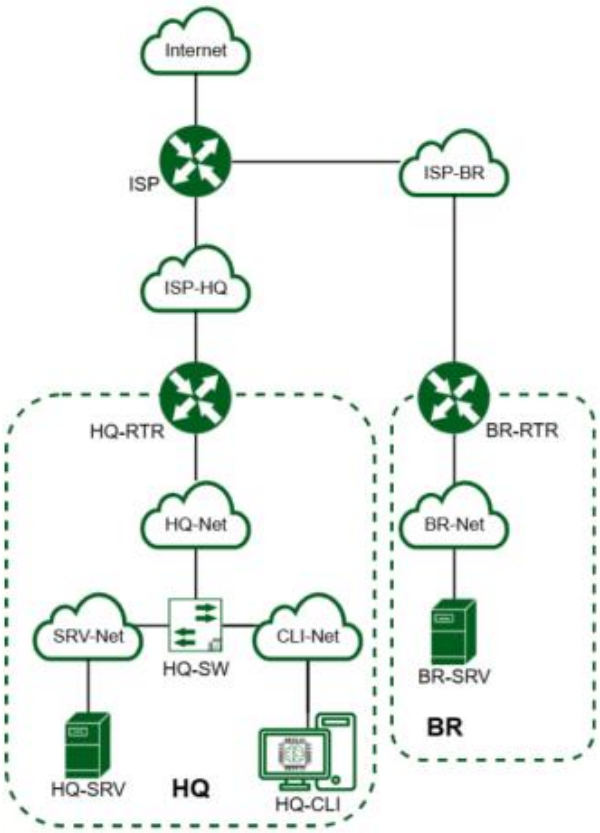


Айпи подсетей:

172.16.1.0/28 – HQ-RTR

172.16.2.0/28 – BR-RTR

192.168.100.0/28 - HQ

192.168.255.0/28 – BR

Устройство	Адаптер	Назначение	Название	IP	Gateway
ISP	ens33	интернет	NAT	-	-
	ens36	172.16.1.0	ISP-HQ	172.16.1.1	-
	ens37	172.16.2.0	ISP-BR	172.16.2.1	-
HQ-RTR	ens33	172.16.1.0	IPS-HQ	172.16.1.2	172.16.1.1
	ens36	192.168.100.0	HQ-NET	192.168.100.1	
BR-RTR	ens33	172.16.2.0	ISP-BR	172.16.2.2	172.16.2.1
	ens36	192.168.255.0	BR-NET	192.168.255.1	

Настройка VMware (Добавление адаптеров, создание LAN Segments и пр при необходимости)

МОДУЛЬ 1

NAT (iptables, 2,8 задание):

Первоначальная настройка ens33 (nano /etc/network/interfaces):

```
auto ens33
iface ens33 inet dhcp
```

После `systemctl restart networking`

Установка на ISP, HQ-RTR,BR-RTR iptables:

```
apt install iptables-persistent
/usr/sbin/iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
/usr/sbin/iptables-save > /etc/iptables/rules.v4
echo "nameserver 8.8.8.8" > /etc/resolv.conf
```

После в nano /etc/sysctl.conf раскоментить `net.ipv4.ip_forward=1`

После `systemctl restart networking`

(При необходимости добавьте nameserver 8.8.8.8 на всех ВМ)

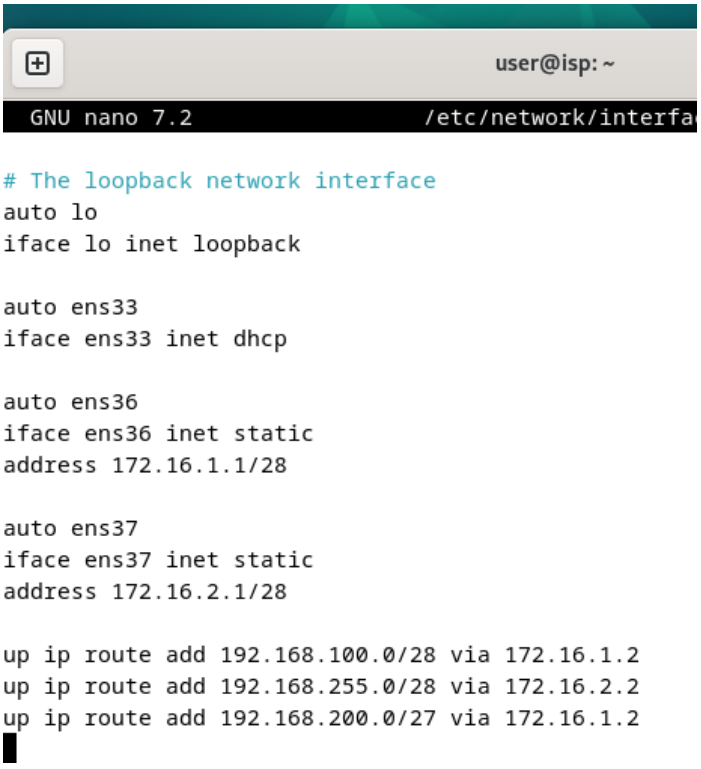


Рисунок – настройка адаптеров ISP

(важно! ens36 и ens37 могут путаться местами, соблюдайте порядок)

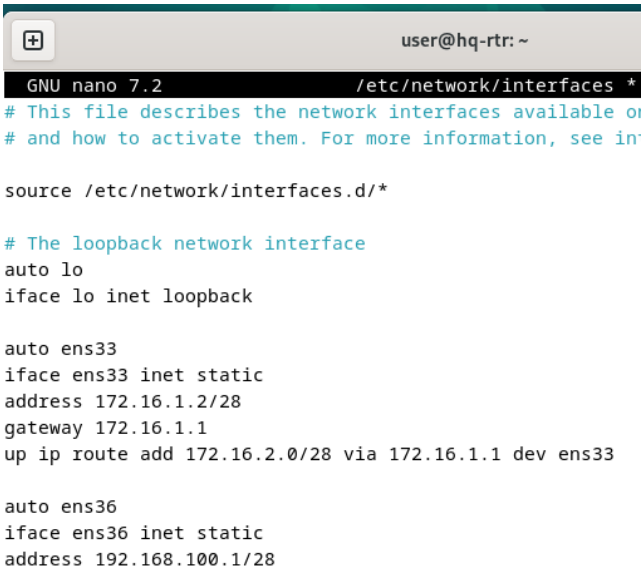


Рисунок – настройка адаптеров HQ-RTR

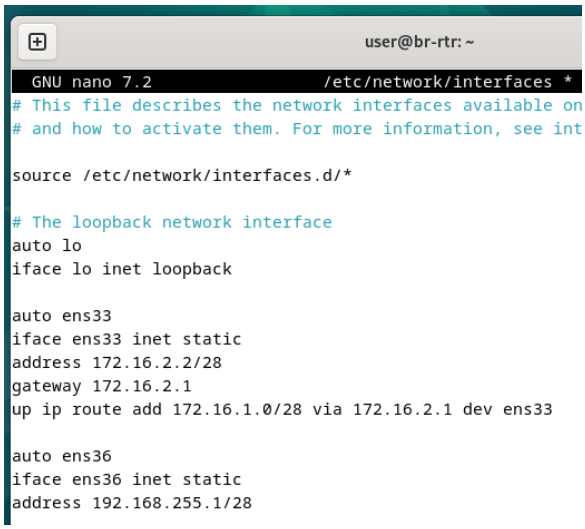


Рисунок – настройка адаптеров BR-RTR

`systemctl restart networking` по необходимости, проверка ping

Создание локальных учетных записей на серверах (HQ-SRV, BR-SRV) и роутерах (HQ-RTR, BR-RTR) (3 задание).

HQ-SRV, BR-SRV:

```
/usr/sbin/useradd remote_user
/usr/sbin/useradd -u 2026 sshuser
passwd sshuser
echo 'sshuser ALL=(ALL) NOPASSWD:ALL' | sudo tee /etc/sudoers.d/sshuser >/dev/null &&
sudo chmod 440 /etc/sudoers.d/sshuser
```

HQ-RTR, BR-RTR:

```
/usr/sbin/useradd net_admin
passwd net_admin
echo 'net_admin ALL=(ALL) NOPASSWD:ALL' | sudo tee /etc/sudoers.d/net_admin >/dev/null
&& sudo chmod 440 /etc/sudoers.d/net_admin
```

Проверка `sudo visudo -cf /etc/sudoers`

Коммутация в сегменте HQ (4 задание).

HQ-RTR:

```
sudo modprobe 8021q
echo 8021q | sudo tee /etc/modules-load.d/8021q.conf >/dev/null
```

```
auto ens36
iface ens36 inet manual

auto ens36.100
iface ens36.100 inet static
  address 192.168.100.1/28

auto ens36.200
iface ens36.200 inet static
  address 192.168.200.1/27

auto ens36.999
iface ens36.999 inet static
  address 192.168.250.1/29
```

Рисунок – редачим ens36 у HQ-RTR

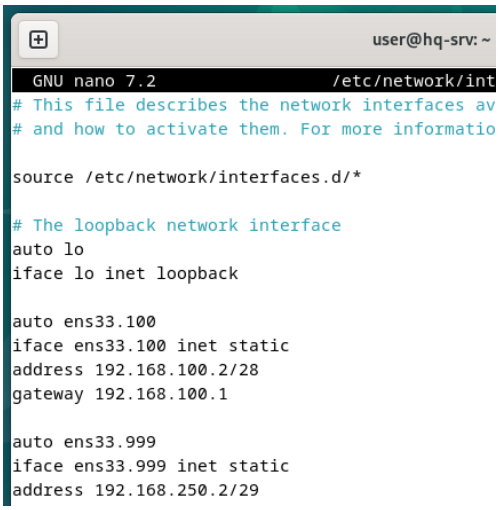


Рисунок - настройка адаптеров HQ-SRV

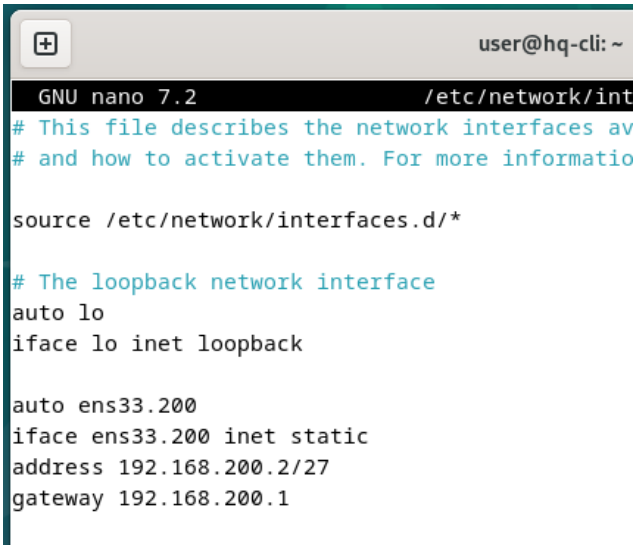


Рисунок - настройка адаптеров HQ-CLI

`systemctl restart networking` по необходимости, проверка `ping`

Настройка SSH на HQ-SRV и BR-SRV (5 Задание).

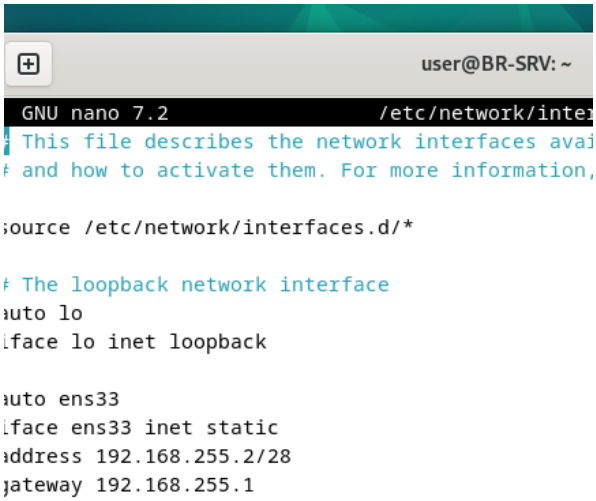


Рисунок – настройка адаптера BR-SRV

Устанавливаем ssh командой:

```
apt install openssh-server
sudo sed -i \
  -e 's/^[#[:space:]]*Port .*/Port 2026/' \
  -e 's/^[#[:space:]]*PermitRootLogin .*/PermitRootLogin no/' \
  -e 's/^[#[:space:]]*MaxAuthTries .*/MaxAuthTries 2/' \
  /etc/ssh/sshd_config
echo 'AllowUsers sshuser' | sudo tee -a /etc/ssh/sshd_config >/dev/null
echo 'Banner /etc/issue.net' | sudo tee -a /etc/ssh/sshd_config >/dev/null
echo 'Authorized access only.' | sudo tee /etc/issue.net >/dev/null
sudo systemctl restart ssh
sudo systemctl enable --now ssh
```

Поставить ssh на всех остальных ВМ (без настроек).

Туннель (GRE) на HQ-RTR и BR-RTR (6 задание).

```
echo ip_gre | sudo tee /etc/modules-load.d/ip_gre.conf >/dev/null && sudo modprobe ip_gre
```

В файле nano /etc/network/interfaces:

Для HR-RTR:

```
auto gre30
iface gre30 inet tunnel
address 10.0.0.1
netmask 255.255.255.252
mode gre
local 172.16.1.2
endpoint 172.16.2.2
ttl 225
post-up ip route add 192.168.255.0/28 via 10.0.0.2
```

Для BR-RTR:

```
auto gre30
iface gre30 inet tunnel
address 10.0.0.2
netmask 255.255.255.252
mode gre
```

```
local 172.16.2.2
endpoint 172.16.1.2
ttl 225
post-up ip route add 192.168.100.0/28 via 10.0.0.1
post-up ip route add 192.168.200.0/27 via 10.0.0.1
```
Потом `systemctl restart networking` при необходимости.

Динамическая маршрутизация на HQ-RTR и BR-RTR (7 задание).

```
apt install frr
sudo sed -i 's/^ospfd=no/ospfd=yes/' /etc/frr/daemons
sudo systemctl restart frr
systemctl enable frr
```
Заходим в оболочку командой vtysh и пишем:

Для HQ-RTR:

```
conf t
ip forwarding
router ospf
passive-interface default
no ip ospf passive
network 192.168.100.0/28 area 0
network 192.168.200.0/27 area 0
network 10.0.0.0/30 area 0
exit
interface gre30
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 1c+rYtGm
exit
exit
wr
exit
```
Для BR-RTR:

```
conf t
ip forwarding
router ospf
passive-interface default
no ip ospf passive
network 192.168.255.0/28 area 0
network 10.0.0.0/30 area 0
exit
interface gre30
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 1c+rYtGm
exit
exit
wr
exit
```
Протокол динамической конфигурации хостов для сети в сторону HQ-CLI (9 задание).

Установка сервера DHCP на HQ-RTR:

```
sudo apt install isc-dhcp-server
```
Привязка к нужному интерфейсу в nano /etc/default/isc-dhcp-server

```
INTERFACESv4="ens36.200"

INTERFACESv6=""
```
Конфигурация DHCP в nano /etc/dhcp/dhcpd.conf (изначальную убрать):

```
authoritative;
ddns-update-style none;
default-lease-time 600;
max-lease-time 7200;
option domain-name "au-team.irpo";
subnet 192.168.200.0 netmask 255.255.255.224 {
  range 192.168.200.2 192.168.200.30;
  option routers 192.168.200.1;
  option domain-name-servers 192.168.100.2;
  option broadcast-address 192.168.200.31;
}
```

Потом:

```
sudo systemctl restart isc-dhcp-server
sudo systemctl enable --now isc-dhcp-server
sudo systemctl status isc-dhcp-server
```

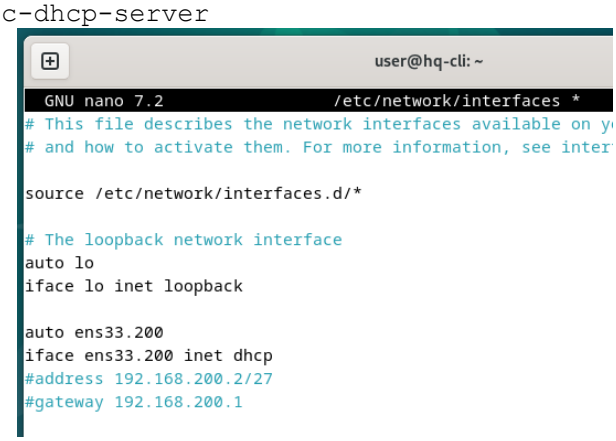


Рисунок – настройки адаптера HQ-CLI

Инфраструктура разрешения доменных имен для офисов HQ и BR (10 задание).

Установка bind9 на HQ-SRV

```
sudo apt install bind9 bind9utils bind9-dnsutils
```

Указать nameserver (nano /etc/resolv.conf) 192.168.100.2, где нет изначально.

nano /etc/bind/named.conf.options и задать форвардеры + сети (изначальную убрать):

```
options {
    directory "/var/cache/bind";
    listen-on { any; };
    listen-on-v6 { none; };
    recursion yes;

    allow-query {
        127.0.0.1;
        192.168.100.0/28;
        192.168.200.0/27;
        192.168.255.0/28;
    };

    forwarders {
        77.88.8.7;
        77.88.8.3;
    };
    forward only;

    dnssec-validation auto;
};
```

Определение зон в nano /etc/bind/named.conf.local

```
zone "au-team.irpo" {
    type master;
    file "/etc/bind/zones/db.au-team.irpo";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.100";
};

zone "200.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.200";
};

zone "255.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.255";
};
```

Каталог и файлы зон:

```
sudo mkdir -p /etc/bind/zones
```

Создание прямой зоны nano /etc/bind/zones/db.au-team.irpo

```
$TTL 3600
@   IN SOA  ns1.au-team.irpo. admin.au-team.irpo. (
        2025101302  ; Serial (увеличил)
        3600 1800 1209600 300 )

@       IN NS  ns1.au-team.irpo.
ns1     IN A   192.168.100.2

hq-rtr  IN A   192.168.100.1
br-rtr  IN A   192.168.255.1
hq-srv  IN A   192.168.100.2
hq-cli  IN A   192.168.200.2      ; если статический; при DHCP можно опустить
br-srv  IN A   192.168.255.2

docker  IN A   172.16.1.1         ; ISP -> HQ-RTR (ISP-HQ)
web     IN A   172.16.2.1         ; ISP -> BR-RTR (ISP-BR)
```

Создание обратных зон:

nano /etc/bind/zones/db.192.168.100

```
$TTL 3600
@   IN SOA ns1.au-team.irpo. admin.au-team.irpo. (
        2025101302 3600 1800 1209600 300 )
@   IN NS ns1.au-team.irpo.

1   IN PTR hq-rtr.au-team.irpo.
2   IN PTR hq-srv.au-team.irpo.
```

nano /etc/bind/zones/db.192.168.200

```
$TTL 3600
@   IN SOA ns1.au-team.irpo. admin.au-team.irpo. (
        2025101302 3600 1800 1209600 300 )
@   IN NS ns1.au-team.irpo.

2   IN PTR hq-cli.au-team.irpo.   ; если HQ-CLI статичен на .2
```

nano /etc/bind/zones/db.192.168.255

```
$TTL 3600
@   IN SOA ns1.au-team.irpo. admin.au-team.irpo. (
        2025101302 3600 1800 1209600 300 )
@   IN NS ns1.au-team.irpo.

1   IN PTR br-rtr.au-team.irpo.
2   IN PTR br-srv.au-team.irpo.
```

Настройка часового пояса на всех устройствах (задание 11).

```
sudo timedatectl set-timezone Europe/Moscow
```

МОДУЛЬ 2

Настройка контроллера домена Samba DC на сервере BR-SRV (1 задание)

Установка samba:

```
sudo apt install samba krb5-user winbind smbclient
```

При установке krb5-user:
AU-TEAM.IRPO – область по умолчанию
br-srv.au-team.irpo – серверы Kerberos для области
br-srv.au-team.irpo – управляющий сервер

Установка имени хоста:

```
hostnamectl set-hostname br-srv.au-team.irpo
```

Настройка контроллера домена:

`sudo rm -rf /etc/samba/smb.conf` – отдельно!

```
sudo samba-tool domain provision \
  --use-rfc2307 \
  --realm=AU-TEAM.IRPO \
  --domain=AU-TEAM \
  --server-role=dc \
  --dns-backend=SAMBA_INTERNAL \
  --adminpass='P@ssw0rd'
```

Запуск службы:

```
sudo systemctl disable --now smbd nmbd winbind 2>/dev/null || true
sudo systemctl enable --now samba-ad-dc
```

Подправка bind9 в HQ-SRV в **nano /etc/bind/zones/db.au-team.irpo**

```
_ldap._tcp           IN SRV 0 100 389 br-srv.au-team.irpo.
_kerberos._tcp       IN SRV 0 100 88  br-srv.au-team.irpo.
_kerberos._udp       IN SRV 0 100 88  br-srv.au-team.irpo.
_kpasswd._tcp        IN SRV 0 100 464 br-srv.au-team.irpo.
_kpasswd._udp        IN SRV 0 100 464 br-srv.au-team.irpo.
_gc._tcp             IN SRV 0 100 3268 br-srv.au-team.irpo.   ; опционально
_kerberos            IN TXT "AU-TEAM.IRPO"
```

Увеличить Serial, systemctl restart bind9

Создание пользователей и группы на BR-SRV:

```
echo "192.168.255.2 br-srv.au-team.irpo br-srv" | sudo tee -a /etc/hosts >/dev/null
sudo samba-tool user create hquser1 P@ssw0rd
sudo samba-tool user create hquser2 P@ssw0rd
```

```
sudo samba-tool user create hquser3 P@ssw0rd
sudo samba-tool user create hquser4 P@ssw0rd
sudo samba-tool user create hquser5 P@ssw0rd
sudo samba-tool group add hq
for i in {1..5}; do sudo samba-tool group addmembers hq hquser$i; done
```

На HQ-CLI:

```
sudo apt install realmd sssd sssd-tools adcli samba-common packagekit krb5-user
sudo realm join -U Administrator au-team.irpo
echo '%hq ALL=(ALL:ALL) NOPASSWD: /usr/bin/cat, /usr/bin/grep, /usr/bin/id' | sudo tee
/etc/sudoers.d/hq >/dev/null
sudo chmod 440 /etc/sudoers.d/hq
sudo visudo -cf /etc/sudoers
getent passwd 'AU-TEAM\hquser1' && id 'AU-TEAM\hquser1'
sudo kinit hquser1@AU-TEAM.IRPO
```

Конфигурация файлового хранилища на HQ-SRV (2 задание).

Добавить диски в HQ-SRV!

```
apt install mdadm
sudo fdisk -l
sudo mdadm --create /dev/md0 --level=0 --raid-devices=2 /dev/sdc /dev/sdb
sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
sudo parted /dev/md0 mklabel gpt
sudo parted -a optimal /dev/md0 mkpart primary ext4 0% 100%
sudo mkfs.ext4 /dev/md0p1
sudo mkdir /raid
sudo mount /dev/md0p1 /raid
```

`sudo blkid /dev/md0p1` – узнать uuid, отдельно

Добавление записи в nano /etc/fstab

```
UUID=свой uuid   /raid   ext4   defaults,nofail   0   0
```

Потом выполнить `sudo update-initramfs -u`

Настройка сервера сетевой файловой системы (nfs) на HQ-SRV (3 Задание).

```
sudo apt install nfs-kernel-server -y
sudo mkdir -p /raid/nfs
sudo chown nobody:nogroup /raid/nfs
sudo chmod 0777 /raid/nfs
```

В nano /etc/exports

```
/raid/nfs 192.168.200.0/27(rw,sync,no_subtree_check)
```

Сохранение и перезапуск:

```
sudo exportfs -ra
sudo systemctl restart nfs-kernel-server
sudo systemctl enable nfs-kernel-server
```

Настройка клиента на HQ-CLI:

```
sudo apt install nfs-common -y
sudo mkdir -p /mnt/nfs
sudo mount 192.168.100.2:/raid/nfs /mnt/nfs
```

Добавить в nano /etc/fstab

```
192.168.100.2:/raid/nfs   /mnt/nfs   nfs   defaults,netdev   0   0
```

Настройка службы сетевого времени на базе сервиса chrony на маршрутизаторе ISP (4 Задание).

```
sudo apt install chrony
```

В файле nano /etc/chrony/chrony.conf (изначальное убираем):

```
local stratum 5

allow 192.168.100.0/28
allow 192.168.200.0/27
allow 192.168.255.0/28
allow 172.16.0.0/16

bindaddress 0.0.0.0

driftfile /var/lib/chrony/chrony.drift

log tracking measurements statistics
logdir /var/log/chrony

rtcsync
```

Перезапуск службы:

```
sudo systemctl restart chrony
sudo systemctl enable chrony
```

На клиентах (HQ-SRV, HQ-CLI, BR-RTR, BR-SRV).

```
sudo apt install chrony
```

В файле nano /etc/chrony/chrony.conf (изначальное убираем):

```
server 172.16.1.1 iburst

driftfile /var/lib/chrony/chrony.drift

log tracking measurements statistics
logdir /var/log/chrony

rtcsync
```

Перезапуск службы:

```
sudo systemctl restart chrony
sudo systemctl enable chrony
```

Конфигурация ansible на сервере BR-SRV (5 Задание).

```
sudo apt install -y ansible sshpass
sudo mkdir -p /etc/ansible
sudo chmod 755 /etc/ansible
```

В файле – nano /etc/ansible/hosts

```
[servers]
hq-srv ansible_host=192.168.100.2 ansible_port=2026 ansible_user=sshuser
ansible_password=P@ssw0rd
hq-cli ansible_host=192.168.200.2 ansible_port=22 ansible_user=user
ansible_password=root ansible_become=false
[routers]
hq-rtr ansible_host=192.168.100.1 ansible_port=22 ansible_user=net_admin
ansible_password=P@ssw0rd
```

```
br-rtr ansible_host=192.168.255.1 ansible_port=22 ansible_user=net_admin
ansible_password=P@ssw0rd
[all:children]
servers
routers
```
В файле – nano /etc/ansible/ansible.cfg

```
[defaults]
inventory = /etc/ansible/hosts
host_key_checking = False
forks = 10
timeout = 10
interpreter_python = auto
remote_tmp = /tmp/.ansible-${USER}
[privilege_escalation]
become = True
become_method = sudo
become_user = root
become_ask_pass = False
```
Проверка:

ansible all -m ping

Веб приложение в docker на сервере BR-SRV (6 Задание)

В VMware добавить Aditional.iso в cd-привод и включить привод.

```
mkdir -p /mnt
mkdir -p /tmp/additional
mount /dev/sr0 /tmp/additional
cp -r /tmp/additional /mnt
apt install curl
sudo curl -fsSL https://get.docker.com | sh
docker load -i /mnt/additional/docker/mariadb_latest.tar
docker load -i /mnt/additional/docker/site_latest.tar
docker images
chmod -R 755 /mnt/additional
```
Создаём nano /mnt/additional/docker/docker-compose.yml

```
# docker-compose.yml
version: '3.8'
services:
  database:
    container_name: db
    image: mariadb:10.11
    restart: always
    ports:
      - "3306:3306"
    environment:
      MARIADB_DATABASE: "testdb"
      MARIADB_USER: "testc"
      MARIADB_PASSWORD: "P@sswOrd"
      MARIADB_ROOT_PASSWORD: "root"

  app:
    container_name: testapp
    image: site:latest
    restart: always
    ports:
      - "8080:8000"
    environment:
      DB_TYPE: "maria"
      DB_HOST: "database"
      DB_PORT: "3306"
      DB_NAME: "testdb"
```

```
      DB_USER: "testc"
      DB_PASS: "P@sswOrd"
    depends_on:
      - database
volumes:
  db_data:
```

Далее запускаем docker-compose:

```
cd /mnt/additional/docker/
docker compose up -d
```

Веб приложение на сервере HQ-SRV (7 Задание)

В VMware добавить Aditional.iso в cd-привод и включить привод.

```
mkdir -p /mnt/additional
mount -t iso9660 /dev/sr0 /mnt/additional
apt install apache2 mariadb-server php php-mysql php-cli php-gd
systemctl enable apache2 mariadb
```

Заходим в mariadb, создаем бд, пользователя и даем права:

mariadb -u root

```
CREATE DATABASE webdb;
CREATE USER web@localhost IDENTIFIED BY 'P@ssw0rd';
GRANT ALL PRIVILEGES ON webdb.* TO web@localhost;
FLUSH PRIVILEGES;
exit;
```

```
mariadb -u root -p webdb < /mnt/additional/web/dump.sql
cp /mnt/additional/web/index.php /var/www/html/
mkdir /var/www/html/images
cp /mnt/additional/web/logo.png /var/www/html/images/
cp /mnt/additional/web/index.php /var/www/html/
chown -R www-data:www-data /var/www/html/
chmod -R 755 /var/www/html/
```

Заходим в файл nano /var/www/html/index.php и редактируем несколько строк:

$servername = "localhost";
$username = "web";
$password = "P@ssw0rd";
$dbname = "webdb";

```
/usr/sbin/a2enmod rewrite
systemctl restart apache2
```

Заходим в nano /etc/apache2/mods-enabled/dir.conf (изначальное убираем)

```
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm
</IfModule>

mv /var/www/html/index.html /var/www/html/index.html.backup
systemctl restart apache2
```

На маршрутизаторах сконфигурировать статическую трансляцию портов (8 Задание).

на hq-rtr:

```
/sbin/iptables -t nat -A PREROUTING -d 172.16.1.2 -p tcp --dport 8080 -j DNAT --to-destination 192.168.100.2:8080
/sbin/iptables -t nat -A PREROUTING -d 172.16.1.2 -p udp --dport 8080 -j DNAT --to-destination 192.168.100.2:8080
/sbin/iptables -t nat -A PREROUTING -d 172.16.1.2 -p tcp --dport 2026 -j DNAT --to-destination 192.168.100.2:2026
/sbin/iptables -t nat -A PREROUTING -d 172.16.1.2 -p udp --dport 2026 -j DNAT --to-destination 192.168.100.2:2026
/usr/sbin/iptables-save > /etc/iptables/rules.v4
```

на br-rtr:

```
/sbin/iptables -t nat -A PREROUTING -d 172.16.2.2 -p tcp --dport 8080 -j DNAT --to-destination 192.168.255.2:8080
/sbin/iptables -t nat -A PREROUTING -d 172.16.2.2 -p udp --dport 8080 -j DNAT --to-destination 192.168.255.2:8080
/sbin/iptables -t nat -A PREROUTING -d 172.16.2.2 -p tcp --dport 2026 -j DNAT --to-destination 192.168.255.2:2026
/sbin/iptables -t nat -A PREROUTING -d 172.16.2.2 -p udp --dport 2026 -j DNAT --to-destination 192.168.255.2:2026
/usr/sbin/iptables-save > /etc/iptables/rules.v4
```

Настройка веб-сервер nginx как обратный прокси-сервер на ISP (9 Задание).

```
apt install nginx
systemctl enable nginx
```

Заходим в nano /etc/nginx/sites-available/reverse_proxy.conf

```
upstream hq_srv_app {
    server 192.168.100.2:80;
}

upstream testapp_app {
    server 192.168.255.2:8080;
}

server {
    listen 80;
    server_name web.au-team.irpo;

    location / {
        proxy_pass http://hq_srv_app;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}

server {
    listen 80;
    server_name docker.au-team.irpo;

    location / {
        proxy_pass http://testapp_app;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

```
ln -sf /etc/nginx/sites-available/reverse_proxy.conf /etc/nginx/sites-
enabled/reverse_proxy.conf
sudo rm -f /etc/nginx/sites-enabled/default
sudo systemctl reload nginx
```
Проверка *http://docker.au-team.irpo/* и *http://web.au-team.irpo/*

На маршрутизаторе ISP настройка web-based аутентификации (10 Задание).

```
apt install apache2-utils -y
htpasswd -c /etc/nginx/.htpasswd WEB
```
Пароль: **P@ssw0rd**

nano /etc/nginx/sites-available/reverse_proxy.conf

И в блоке:

```
server {
    listen 80;
    server_name web.au-team.irpo;
```
Добавляем **перед location** /:

```
    auth_basic           "Authorization Required";
    auth_basic_user_file /etc/nginx/.htpasswd;


systemctl reload nginx
```

Установка Яндекс Браузера на HQ-CLI (11 Задание).

Скачать deb пакет с официального сайта

Установка:

```
cd /home/user/Загрузки
sudo dpkg -i Yandex.deb
sudo apt --fix-broken install -y
```
Или графически через папку Загрузки (пкм по пакета, выбрать установщик приложением)

МОДУЛЬ 3

Выполните импорт пользователей в домен au-team.irpo на BR-SRV (1 задание).

В VMware добавить Aditional.iso в cd-привод и включить привод.

Создаём скрипт и выдаём ему права на исполнение:
```
touch /mnt/additional/import_user.sh
chmod +x /mnt/additional/import_user.sh
```

В файле nano /mnt/additional/import_user.sh
```
#!/bin/bash
csv_file="$1"
# Create OU
awk -F ';' 'NR>1 {print $5}' "$csv_file" | sort | uniq | while read ou; do
    samba-tool ou add OU="$ou",DC=au-team,DC=irpo;
done
# Create Users
while IFS=";" read -r firstName lastName role phone ou street zip city country
password; do
    if [ "$firstName" == "First Name" ]; then
        continue
```

```
    fi
    username="${firstName,,}.${lastName,,}"
    samba-tool user add "$username" "$password" \
        --given-name="$firstName" \
        --surname="$lastName" \
        --telephone-number="$phone" \
        --job-title="$role" \
        --userou="OU=$ou"
    samba-tool user setexpiry "$username" --noexpiry
done < "$csv_file"
```

Активация скрипта:

/mnt/additional/import_user.sh /mnt/additional/Users.csv

Выполните настройку центра сертификации на базе HQ-SRV (2 задание).

Установка на hq-srv и на isp:

```
apt install openssl libengine-gost-openssl
```

Добавляем на hq-srv и isp в конец файла nano /etc/ssl/openssl.cnf

```
openssl_conf = openssl_init

[openssl_init]
engines = engine_section

[engine_section]
gost = gost_section

[gost_section]
engine_id = gost
dynamic_path = /usr/lib/x86_64-linux-gnu/engines-3/gost.so
default_algorithms = ALL
```

Обновляем данные openssl на hq-srv и isp:

```
OPENSSL_CONF=/etc/ssl/openssl.cnf openssl engine -t -c
```

На hq-srv создаём сертификаты:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCB -out ca.key
openssl req -new -x509 -md_gost12_256 -days 30 -key ca.key -out ca.cer
```

```
root@hq-srv:/home/user/test.d# openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCB -out ca.key
root@hq-srv:/home/user/test.d# openssl req -new -x509 -md_gost12_256 -days 30 -key ca.key -out ca.cer
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Tatarstan
Locality Name (eg, city) []:Kazan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:au-team.irpo
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:hq-srv.au-team.irpo
Email Address []:
root@hq-srv:/home/user/test.d#
```

```
openssl x509 -noout -text -in ca.cer
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out web.au-team.irpo.key
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out docker.au-team.irpo.key
openssl req -new -md_gost12_256 -key web.au-team.irpo.key -out web.au-team.irpo.csr
```

```
root@hq-srv:/home/user/test.d# openssl req -new -md_gost12_256 -key web.au-team.irpo.key -out web.au-team.irpo.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Tatarstan
Locality Name (eg, city) []:Kazan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:au-team.irpo
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:web.au-team.irpo
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@hq-srv:/home/user/test.d#
```

```
openssl req -new -md_gost12_256 -key docker.au-team.irpo.key -out docker.au-team.irpo.csr
```

```
root@hq-srv:/home/user/test.d# openssl req -new -md_gost12_256 -key docker.au-team.irpo.key -out docker.au-team.irpo.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Tatarstan
Locality Name (eg, city) []:Kazan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:au-team.irpo
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:docker.au-team.irpo
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@hq-srv:/home/user/test.d#
```

```
openssl x509 -req -in web.au-team.irpo.csr -CA ca.cer -CAkey ca.key -CAcreateserial -out web.au-team.irpo.cer -days 30
openssl x509 -req -in docker.au-team.irpo.csr -CA ca.cer -CAkey ca.key -CAcreateserial -out docker.au-team.irpo.cer -days 30
```

Перекидываем файлы с hq-srv на isp и hq-cli (пароль root):

```
scp web.au-team.irpo.key user@172.16.2.1:/tmp
scp web.au-team.irpo.cer user@172.16.2.1:/tmp
scp docker.au-team.irpo.key user@172.16.2.1:/tmp
scp docker.au-team.irpo.cer user@172.16.2.1:/tmp
scp ca.cer user@192.168.200.2:/tmp
```

На isp копируем файлы:

```
mkdir /etc/nginx/ssl
cp /tmp/web.au-team.irpo.* /etc/nginx/ssl
cp /tmp/docker.au-team.irpo.* /etc/nginx/ssl
```

Добавить в nano /etc/nginx/sites-available/web.au-team.irpo

```
server {
        listen 443 ssl;
        server_name web.au-team.irpo;
        ssl_certificate /etc/nginx/ssl/web.au-team.irpo.cer;
        ssl_certificate_key /etc/nginx/ssl/web.au-team.irpo.key;
        ssl_ciphers GOST2012-GOST8912-GOST8912:HIGH:MEDIUM;
        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_prefer_server_ciphers on;
        location / {
                proxy_pass http://192.168.100.2:80;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
```

```
                auth_basic "Restricted area";
                auth_basic_user_file /etc/nginx/.htpasswd;
                sub_filter 'http://' 'https://';
                sub_filter_once off;
                sub_filter_types text/css text/javascript application/javascript;
        }
}
```

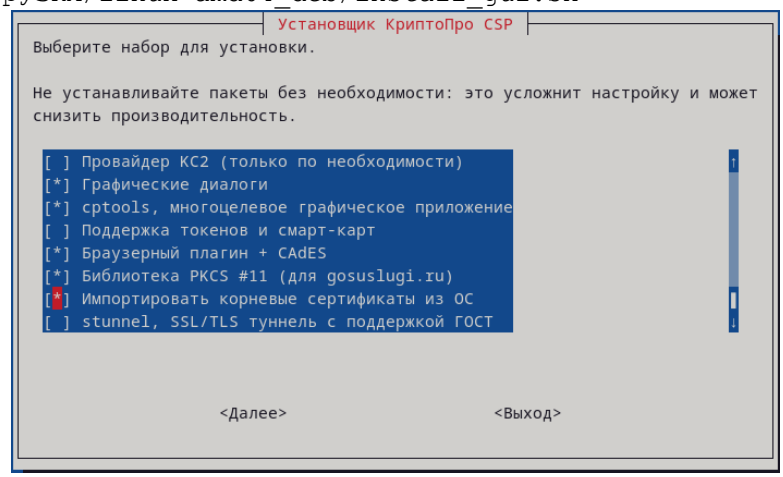
Редактируем файл nano /etc/nginx/sites-available/docker.au-team.irpo

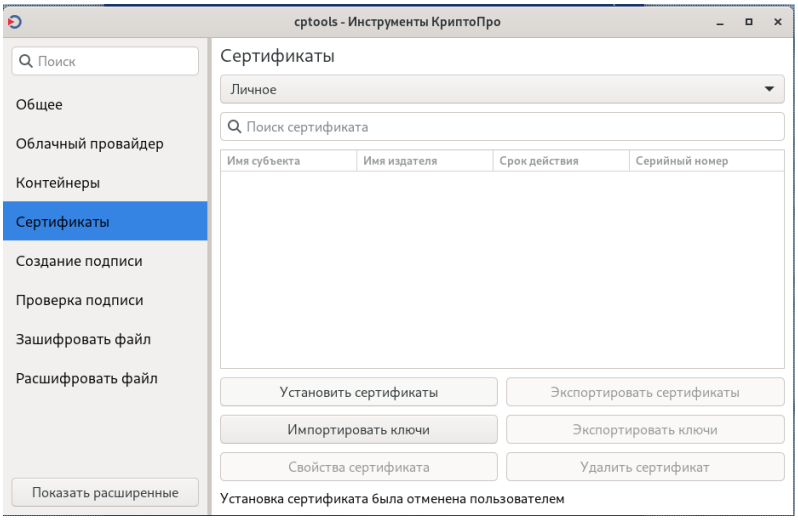
```
server {
        listen 443 ssl;
        server_name docker.au-team.irpo;
        ssl_certificate /etc/nginx/ssl/docker.au-team.irpo.cer;
        ssl_certificate_key /etc/nginx/ssl/docker.au-team.irpo.key;
        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        location / {
                proxy_pass http://192.168.255.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
                sub_filter 'http://' 'https://';
                sub_filter_once off;
                sub_filter_types text/css text/javascript application/javascript;
    }
}
```

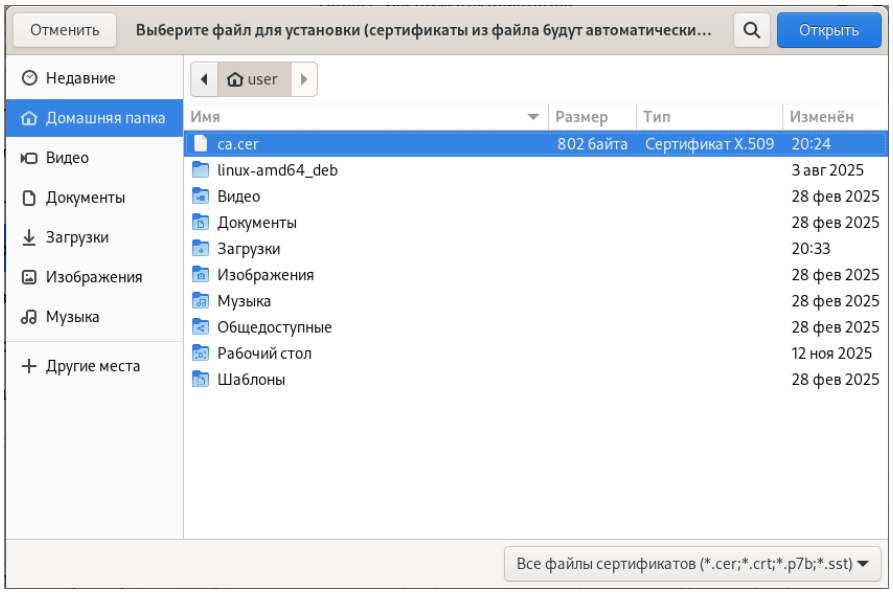
ln -s /etc/nginx/sites-available/web.au-team.irpo /etc/nginx/sites-enabled/
ln -s /etc/nginx/sites-available/docker.au-team.irpo /etc/nginx/sites-enabled/

Настройка на hq-cli:
Ссылка на скачивание криптопро : https://cryptopro.ru/products/csp
Обеспечиваем на клиенте доверие центру сертификации:

```
cp /tmp/ca.cer /home/user
tar -xzvf /home/user/Загрузки/linux-amd64_deb.tgz -C /home/user/Загрузки
sudo /home/user/Загрузки/linux-amd64_deb/install_gui.sh
```







Перенастройте ip-туннель с базового до уровня туннеля, обеспечивающего шифрование трафика (3 задание).

Установка StrongSwan на маршрутизаторе hq-rtr и br-rtr:

```
apt install strongswan strongswan-swanctl -y
```

Конфигурация IPsec на HQ-RTR nano /etc/ipsec.conf (изначальное убрать):

```
# /etc/ipsec.conf - HQ-RTR
config setup
    charondebug="ike 2, knl 2, cfg 2"
    uniqueids=no
conn %default
    keyexchange=ikev2
    ike=aes256-sha2_256-modp2048!
    esp=aes256-sha2_256!
    leftauth=psk
    rightauth=psk
    auto=start
    dpdaction=restart
    closeaction=restart
# Transport mode for GRE encryption
conn gre-encrypt
    left=172.16.1.2
    leftid=@hq-rtr.au-team.irpo
```

```
    right=172.16.2.2
    rightid=@br-rtr.au-team.irpo
    type=transport
    authby=psk
    esp=aes256-sha2_256!
    ike=aes256-sha2_256-modp2048!
    keyexchange=ikev2
    leftprotoport=gre
    rightprotoport=gre
    leftfirewall=yes
    rightfirewall=yes
```

На HQ-RTR в файле nano /etc/ipsec.secrets

```
@hq-rtr.au-team.irpo @br-rtr.au-team.irpo : PSK "P@ssw0rd"
```

Конфигурация IPsec на BR-RTR nano /etc/ipsec.conf (изначальное убрать):

```
# /etc/ipsec.conf - BR-RTR
config setup
    charondebug="ike 2, knl 2, cfg 2"
    uniqueids=no
conn %default
    keyexchange=ikev2
    ike=aes256-sha2_256-modp2048!
    esp=aes256-sha2_256!
    leftauth=psk
    rightauth=psk
    auto=start
    dpdaction=restart
    closeaction=restart
# Transport mode for GRE encryption
conn gre-encrypt
    left=172.16.2.2
    leftid=@br-rtr.au-team.irpo
    right=172.16.1.2
    rightid=@hq-rtr.au-team.irpo
    type=transport
    authby=psk
    esp=aes256-sha2_256!
    ike=aes256-sha2_256-modp2048!
    keyexchange=ikev2
    leftprotoport=gre
    rightprotoport=gre
    leftfirewall=yes
    rightfirewall=yes
```

На br-rtr в файле nano /etc/ipsec.secrets

```
@br-rtr.au-team.irpo @hq-rtr.au-team.irpo : PSK "P@ssw0rd"
```

Запуск и проверка

```
systemctl restart ipsec
systemctl enable ipsec
systemctl status ipsec
```

Настройте межсетевой экран на маршрутизаторах HQ-RTR и BR-RTR на сеть в сторону ISP (4 задание).

Пишем на hq-rtr и br-rtr ахахаха

```
/sbin/iptables -F
/sbin/iptables -t nat -F
/sbin/iptables -t mangle -F
```

```
/sbin/iptables -t raw -F
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -A INPUT  -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
/sbin/iptables -A INPUT   -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A OUTPUT  -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
/sbin/iptables -A INPUT  -p icmp -j ACCEPT
/sbin/iptables -A FORWARD -p icmp -j ACCEPT
/sbin/iptables -A OUTPUT -p icmp -j ACCEPT
/sbin/iptables -A INPUT  -p ospf -j ACCEPT
/sbin/iptables -A FORWARD -p ospf -j ACCEPT
/sbin/iptables -A OUTPUT -p ospf -j ACCEPT
/sbin/iptables -A INPUT  -p gre -j ACCEPT
/sbin/iptables -A FORWARD -p gre -j ACCEPT
/sbin/iptables -A OUTPUT -p gre -j ACCEPT
/sbin/iptables -A INPUT  -p 50 -j ACCEPT
/sbin/iptables -A OUTPUT -p 50 -j ACCEPT
/sbin/iptables -A FORWARD -p 50 -j ACCEPT
/sbin/iptables -A INPUT  -p 51 -j ACCEPT
/sbin/iptables -A OUTPUT -p 51 -j ACCEPT
/sbin/iptables -A FORWARD -p 51 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 500 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --dport 500 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 500 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 4500 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --dport 4500 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 4500 -j ACCEPT

/sbin/iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 53 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 53 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 53 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp --dport 53 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp -m multiport --dports 80,443,8080 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -m multiport --dports 80,443,8080 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -m multiport --dports 80,443,8080 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --sport 68 --dport 67 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --sport 67 --dport 68 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --sport 68 --dport 67 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --sport 67 --dport 68 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --sport 68 --dport 67 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --sport 67 --dport 68 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp --dport 2049 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 2049 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 2049 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 2049 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --dport 2049 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 2049 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 123 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --dport 123 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 123 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 514 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp --dport 514 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --dport 514 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 514 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 514 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 514 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp -m multiport --dports 22,2026 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -m multiport --dports 22,2026 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -m multiport --dports 22,2026 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp -m multiport --dports 10050,10051 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -m multiport --dports 10050,10051 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -m multiport --dports 10050,10051 -j ACCEPT
```

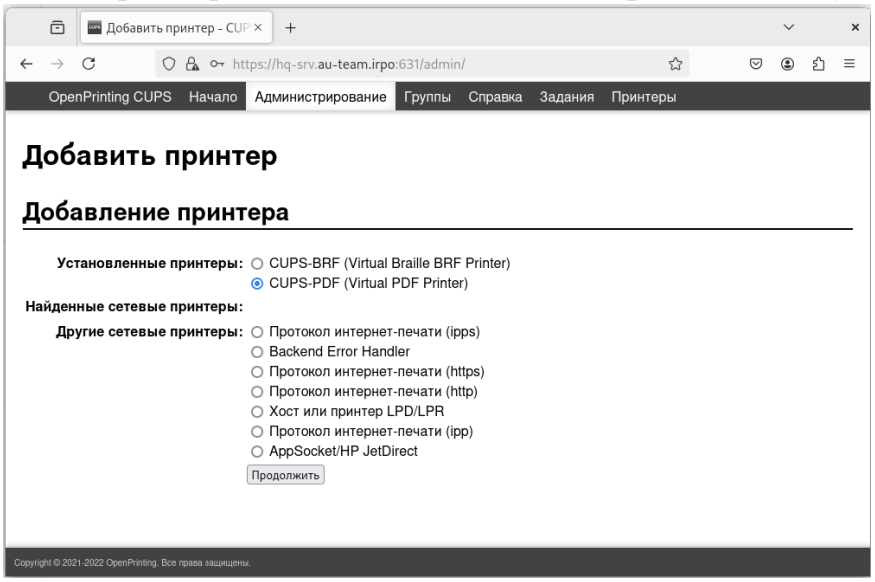
```
/sbin/iptables -A INPUT  -p tcp --dport 631 -j ACCEPT
/sbin/iptables -A INPUT  -p udp --dport 631 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 631 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp --dport 631 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 631 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 631 -j ACCEPT
/sbin/iptables -A INPUT  -p tcp -m multiport --dports 88,389,636,3268,3269,139,445,464
-j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -m multiport --dports 88,389,636,3268,3269,139,445,464
-j ACCEPT
/sbin/iptables -A FORWARD -p tcp -m multiport --dports 88,389,636,3268,3269,139,445,464
-j ACCEPT
/sbin/iptables -A INPUT  -p udp -m multiport --dports 88,137,138,464 -j ACCEPT
/sbin/iptables -A OUTPUT -p udp -m multiport --dports 88,137,138,464 -j ACCEPT
/sbin/iptables -A FORWARD -p udp -m multiport --dports 88,137,138,464 -j ACCEPT
/usr/sbin/iptables-save > /etc/iptables/rules.v4
```

Настройте принт-сервер cups на сервере HQ-SRV (5 задание).

Установка cups:

```
apt install cups cups-pdf printer-driver-cups-pdf -y
/usr/sbin/usermod -a -G lpadmin sshuser
/usr/sbin/cupsctl --share-printers --remote-any
```

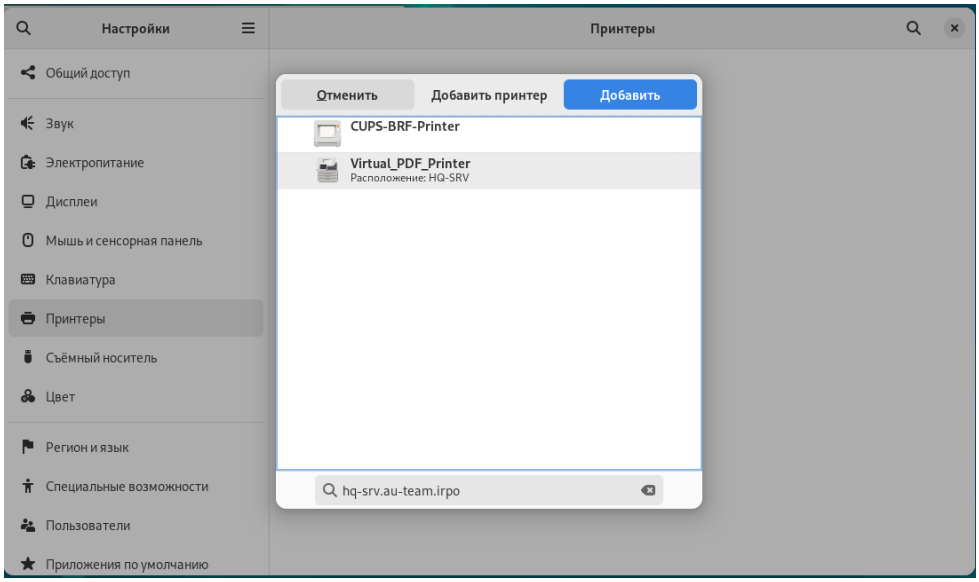
В веб-интерфейсе создаём новый виртуальный принтер (127.0.0.1:631/admin, логин sshuser, пароль P@ssw0rd).
Необходимо добавить принтер CUPS-PDF, дальше настройки на похуй).

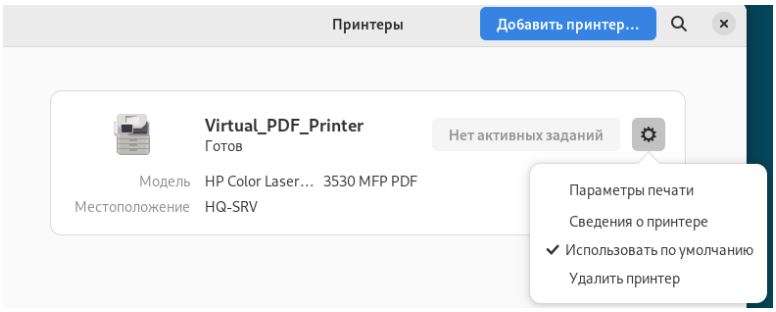


На hq-srv для сохранения настроек:

```
/usr/sbin/cupsctl --share-printers
```

Добавление принтера на HQ-CLI через настройки





Реализуйте логирование при помощи rsyslog на устройствах HQ-RTR, BR-RTR, BR-SRV (6 задание).

Установка rsyslog на hq-srv, hq-rtr, br-rtr, br-srv:

```
apt install rsyslog -y
```

Редактируем файл nano /etc/rsyslog.conf на hq-srv (добавляем):

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# Правила для сохранения логов удаленных хостов
$template RemoteLogs,"/opt/%HOSTNAME%/%$YEAR%-%$MONTH%-%$DAY%.log"

if $fromhost-ip != '127.0.0.1' and $fromhost-ip != '192.168.100.2' then {
    if $syslogseverity <= 4 then {
        ?RemoteLogs
        stop
    }
}
```

Добавляем в конец файла nano /etc/rsyslog.conf на br-srv, br-rtr, hq-rtr:

```
*.* @192.168.100.2:514
```

Перезапускаем rsyslog на всех устройствах:

```
systemctl restart rsyslog
```

На сервере HQ-SRV реализуйте мониторинг устройств с помощью открытого программного обеспечения (7 задание).

В файле nano /etc/bind/zones/db.au-team.irpo добавляем строку:

```
mon.au-team.irpo.       IN      CNAME   hq-srv.au-team.irpo.
```

Увеличиваем Serial и перезапускаем сервис bind9:

```
systemctl restart bind9
```

Установка Zabbix:

```
wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb
export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin:/bin:/usr/bin
dpkg -i zabbix-release_6.4-1+debian12_all.deb
apt update
apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

Настройка MariaDB:

mariadb - отдельно

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'P@ssw0rd';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
FLUSH PRIVILEGES;
EXIT;

zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -pP@ssw0rd zabbix
```

Файл: nano /etc/zabbix/zabbix_server.conf отредактируем (расскоментить, поменять) следующие строки:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=P@ssw0rd
```

Создаём файл nano /etc/apache2/sites-available/zabbix.conf

```
<VirtualHost *:80>
    ServerName mon.au-team.irpo
    DocumentRoot /usr/share/zabbix
    <Directory /usr/share/zabbix>
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/zabbix_error.log
    CustomLog ${APACHE_LOG_DIR}/zabbix_access.log combined
</VirtualHost>
```

Включаем сайт apache2:

```
a2ensite zabbix.conf
a2enmod rewrite
systemctl restart apache2
```

Перезапуск Zabbix-server:

```
systemctl restart zabbix-server
systemctl enable zabbix-server
```

Устанавливаем агенты на hq-srv и br-srv:

```
wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb
export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin:/bin:/usr/bin
dpkg -i zabbix-release_6.4-1+debian12_all.deb
apt update
apt install zabbix-agent
```

Настройка агента на hq-srv nano /etc/zabbix/zabbix_agentd.conf

```
PidFile=/var/run/zabbix/zabbix_agentd.pid
LogFile=/var/log/zabbix/zabbix_agentd.log
LogFileSize=0
Server=192.168.100.2
ServerActive=192.168.100.2
Hostname=hq-srv.au-team.irpo
Timeout=30
EnableRemoteCommands=1
Include=/etc/zabbix/zabbix_agentd.d/*.conf
```

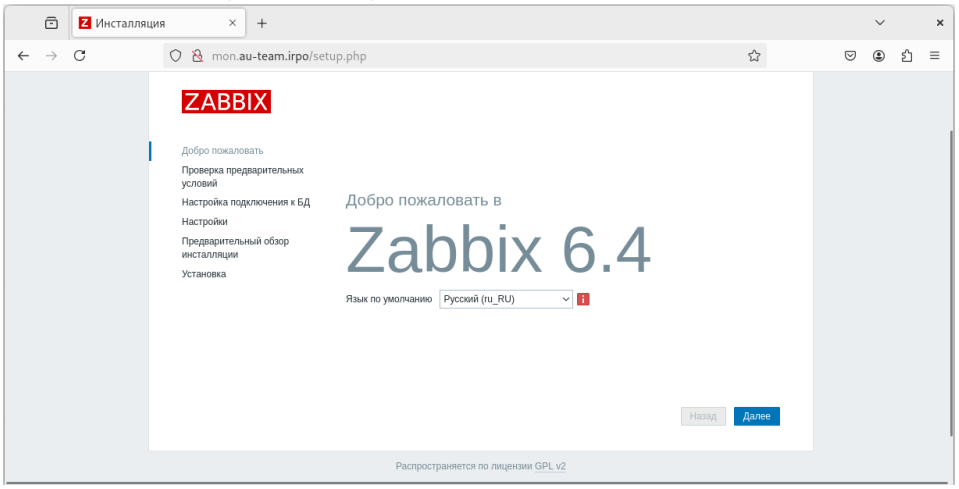
Настройка агента на br-srv nano /etc/zabbix/zabbix_agentd.conf

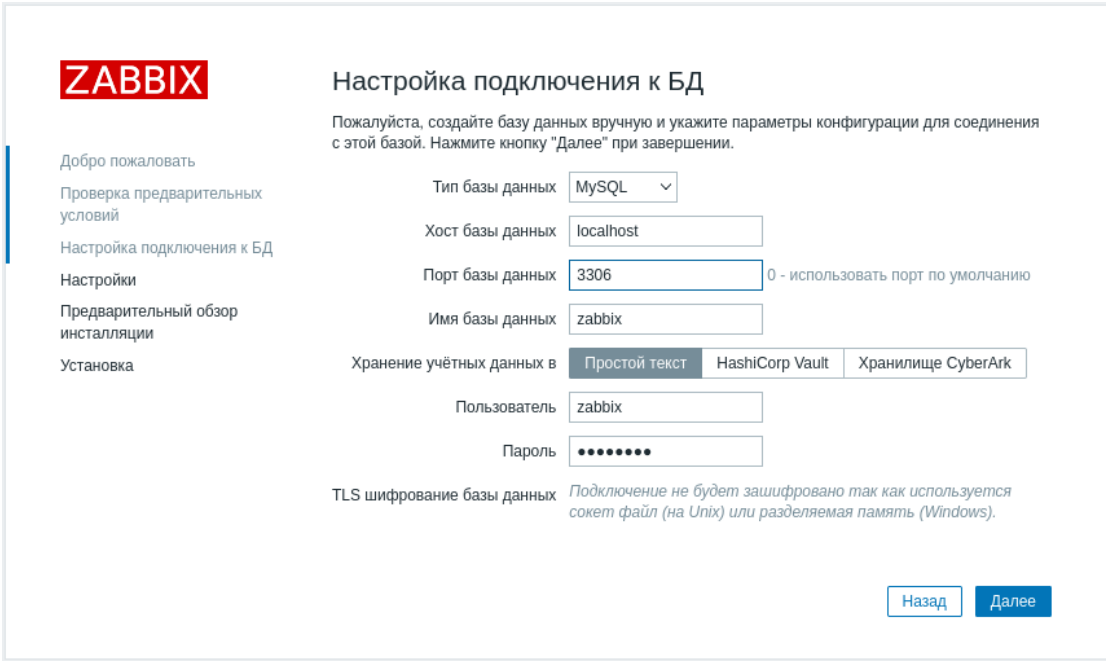
```
PidFile=/var/run/zabbix/zabbix_agentd.pid
LogFile=/var/log/zabbix/zabbix_agentd.log
LogFileSize=0
Server=192.168.100.2
ServerActive=192.168.100.2
Hostname=br-srv.au-team.irpo
Timeout=30
EnableRemoteCommands=1
Include=/etc/zabbix/zabbix_agentd.d/*.conf
```

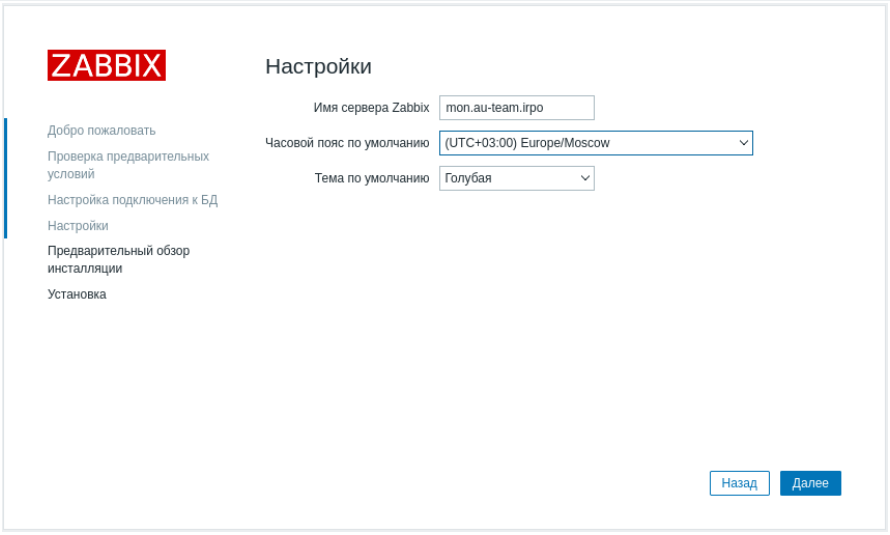
Перезапуск агента Zabbix:

```
systemctl enable zabbix-agent
systemctl restart zabbix-agent
```

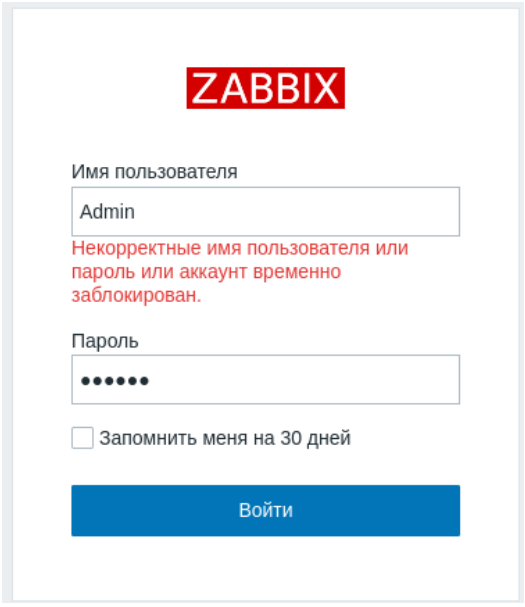
На сервере выполняем web-установку Zabbix:



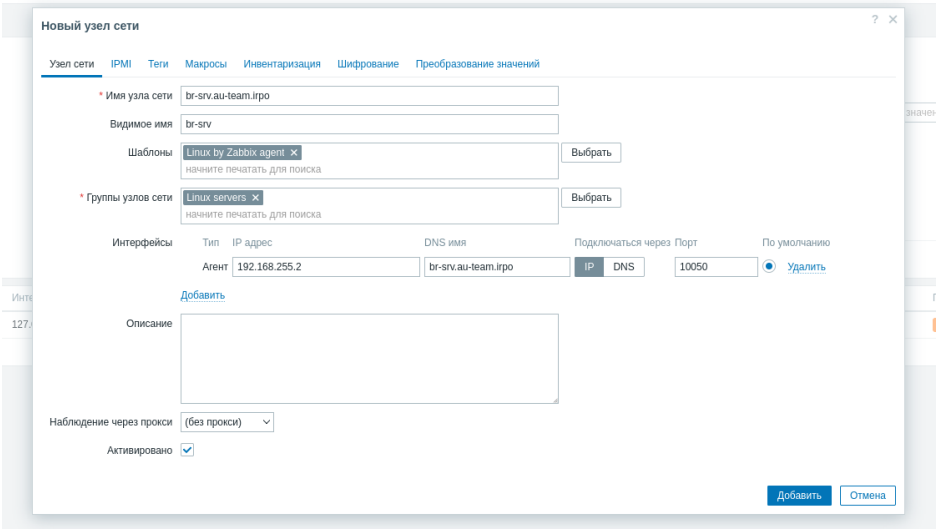


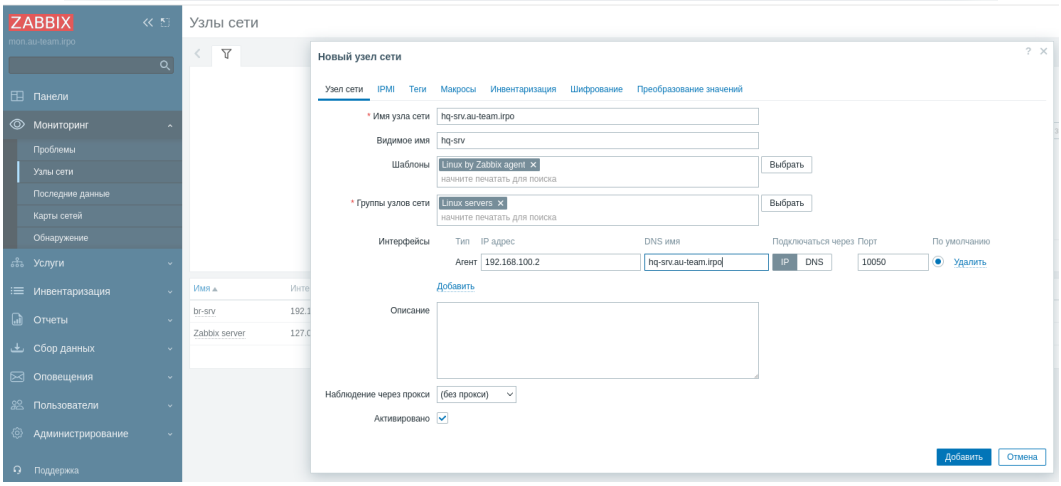


Вводим учётные данные по умолчанию логин Admin и пароль zabbix

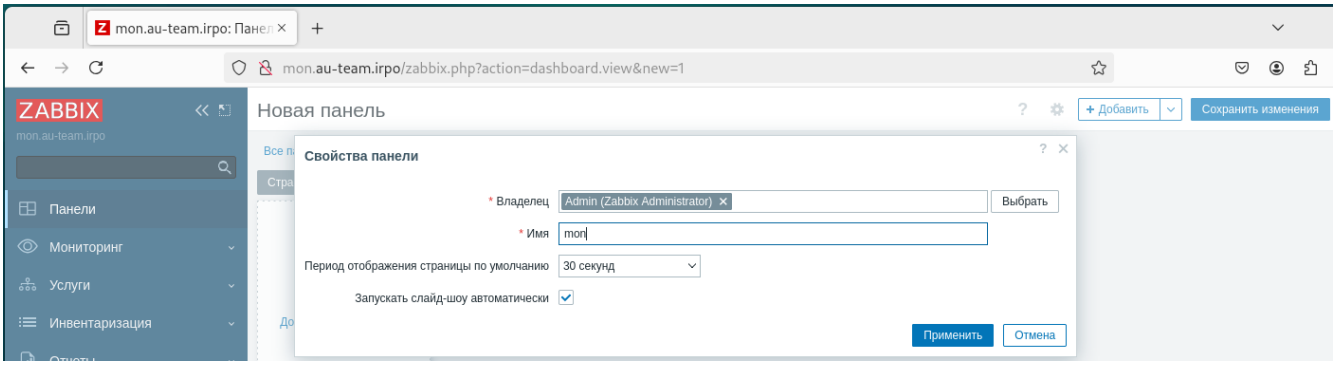


Создание узлов сети серверов hq-srv и br-srv:

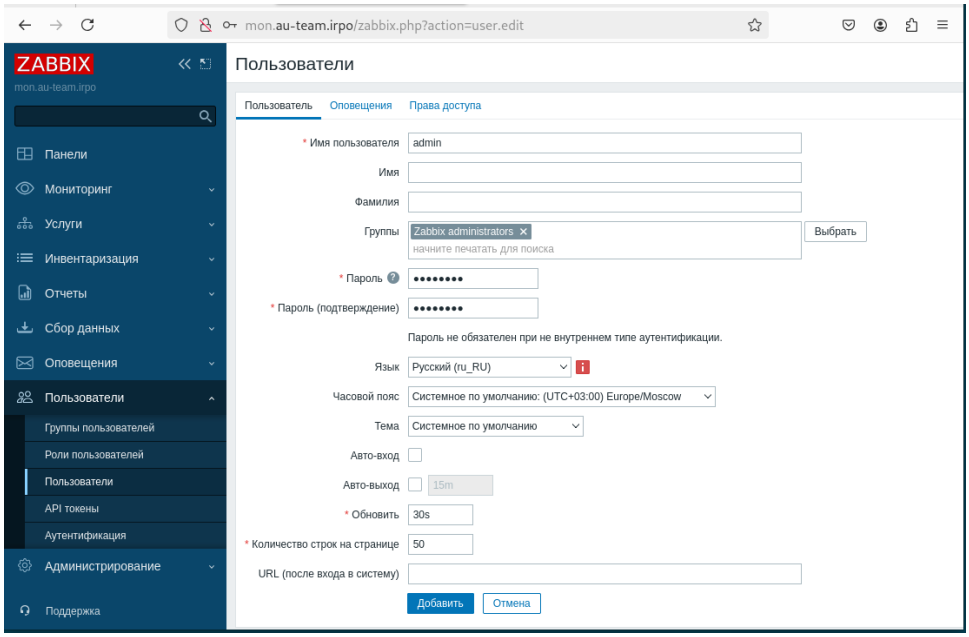




Создаём панель:



Создание нового пользователя admin с паролем P@ssw0rd123, указываем права доступа



Реализуйте механизм инвентаризации машин HQ-SRV и HQ-CLI через Ansible на BR-SRV (8 задание).

Создаём нужные директории:

```
mkdir /etc/ansible/PC-INFO
mkdir /etc/ansible/playbook
```

Создаём и редактируем файл nano /etc/ansible/playbook/get_hostname_address.yml

```
- name: получение данных с хоста
  hosts: hq-srv,hq-cli
  gather_facts: yes
  tasks:
    - name: создание отчета на BR-SRV
      copy:
        dest: /etc/ansible/PC-INFO/{{ ansible_hostname }}.yml
        content: |
          computer_name: {{ ansible_hostname }}
          ip_address: {{ ansible_default_ipv4.address }}
      delegate_to: localhost
      run_once: false
```

Запускаем playbook:

```
ansible-playbook /etc/ansible/playbook/get_hostname_address.yml
cat /etc/ansible/cat /etc/ansible/PC-INFO/hq-cli.yml
cat /etc/ansible/cat /etc/ansible/PC-INFO/hq-srv.yml
```

На HQ-SRV настройте программное обеспечение fail2ban для защиты ssh (9 задание).

Установка fail2ban:

```
apt install fail2ban -y
```

Создаём и редактируем файл nano /etc/fail2ban/jail.local

```
[DEFAULT]
bantime = 60
```

```
findtime = 600
maxretry = 3
backend = auto
banaction = iptables-multiport
action = %(action_)s
[sshd]
enabled = true
port = 2026
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 60
findtime = 600
[sshd-ddos]
enabled = false
```

Перезапуск fail2ban:

```
systemctl restart fail2ban
```

Настройка резервного копирования директории сервера HQ-SRV (10 задание).

На HQ-CLI:

```
apt update
apt install -y borgbackup openssh-server
systemctl enable --now ssh
mkdir -p /backup/irpo/borg
chmod 755 /backup
chmod 755 /backup/irpo
chmod 755 /backup/irpo/borg
sudo useradd -m -s /bin/bash backupsvc
passwd -l backupsvc
chown -R backupsvc:backupsvc /backup/irpo
mkdir -p /home/backupsvc/.ssh
chmod 700 /home/backupsvc/.ssh
touch /home/backupsvc/.ssh/authorized_keys
chmod 600 /home/backupsvc/.ssh/authorized_keys
chown -R backupsvc:backupsvc /home/backupsvc/.ssh
```

На HQ-SRV:

```
sudo useradd -m -s /bin/bash irpoadmin
echo 'irpoadmin:P@ssw0rd' | sudo chpasswd
echo 'irpoadmin ALL=(ALL) NOPASSWD:ALL' > /etc/sudoers.d/irpoadmin
chmod 440 /etc/sudoers.d/irpoadmin
apt update
apt install -y borgbackup mariadb-client openssh-client gzip
sudo -iu irpoadmin
mkdir -p ~/.ssh && chmod 700 ~/.ssh
ssh-keygen -t ed25519 -N "" -f ~/.ssh/borg_irpo
cat ~/.ssh/borg_irpo.pub
```

На HQ-CLI открыть файл nano /home/backupsvc/.ssh/authorized_keys

В HQ-SRV выйдет строка с ключом. Сделать из неё **одну строку** такого вида (вставь свой ключ после параметров):

```
command="borg serve --append-only --restrict-to-path /backup/irpo/borg",restrict,no-pty,no-port-forwarding,no-agent-forwarding,no-X11-forwarding ваш ключ
```

На HQ-SRV:

```
sudo -iu irpoadmin
export BORG_RSH="ssh -i /home/irpoadmin/.ssh/borg_irpo -o IdentitiesOnly=yes"
export BORG_PASSPHRASE='P@ssw0rd'
borg init --encryption=repokey-blake2 backupsvc@192.168.200.2:/backup/irpo/borg
```

B nano /usr/local/sbin/irpo-backup-etc.sh

```
#!/bin/bash
set -euo pipefail
export BORG_RSH="ssh -i /home/irpoadmin/.ssh/borg_irpo -o IdentitiesOnly=yes"
export BORG_PASSPHRASE='P@ssw0rd'
REPO="backupsvc@192.168.200.2:/backup/irpo/borg"
ARCH="irpo-etc-$(date +%F_%H-%M-%S)"
borg create --stats --compression zstd,6 "$REPO::$ARCH" /etc


chmod +x /usr/local/sbin/irpo-backup-etc.sh
sudo -iu irpoadmin /usr/local/sbin/irpo-backup-etc.sh
```

B nano /usr/local/sbin/irpo-backup-webdb.sh

```
#!/bin/bash
set -euo pipefail

export BORG_RSH="ssh -i /home/irpoadmin/.ssh/borg_irpo -o IdentitiesOnly=yes"
export BORG_PASSPHRASE='P@ssw0rd'
REPO="backupsvc@192.168.200.2:/backup/irpo/borg"
TS="$(date +%F_%H-%M-%S)"
DUMP="/tmp/webdb_${TS}.sql.gz"

if mariadb -u root -e "USE webdb;" >/dev/null 2>&1; then
  mariadb-dump -u root --single-transaction --routines --triggers webdb | gzip -9 >
"$DUMP"
else
  mariadb-dump -u web -p'P@ssw0rd' --single-transaction --routines --triggers webdb |
gzip -9 > "$DUMP"
fi

ARCH="irpo-webdb-${TS}"
borg create --stats --compression zstd,6 "$REPO::$ARCH" "$DUMP"
rm -f "$DUMP"


chmod +x /usr/local/sbin/irpo-backup-webdb.sh
sudo -iu irpoadmin /usr/local/sbin/irpo-backup-webdb.sh
sudo -iu irpoadmin
export BORG_RSH="ssh -i /home/irpoadmin/.ssh/borg_irpo -o IdentitiesOnly=yes"
export BORG_PASSPHRASE='P@ssw0rd'
borg list backupsvc@192.168.200.2:/backup/irpo/borg
```