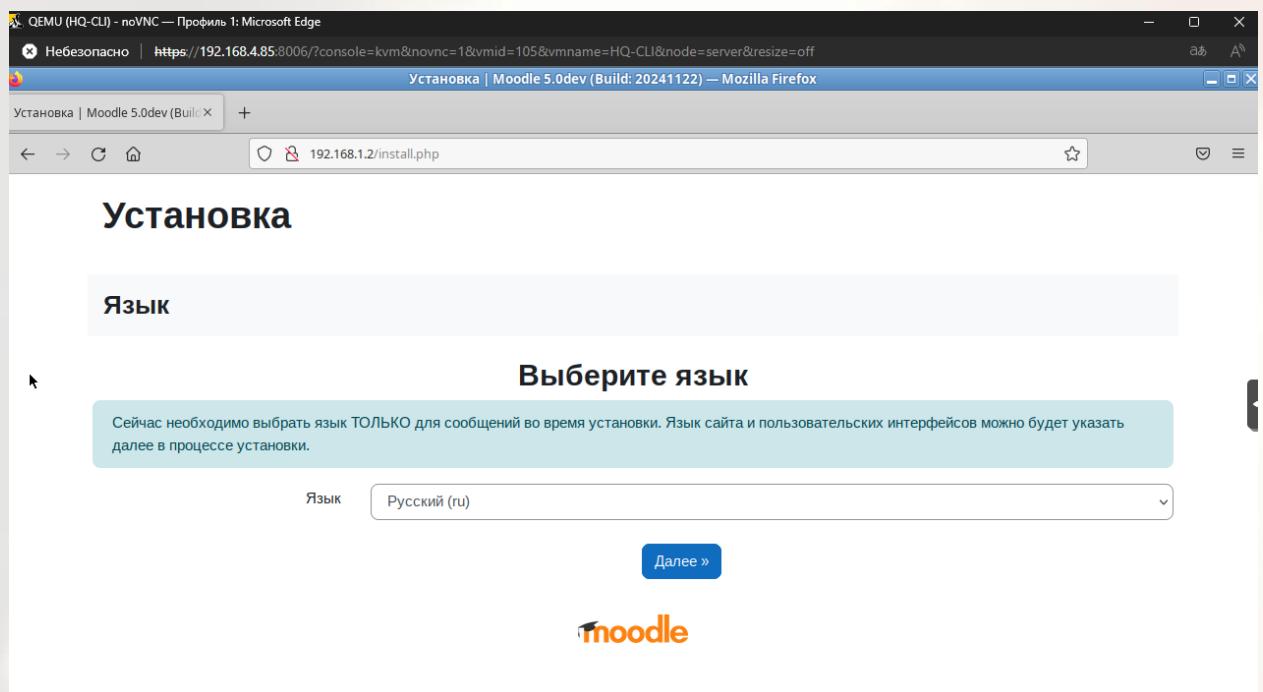
```
rm index.html
```

Перезапускаем службу **httpd2**:

```
systemctl restart httpd2
```

Теперь подключаемся с клиента HQ-CLI и начинаем настройку:

**http://192.168.1.2/install.php**



Жмём далее, т.к. каталог у нас уже создан:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

QEMU (HQ-CLI) - noVNC — Профиль 1: Microsoft Edge  
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=105&vmname=HQ-CLI&node=server&resize=off  
Установка | Moodle 5.0dev (Build: 20241122) — Mozilla Firefox

Установка | Moodle 5.0dev (Build: 20241122) +  
192.168.1.2/install.php

Если указанный здесь адрес неверный, измените URL в адресной строке браузера и перезапустите установку.

**Каталог Moodle**  
Полный путь к каталогу установки Moodle.

**Каталог данных**  
Каталог, в котором Moodle будет хранить все файлы, размещаемые пользователями.  
Этот каталог должен быть доступен для чтения и ЗАПИСИ тому пользователю, от чьего имени запускается веб-сервер (обычно 'www-data', 'nobody' или 'apache').  
Этот каталог не должен быть доступен напрямую через Интернет.  
Программа установки попробует создать этот каталог, если он не существует.

Веб-адрес: http://192.168.1.2  
Каталог Moodle: /var/www/html  
Каталог данных: /var/www/moodledata

« Назад Далее »

Выбираем MariaDB в качестве драйвера базы данных:

QEMU (HQ-CLI) - noVNC — Профиль 1: Microsoft Edge  
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=105&vmname=HQ-CLI&node=server&resize=off  
Установка | Moodle 5.0dev (Build: 20241122) — Mozilla Firefox

Установка | Moodle 5.0dev (Build: 20241122) +  
192.168.1.2/install.php

## Установка

### Название базы данных

### Выберите драйвер базы данных

Moodle поддерживает несколько типов серверов баз данных. Свяжитесь с администратором сервера, если не знаете, какой именно тип выбрать.

Тип: MariaDB (<родной>/mariadb)

« Назад Далее »

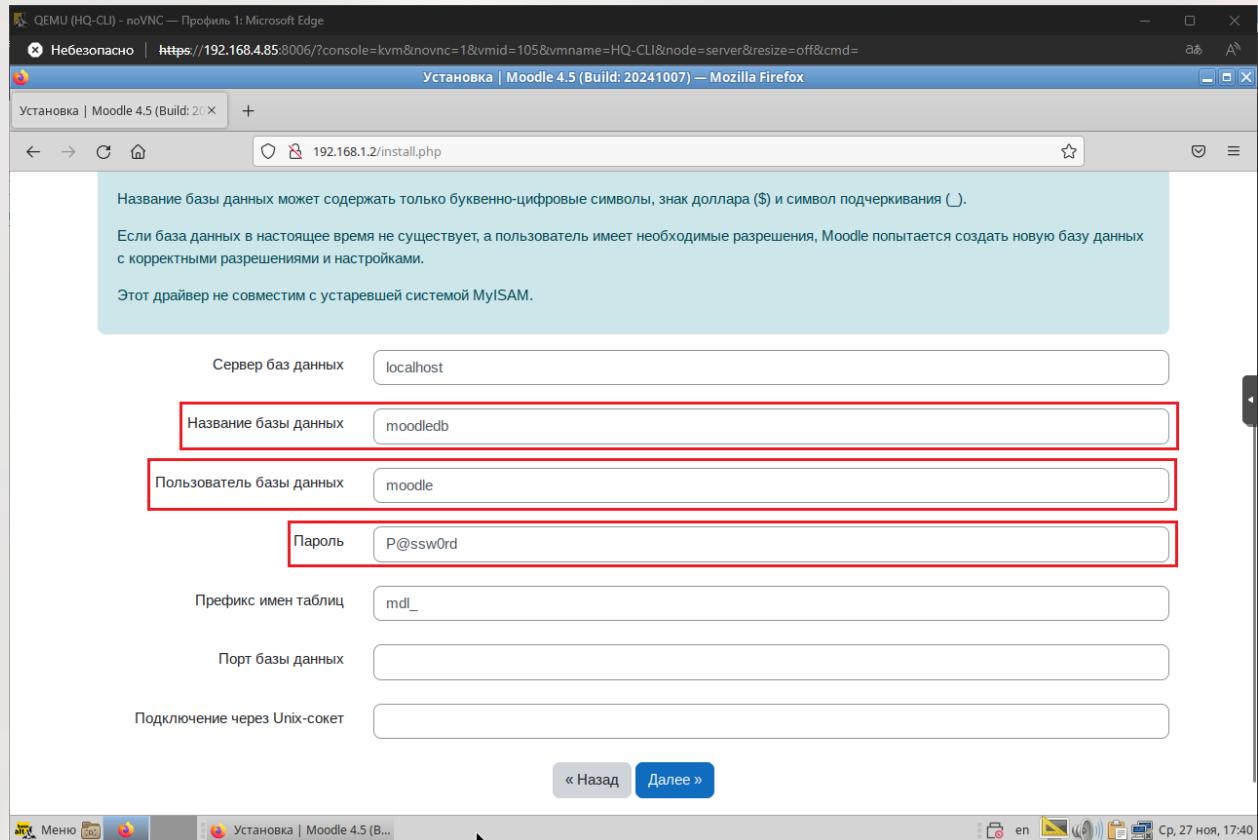
AUTHORS  
NECHAEV  
NAUMOV  
NAGORNOVA

Введём нужные данные в следующие строки:

**Название базы данных:** moodledb

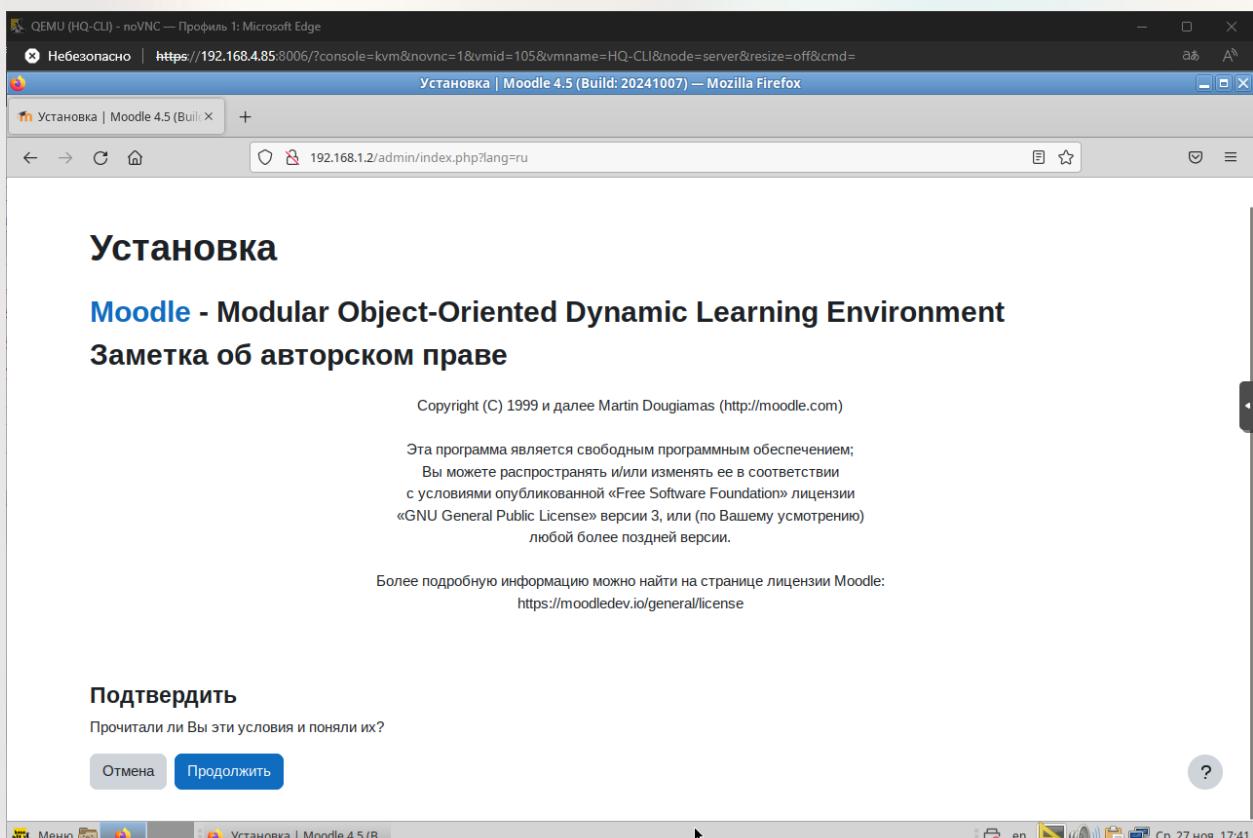
**Пользователь базы данных:** moodle

**Пароль:** P@ssw0rd

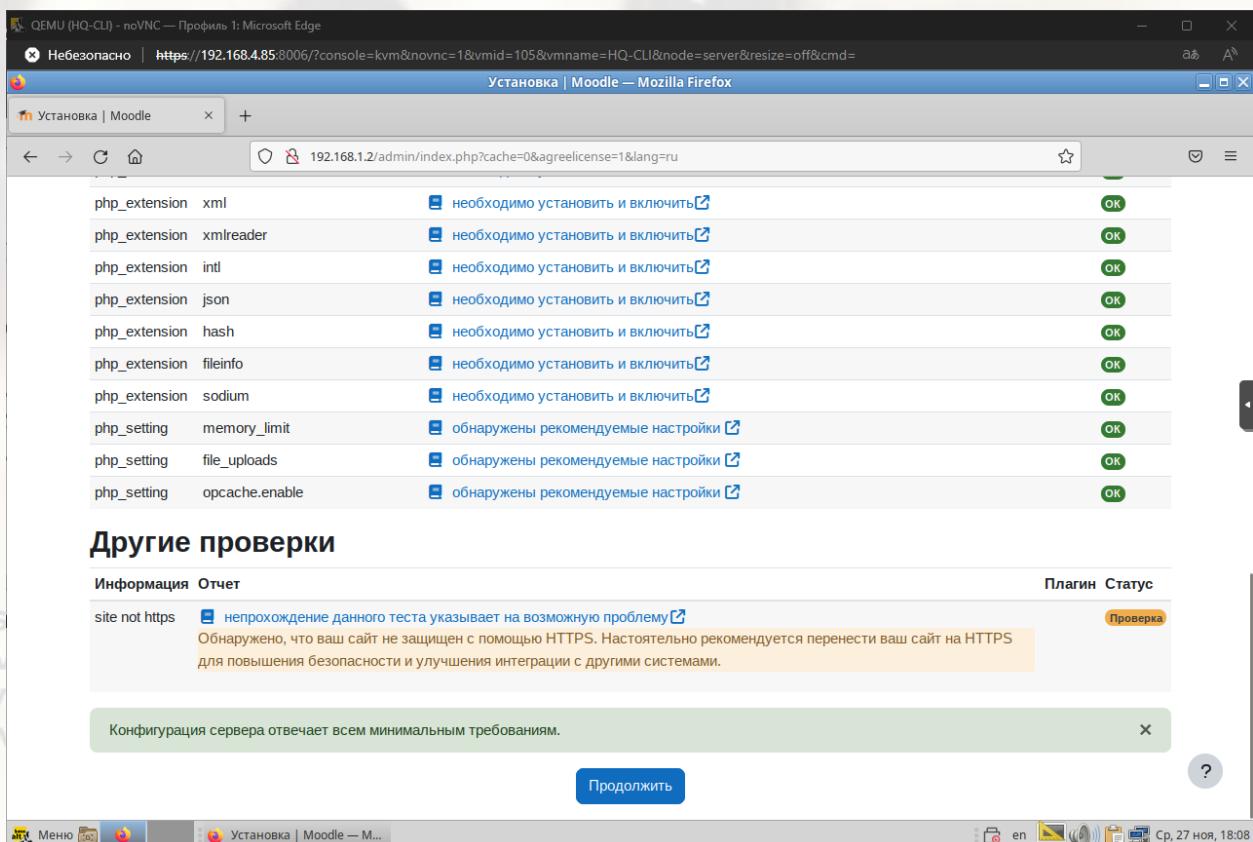


Нажимаем “Продолжить”:

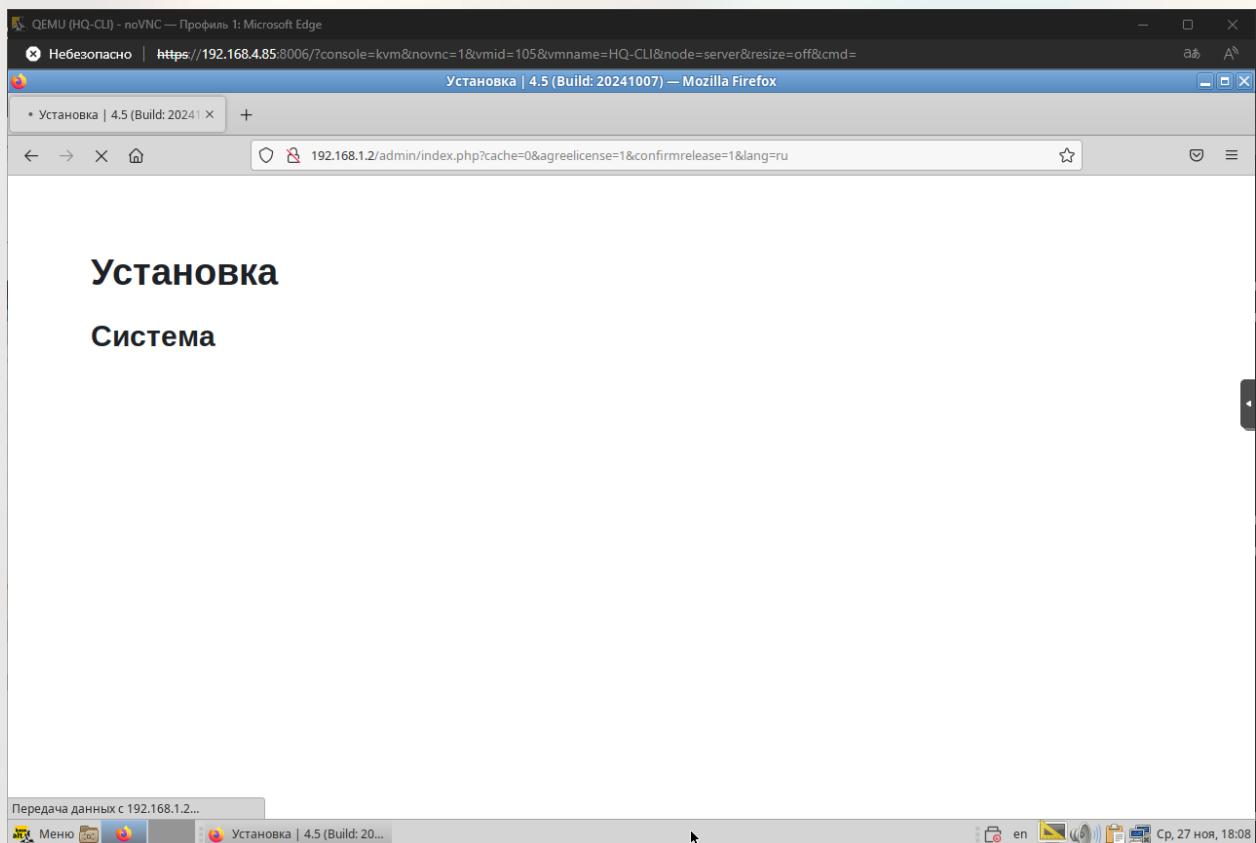
AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



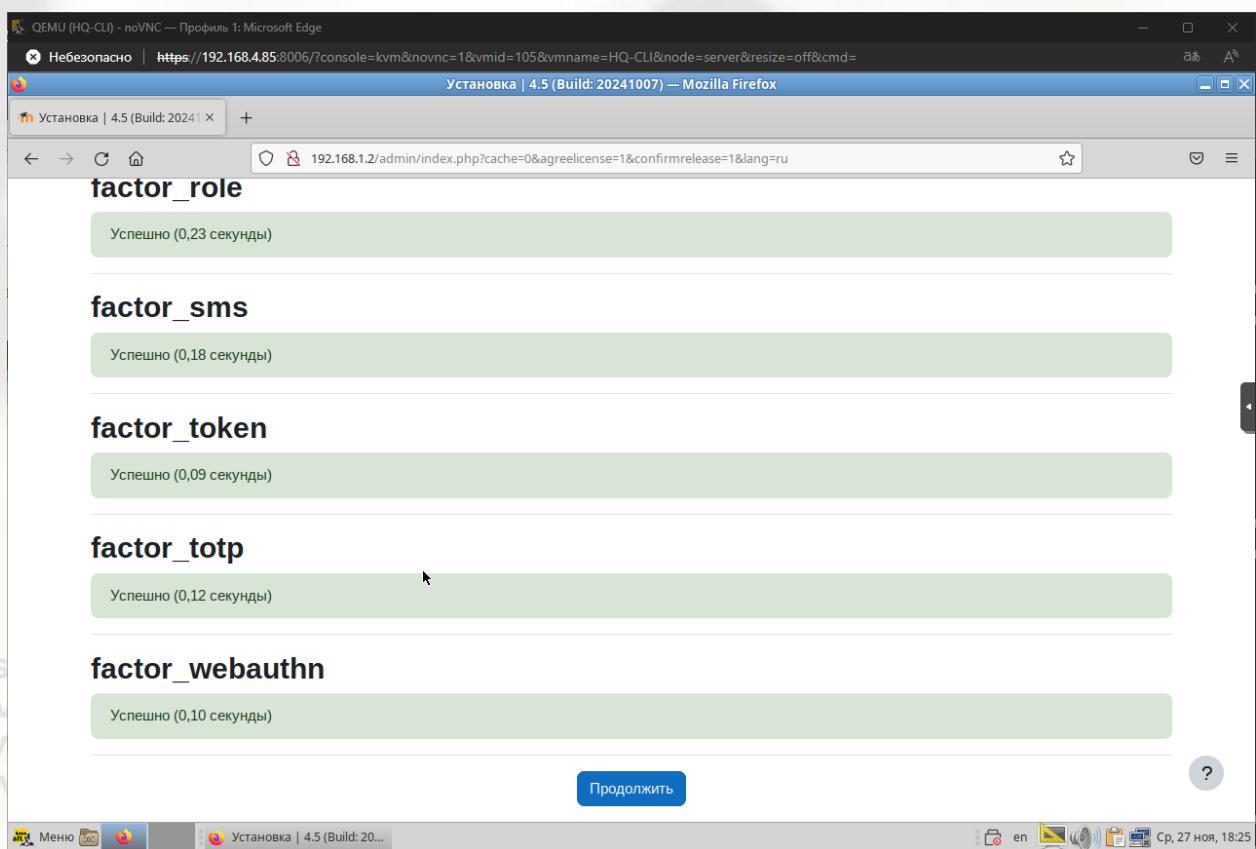
Просматриваем всё ли в статус “OK” или “Проверка” и прожимаем “Продолжить”:



Дальше пойдёт процесс установки в виде такого окна, процесс этот может быть долгим, не пугайтесь:



После установки видим, что всё прошло успешно и жмём “Продолжить”:



Далее заполняем обязательные поля для создания основного администратора:

**Логин:** admin

**Новый пароль:**

P@ssw0rd

**Имя:**

**Администратор** (можно любое)

**Фамилия:**

**Пользователь** (можно любое)

**Адрес электронной почты:** [test.test@mail.ru](mailto:test.test@mail.ru) (можно любое)

И нажимаем “Обновить профиль”:

Основные

Логин admin

Выберите метод аутентификации Ручная регистрация

Пароль должен содержать символов - не менее 8, цифр - не менее 1, строчных букв - не менее 1, прописных букв - не менее 1, не менее 1 специальных символов, таких как \*, - или #.

Новый пароль P@ssw0rd

Принудительная смена пароля

Имя Администратор

Фамилия Пользователь

Адрес электронной почты test.test@mail.ru

Показывать адрес электронной почты Всем

Город

Теперь заполним ещё некоторые строки на следующем шаге:

**Полное название сайта:**

**moodle** (можно любое)

**Краткое название сайта:**

**11** (согласно вашему рабочему месту)

**Настройки местоположения:**

**Азия/Барнаул** (согласно вашему региону)

**Контакты службы поддержки:**

**[test.test@mail.ru](mailto:test.test@mail.ru)** (можно любое)

И жмём “Сохранить изменения” в конце страницы:

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

The screenshot shows the 'Frontpage Settings' section of the Moodle administration interface. It includes fields for 'Full name' (fullname) containing '11', 'Short name' (shortname) containing 'moodle', and a summary field. A toolbar at the bottom provides options like 'Edit', 'View', 'Insert', 'Format', and 'Tools'. The URL in the browser bar is `moodle.au-team.irpo/admin/settings.php?section=frontpagesettings`.

И после всего нас встречает рабочий сайт **moodle**, смотрим, что все наши указанные параметры отображаются:

The screenshot shows the Moodle homepage. The site title 'moodle' is highlighted with a red box and labeled 'Название сайта'. The page number '11' is also highlighted with a red box and labeled 'Номер рабочего места'. The URL in the browser bar is `moodle.au-team.irpo/?redirect=0`.

AUTHORS  
NECHAEV

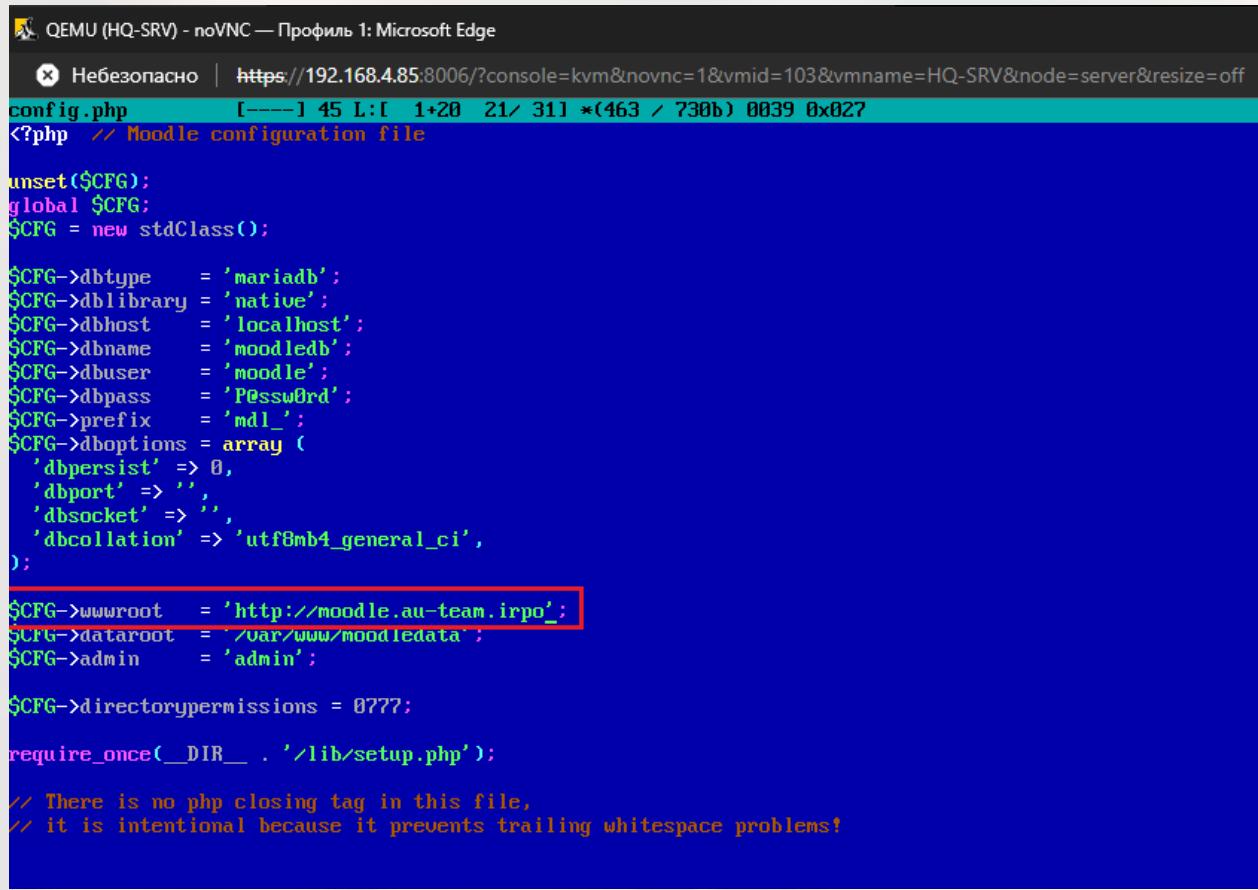
NAUMOV  
NAGORNOVA

## 8. Настройте веб-сервер nginx как обратный прокси-сервер на HQ-RTR

Поменяем значение `wwwroot` в конфигурации `moodle` на **HQ-SRV**:

`mcedit /var/www/html/config.php`

**\$CFG->wwwroot = ‘http://moodle.au-team.irpo’;**



```
QEMU (HQ-SRV) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=103&vmname=HQ-SRV&node=server&resize=off
config.php [---] 45 L:1 1+20 21/ 311 *(463 / 730б) 0039 0x027
<?php // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost = 'localhost';
$CFG->dbname = 'moodle';
$CFG->dbuser = 'moodle';
$CFG->dbpass = 'P@ssw0rd';
$CFG->prefix = 'mdl_';
$CFG->dboptions = array (
    'dbpersist' => 0,
    'dbport' => '',
    'dbsocket' => '',
    'dbcollation' => 'utf8mb4_general_ci',
);

$CFG->wwwroot = 'http://moodle.au-team.irpo';
$CFG->dataroot = '/var/www/moodledata';
$CFG->admin = 'admin';

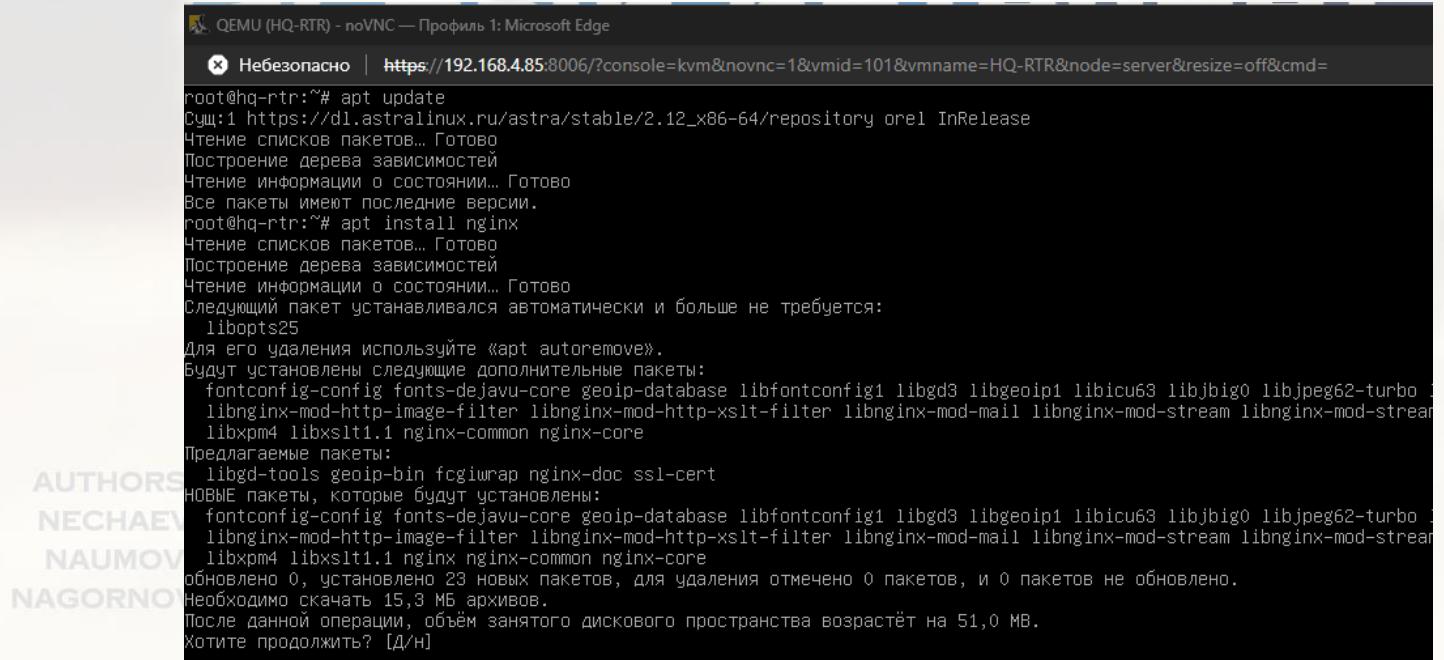
$CFG->directorypermissions = 0777;

require_once(__DIR__ . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!
```

Устанавливаем пакет **nginx** на **HQ-RTR** для дальнейшей настройки:

**apt install nginx**



```
QEMU (HQ-RTR) - noVNC — Профиль 1: Microsoft Edge
Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=101&vmname=HQ-RTR&node=server&resize=off&cmd=
root@hq-rtr:~# apt update
Судя по https://dl.astralinux.ru/astra/stable/2.12_x86-64/repository orel InRelease
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состояниях... Готово
Все пакеты имеют последние версии.
root@hq-rtr:~# apt install nginx
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состояниях... Готово
Следующий пакет устанавливается автоматически и больше не требуется:
 libopts25
Для его удаления используйте «apt autoremove».
Будут установлены следующие дополнительные пакеты:
 fontconfig-config fonts-dejavu-core geoip-database libfontconfig1 libgd3 libgeoip1 libicu63 libjbig0 libjpeg62-turbo ...
 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream ...
 libxpm4 libxsrlt1.1 nginx nginx-common nginx-core
Предлагаемые пакеты:
 libgd-tools geoip-bin fcgiwrap nginx-doc ssl-cert
НОВЫЕ пакеты, которые будут установлены:
 fontconfig-config fonts-dejavu-core geoip-database libfontconfig1 libgd3 libgeoip1 libicu63 libjbig0 libjpeg62-turbo ...
 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream ...
 libxpm4 libxsrlt1.1 nginx nginx-common nginx-core
обновлено 0, установлено 23 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 15,3 МБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 51,0 МВ.
Хотите продолжить? [Д/Н]
```

Создаём новый конфигурационный файл **proxy**:

**mcedit /etc/nginx/sites-available/proxy**

И заполняем его следующими строками:

```
server {  
    listen 80;  
    server_name moodle.au-team.irpo;  
    location / {  
        proxy_pass http://192.168.1.2:80;  
        proxy_set_header Host $host;  
        proxy_set_header X-Real-IP $remote_addr;  
        proxy_set_header X-Forwarded-For $remote_addr;  
    }  
}
```

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA

```

server {
    listen 80;
    server_name wiki.au-team.irpo;
    location / {
        proxy_pass http://192.168.4.2:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $remote_addr;
    }
}

```

```

HQ-RTR (shit2) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
/etc/nginx/sites-available/proxy  [---]  0 L:[ 1+20 21/ 21] *(466
server {
<----->listen 80;
<----->server_name moodle.au-team.irpo;
<----->location / {
<-----><----->proxy_pass http://192.168.1.2:80;
<-----><----->proxy_set_header Host $host;
<-----><----->proxy_set_header X-Real-IP $remote_addr;
<-----><----->proxy_set_header X-Forwarded-For $remote_addr;
<----->}
}
server {
<----->listen 80;
<----->server_name wiki.au-team.irpo;
<----->location / {
<-----><----->proxy_pass http://192.168.4.2:8080;
<-----><----->proxy_set_header Host $host;
<-----><----->proxy_set_header X-Real-IP $remote_addr;
<-----><----->proxy_set_header X-Forwarded-For $remote_addr;
<----->}
}

```

Удаляем конфигурацию (**default**), которую создал **nginx**, потом включаем созданную нами ранее (**proxy**), путём создания символической ссылки, а затем перезапускаем службу **nginx**:

**AUTHORS:**

**NECHAEV** **rm -rf /etc/nginx/sites-available/default**

**NAUMOV**

**NAGORNOY** **rm -rf /etc/nginx/sites-enabled/default**

**ln -s /etc/nginx/sites-available/proxy /etc/nginx/sites-enabled**

**ls -la /etc/nginx/sites-enabled**

**systemctl restart nginx**

```
QEMU (HQ-RTR) - noVNC — Профиль 1: Microsoft Edge
• Небезопасно | https://192.168.4.85:8006/?console=kvm&novnc=1&vmid=101&vmname=HQ-RTR&node=server&resize=off&cmd=
root@hq-rtr:~# rm -rf /etc/nginx/sites-available/default
root@hq-rtr:~# rm -rf /etc/nginx/sites-enabled/default
root@hq-rtr:~# ln -s /etc/nginx/sites-available/proxy /etc/nginx/sites-enabled/
root@hq-rtr:~# ls -la /etc/nginx/sites-enabled/
итого 8
drwxr-xr-x 2 root root 4096 ноя 27 21:26 .
drwxr-xr-x 8 root root 4096 ноя 27 21:10 ..
lrwxrwxrwx 1 root root 32 ноя 27 21:26 proxy -> /etc/nginx/sites-available/proxy
root@hq-rtr:~# systemctl restart nginx
root@hq-rtr:~#
```

Проверим работу нашего обратного прокси и зайдем на наши поднятые ранее сайты **moodle** и **wiki** с клиента **HQ-CLI**.

The screenshot shows two Mozilla Firefox browser windows running on the HQ-CLI terminal. The top window displays the Moodle website at <https://moodle.au-team.ipro>, showing the main course list. The bottom window displays the MediaWiki website at [https://cock.wiki.au-team.ipro/index.php/Заглавная\\_страница](https://cock.wiki.au-team.ipro/index.php/Заглавная_страница), showing the main page of the MediaWiki installation.

Настройка обратного прокси-сервера завершена.

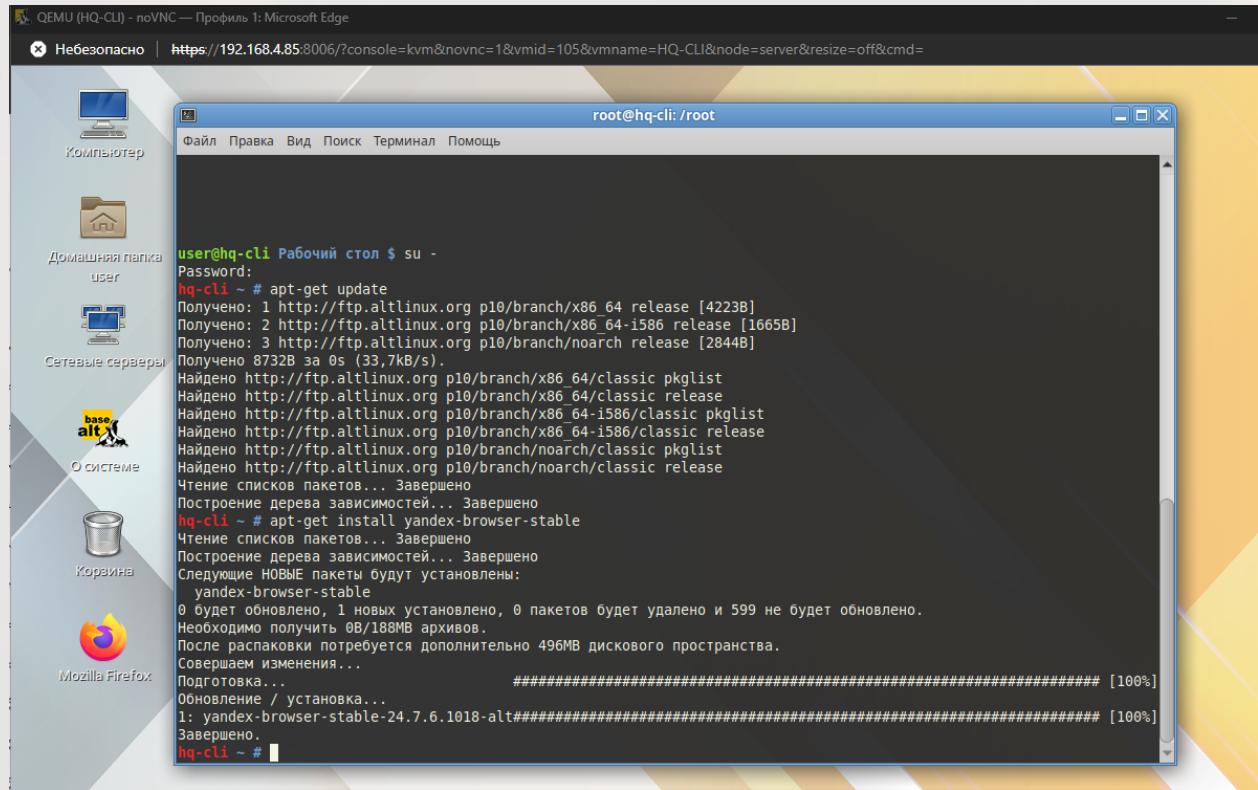
## 9. Удобным способом установите приложение Яндекс Браузер для организаций на HQ-CLI

Установим Яндекс Браузер на **HQ-CLI** через терминал командами:

link community - <https://t.me/sysdemocommunity>

**apt-get update**

**apt-get install yandex-browser-stable**

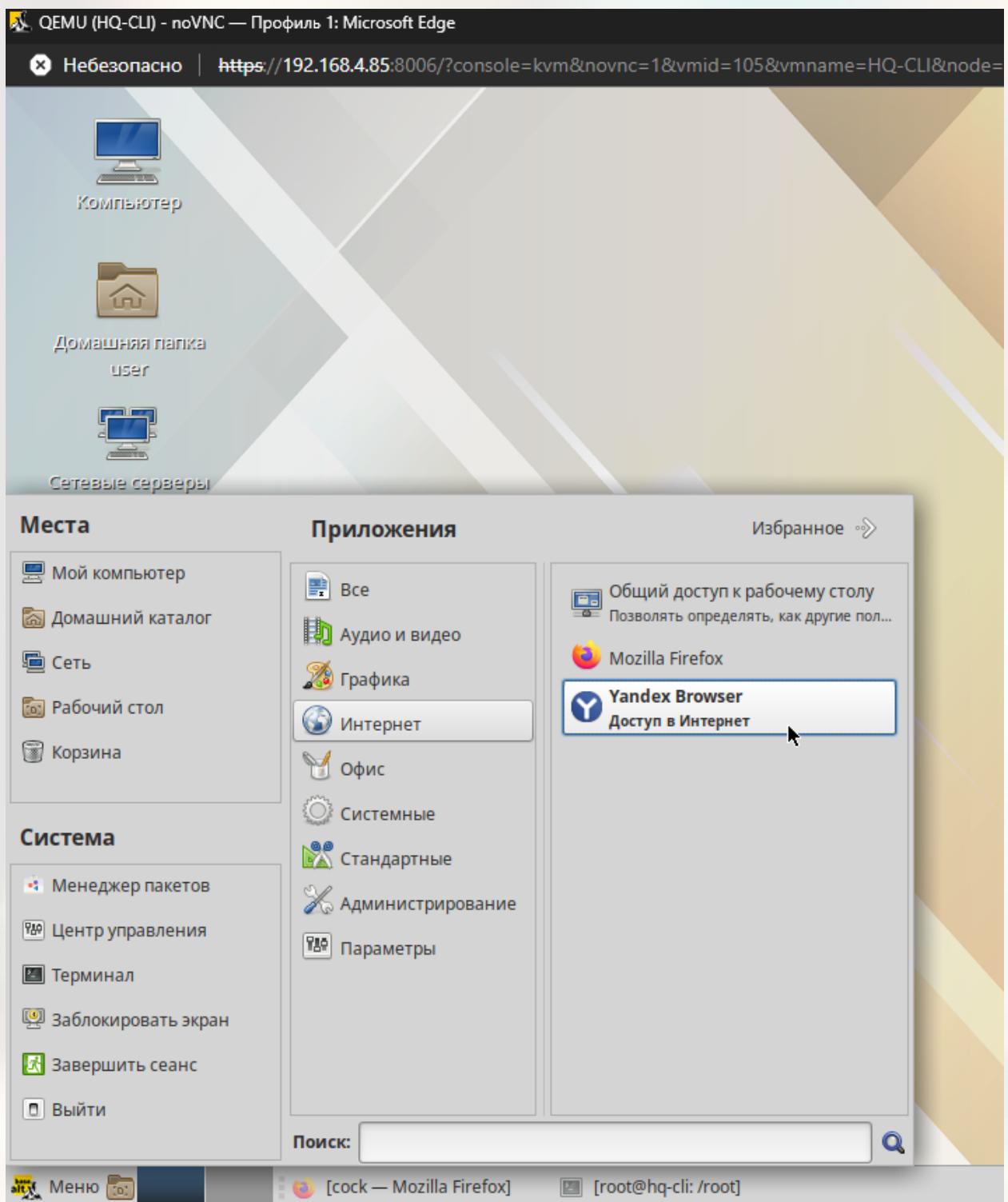


Видим, что установка завершена, теперь запустим его из меню **Пуск**.

Должен быть по пути:

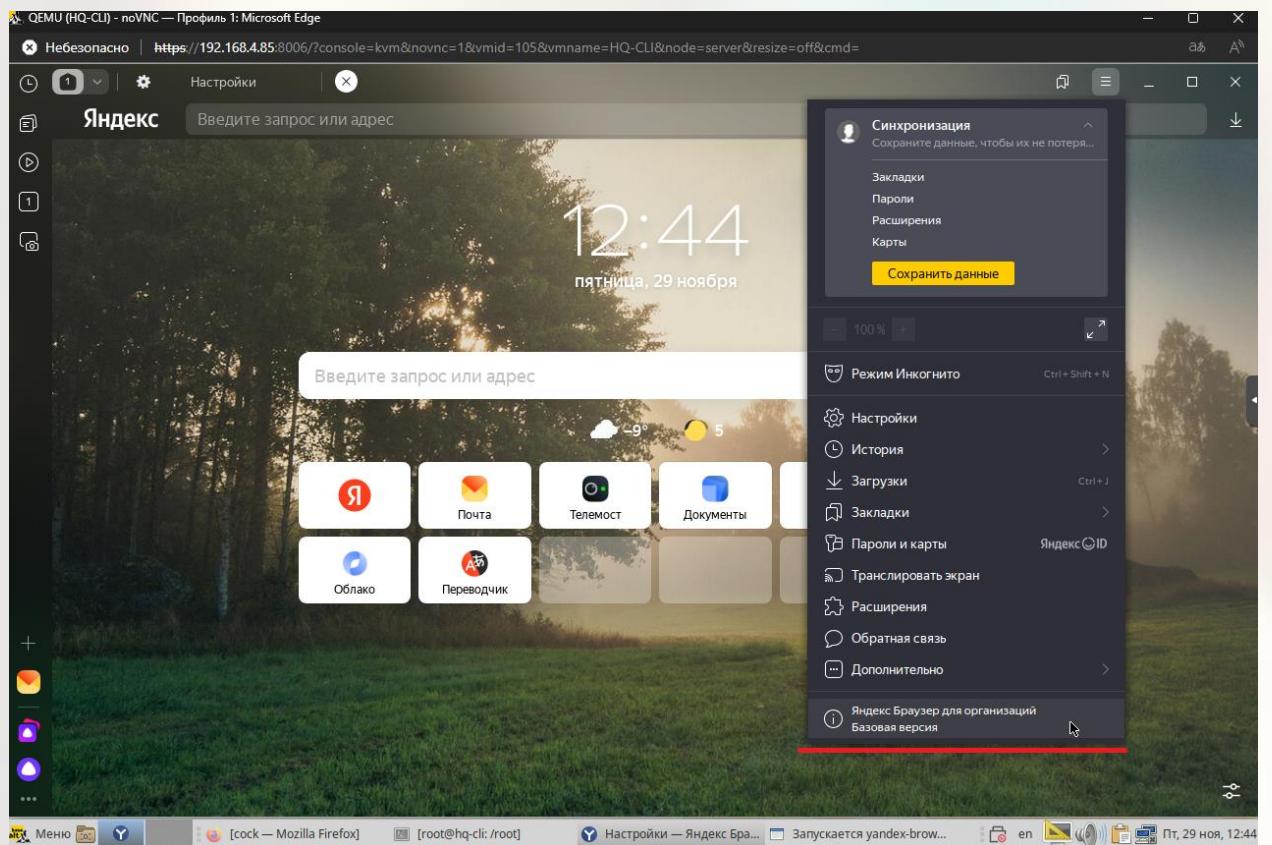
**Пуск → Интернет → Yandex Browser**

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA



При нажатии “≡” мы увидим внизу надпись “**Яндекс.Браузер для организаций**”, это значит, что мы установили правильную версию браузера.

AUTHORS  
NECHAEV  
NAUMOV  
NAGORNOVA



Задание выполнено! Второй модуль завершён!

## МОДУЛЬ №3

AUTHORS:  
NECHAEV  
NAUMOV  
NAGORNOVA