**Модуль 1**

Задание 1

|  |  |  |  |
| --- | --- | --- | --- |
|  | IP-адрес | К устройству | Шлюз по умолчанию |
| ISP | Внешний  172.16.4.1/28  172.16.5.1/28 | HQ-RTR  BR-RTR | Внешний |
| HQ-RTR | 172.16.4.2/28  192.168.20.1/26 192.168.20.97/28 192.168.20.113/29  192.168.20.121/30 | ISP  HQ-SRV (100)  HQ-CLI (200)  (VLAN 999)  (IP-tunnel) | 172.16.4.1 |
| HQ-SRV | 192.168.20.2/28 |  | 192.168.20.1 |
| HQ-CLI | 192.168.20.98/28 |  | 192.168.20.97 |
| BR-RTR | 172.16.5.2/28  192.168.20.65/27  192.168.20.122/30 | ISP  BR-SRV  (IP-tunnel) | 172.16.5.1 |
| BR-SRV | 192.168.20.66/27 |  | 192.168.20.65 |
| Vlan100 | 192.168.20.0/26 |  |  |
| Vlan200 | 192.168.20.96/28 |  |  |
| IP-tunnel | 192.168.20.120/30 |  |  |
| Vlan999 | 192.168.20.112/29 |  |  |
| BR-RTR <-> BR-SRV | 192.168.20.64 |  |  |

# приватные адреса: 192.168.. /172.16.. /10.10..

# посмотреть все записи папки:

sudo whoami

sudo apt-get update –y

cat /etc/net/ifaces/ens18/\*

vim /etc/sysconfig/iptables

ip -c a ; смотрим mac-адреса

ip r #показывает известныe сети -?

>> допишет (> перезапишет)

ПРОДУМАТЬ СКРИНЫ И СДЕЛАТЬ ПОДПИСИ!!!

Сделать hostname и юзера – показать && BR-RTR созд. Пользователь и задан hostname

# ISP:;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

root – toor

hostnamectl hostname ISP.au-teame.irpo; exec bash

apt-get update

apt-get install NetworkManager-tui -y

apt-get install -y iptables

systemctl enable --now NetworkManager

systemctl restart network

nmtui => ens19: ProfileName: HQ

ADDRESSES: 172.16.4.1/28

DNS servers: 192.168.20.2

Search Domains: au-team.irpo

nmtui => ens20: ProfileName: BR

ADDRESSES: 172.16.5.1/28

DNS servers: 192.168.20.2

Search Domains: au-team.irpo

hostname: ISP.au-team.irpo

activate -> dactivate -> activate

systemctl restart network

systemctl restart NetworkManager

iptables -t nat -j MASQUERADE -A POSTROUTING -o ens18

iptables-save >> /etc/sysconfig/iptables

iptables-save

vim /etc/net/sysctl.conf =>

...

net.ipv4.ip\_forward = 0 => net.ipv4.ip\_forward = 1

...

systemctl restart network

&& ip -br a && Задан hostname и настроенs ens19 b ens20

# BRRTR:;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

root - toor

hostnamectl hostname BR-RTR.au-team.irpo ; exec bash

##### 3 – users

&& cat /etc/passwd BR-RTR созд. Пользователь и задан hostname

ip -br a

vim /etc/net/ifaces/ens18/options ; меняем dhcp на static

echo '172.16.5.2/28' >> /etc/net/ifaces/ens18/ipv4address

echo 'default via 172.16.5.1' >> /etc/net/ifaces/ens18/ipv4route

echo 'nameserver 8.8.8.8' >> /etc/net/ifaces/ens18/resolv.conf

systemctl restart network

##### настройка ens19 для BR-SRV

mkdir /etc/net/ifaces/ens19

cp /etc/net/ifaces/ens18/options /etc/net/ifaces/ens19/options

vim /etc/net/ifaces/ens19/options => NM\_CONTROLLED=yes ; меняем dhcp на static

vim /etc/net/sysctl.conf =>

...

net.ipv4.ip\_forward = 0 => net.ipv4.ip\_forward = 1

...

systemctl restart network

ping 8.8.8.8

apt-get update -y

apt-get install NetworkManager-tui -y

systemctl enable --now NetworkManager

nmtui => ens19: ProfileName: BR

ADDRESSES: 192.168.20.65/27

DNS servers: 192.168.20.2

Search Domains: au-team.irpo

hostname: BR-RTR.au-team.irpo

##### 6 ip-tunnel && Настройка GRE на BR-RTR

nmtui => "add" => IP tunnel

ProfileName: gre1

device: gre1

Parent: ens18

LocalIp: 172.16.5.2

RemotIp: 172.16.4.2

ipv4 configuration Addresses: 192.168.20.122/30

activate -> dactivate -> activate

systemctl restart network

systemctl restart NetworkManager

ls /etc/NetworkManager/system-connections => gre1.nmconnection

vim /etc/NetworkManager/system-connections/gre1.nmconnection => после строчки remote добавить ttl=128

nmcli connection edit gre1

nmcli => set ip-tunnel.ttl 64

save

quit

##### 7 Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса.

apt-get install -y frr

vim /etc/frr/daemons => ospfd=yes

systemctl restart frr

systemctl enable frr

vtysh

conf t

ip forwarding

router ospf

network 192.168.20.120/30 area 0 #IP-tunnel remote

network 192.168.20.64/27 area 0 #сеть br-rtr <-> br-srv 192.168.20.65

do sh run #проверка

passive-interface default

ex

int gre1

no ip ospf passive

ex

ex

wr

ex

# посленастройки frr на HQ-RTR:

systemctl restart frr.service

systemctl restart network

systemctl restart NetworkManager

&& ping 192.168.20.122 && проверка работы ip-туннеля

###### 8 Настройка динамической трансляции адресов.

apt-get install -y iptables

iptables -t nat -j MASQUERADE -A POSTROUTING

iptables-save >> /etc/sysconfig/iptables

systemctl enable --now iptables

&& iptables-save && Настройка динамической трансляции адресов

; проверяем интернет на BR-SRV

###### настройка времени 11

apt-get install -y chrony

vim /etc/chrony.conf => server 192.168.20.1 iburst + комментировать pool pool.ntp.org iburst

systemctl restart chronyd

#. проверка после настройки HQ-RTR:

&& chronyc tracking && проверка настройки времени

; vim /etc/net/ifaces/ens19/options ; меняем dhcp на static NM\_CONTRILLED=yes;

; cat /etc/net/ifaces/ens18/ipv4address => 172.16.5.2/28

; cat /etc/net/ifaces/ens18/ipv4route => default via 172.16.5.1 ; проверяем шлюз

; vim /etc/net/ifaces/ens19/resolv.conf => nameserver 8.8.8.8

; systemctl restart network

; ping 172.16.5.1

; ping 172.16.4.2

; ping 8.8.8.8

; ping 192.168.100.1

; systemctl restart network

; systemctl restart NetworkManager

# HQRTR:;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

root - toor

ip -br a

hostnamectl hostname HQ-RTR.au-team.irpo ; exec bash

##### 3 - users

&& cat /etc/passwd HQ-RTR созд. Пользователь и задан hostname

ens18:

vim /etc/net/ifaces/ens18/options =>

BOOTPROTO=static

...

SYSTEMD\_BOOTPROTO=static

echo '172.16.4.2/28' >> /etc/net/ifaces/ens18/ipv4address

echo 'default via 172.16.4.1' >> /etc/net/ifaces/ens18/ipv4route

echo 'nameserver 8.8.8.8' >> /etc/net/ifaces/ens18/resolv.conf

vim /etc/net/sysctl.conf =>

...

net.ipv4.ip\_forward = 0 => net.ipv4.ip\_forward = 1

...

systemctl restart network

ip -br a

ping 172.16.4.1

ping 8.8.8.8 # проверка связи с интернетом

###### 4 VLAN

apt-get install -y openvswitch

systemctl enable --now openvswitch

ovs-vsctl add-br HQ-SW

ovs-vsctl list-br

ovs-vsctl add-port HQ-SW ens19

ovs-vsctl add-port HQ-SW vlan100 tag=100 -- set interface vlan100 type=internal

ovs-vsctl add-port HQ-SW vlan200 tag=200 -- set interface vlan200 type=internal

ovs-vsctl add-port HQ-SW vlan999 tag=999 -- set interface vlan999 type=internal

mkdir /etc/net/ifaces/vlan100

mkdir /etc/net/ifaces/vlan200

mkdir /etc/net/ifaces/vlan999

cp /etc/net/ifaces/ens18/options /etc/net/ifaces/vlan100/options

cp /etc/net/ifaces/ens18/options /etc/net/ifaces/vlan200/options

cp /etc/net/ifaces/ens18/options /etc/net/ifaces/vlan999/options

echo '192.168.20.1/26' >> /etc/net/ifaces/vlan100/ipv4address

echo '192.168.20.97/28' >> /etc/net/ifaces/vlan200/ipv4address

echo '192.168.20.113/29' >> /etc/net/ifaces/vlan999/ipv4address

systemctl restart network

&& ip -br a && настройка адресации и vlan

##### 6 ip-tunnel && Настройка GRE на HQ-RTR

apt-get install NetworkManager-tui –y

systemctl enable --now NetworkManager

nmtui => "add" => ip tunnel

ProfileName: gre1

MODE: GRE

device: gre1

Parent: ens18

LocalIp: 172.16.4.2

RemotIp: 172.16.5.2

ipv4 configuration => manual => Addresses: 192.168.20.121/30

hostname: HQ-RTR.au-teame.irpo

activate -> dactivate -> activate

ls /etc/NetworkManager/system-connections => gre1.nmconnection

vim /etc/NetworkManager/system-connections/gre1.nmconnection => после строчки remote добавить ttl=128

reboot

nmcli connection edit BR-RTR

nmcli >>> set ip-tunnel.ttl 64

save

quit

###### 7 Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса.

apt-get update

apt-get install -y frr

vim /etc/frr/daemons => ospfd=yes

systemctl restart frr

systemctl enable --now frr

vtysh #вход

conf t #доступ к редактированию

ip forwarding

router ospf

network 192.168.20.120/30 area 0 #IP-tunnel

network 192.168.20.0/26 area 0 #100

network 192.168.20.96/28 area 0 #200

network 192.168.20.112/29 area 0 #999

do sh run #проверка

passive-interface default

ex

int gre1

no ip ospf passive

ex

ex

wr

ex

systemctl restart network

systemctl restart NetworkManager

&& ping 192.168.20.121 && проверка работы ip-туннеля

##### переход на **BR-RTR**

systemctl restart frr.service #после рестарата на настроенном br-rtr и hq-rtr

ping 192.168.20.122 #ping на **BR-RTR**

###### 8 Настройка динамической трансляции адресов.

apt-get install -y iptables

iptables -t nat -j MASQUERADE -A POSTROUTING

iptables-save >> /etc/sysconfig/iptables

systemctl enable --now iptables

&& iptables-save && Настройка динамической трансляции адресов HQ-RTR

&& проверка связанности сети на HQ-SRW

&& проверка связанности сети на HQ-CLI

&& проверка связанности сети на BR-RTR

###### 9 Настройка протокола динамической конфигурации хостов.

apt-get update

apt-get install -y dhcp-server

vim /etc/sysconfig/dhcpd => DHCPDARGS=vlan200

cp /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf

vim /etc/dhcp/dhcpd.conf => 'example.org' меняем на 'au-team.irpo' и в след. строке меняем два ххх.org на один 192.168.20.2 и раскомичиваем ddns-update-style none; => ddns-update-style interim;

; option domain-name-servers 192.168.20.2, 192.168.20.66

; ниже пишем:

update-static-leases on;

zone au-team.irpo{

primary 192.168.20.2;

}

zone 20.168.192.in-addr.arpa{

primary 192.168.20.2;

}

# zone <обратный ip сети с третьего октета (см. выше)>.in-addr.arpa{

# primary 192.168.20.2;

# } пишем, если у нас различаются третьи октеты в vlan100 и vlan200

# в строчке

subnet 192.168.20.96 netmask 255.255.255.240 { # маска 28

range 192.168.20.98 192.168.20.103;

option routers 192.168.20.97;

}

# для постоянного dhcp для HQ-CLI:

# для DNS HQ-CLI после пинга и проверки DNS: fantasia стираем, пишем:

host HQ-CLI {

hardware ethernet BC:24:11:0B:B4:FE; mac адрес на HQ-CLI (в оборудовании)

fixed-address 192.168.20.98; адрес HQ-CLI

}

; все host и subnet комментируем

systemctl restart dhcpd

systemctl enable dhcpd

systemctl status dhcpd

&& проверка на HQ-CLI + скриншот на всякий

###### 11 настройка времени

timedatectl set-timezone Europe/Moscow

apt-get install -y chrony

vim /etc/chrony.conf => комментировать pool pool.ntp.org iburst

server 192.168.20.1 iburst ;hq-rtr

local stratum 5

allow 192.168.20.0/26 ; 100

allow 192.168.20.96/28 ;200

allow 192.168.20.64/27 ;br-rtr <-> br-srv

allow 192.168.20.120/30 ;br-rtr <-> hq-rtr ip-tunnel

systemctl restart chronyd

# Настройка клиентов синхронизации времени (HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.) на каждом:

apt-get install -y chrony

vim /etc/chrony.conf => server 192.168.20.1 iburst + комментировать pool pool.ntp.org iburst

systemctl restart chronyd

#проверка:

&& chronyc tracking && проверка настройки времени

; vim /etc/net/ifaces/ens18/ipv4address => 172.16.4.2/28

; vim /etc/net/ifaces/ens18/ipv4route => default via 172.16.4.1 ; прописываем шлюз

; vim /etc/net/ifaces/ens18/resolv.conf => nnameserver 192.168.20.2

; domain au-team.irpo (исправить после настройки DNS)

systemctl restart network

; vim /etc/net/ifaces/ens18/resolv.conf

; cat /etc/net/ifaces/ens19/options //проверяем static

; vim /etc/net/ifaces/ens19/ipv4address

; 192.168.100.1/28

; systemctl restart network

ip -br a

# HQSRV;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

root - toor

hostnamectl hostname HQ-SRV.au-team.irpo ; exec bash

vim /etc/net/ifaces/ens18/options ; меняем dhcp на static

echo '192.168.20.2/28' >> /etc/net/ifaces/ens18/ipv4address

echo 'default via 192.168.20.1' >> /etc/net/ifaces/ens18/ipv4route

echo 'nameserver 8.8.8.8' >> /etc/net/ifaces/ens18/resolv.conf

systemctl restart network

&&

ip -br a

ping 192.168.20.1 -c3

ping 8.8.8.8 -c3

&&

##### 3 – users

&& cat /etc/passwd HQ-SRV созд. Пользователь и задан hostname

##### 5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV:

apt-get update

apt-get install openssh-server

cd /etc/openssh

cp ssh\_config ssh\_config.back

vim sshd\_config => port 2024

MaxAuthTries 2

Banner /etc/openssh/banner

AllowUsers sshuser

vim /etc/openssh/banner =>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \* Authorized access only \* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

systemctl restart sshd

&& ping 192.168.20.66 && проверка SSH

apt-get install -y chrony

vim /etc/chrony.conf => server 192.168.20.1 iburst + комментировать pool pool.ntp.org iburst

systemctl restart chronyd

&& chronyc tracking && проверка настройки времени

timedatectl status

###### 10 Настройка DNS для офисов HQ и BR.

; apt-get update -y

apt-get install -y bind

vim /var/lib/bind/etc/options.conf =>

listen-on { any; };

listen-on-v6 { none; };

forwarders { 8.8.8.8; };раском-м

allow-query { any; };

allow-recursion { any; };

vim /var/lib/bind/etc/rfc1912.conf =>

zone "au-team.irpo" {

type master;

file "au-team"; (au-team.db)

allow-update { any; };

allow-transfer { any; };

; localdomain удалем

zone "20.168.192.in-addr.arpa" {

type master;

file "20.in-addr.arpa";

allow-update { any; }

}

# ненужные зоны удаляем

&& настройка DNS

# Копируем файл empty (шаблон) в au-team,

# 100.168.192.in-addr.arpa, 200.168.192.in-addr.arpa:

cd /var/lib/bind/etc/zone

ls -la

cp empty au-team

vim au-team => @ IN SOA hq-srv.au-team.irpo. root.au-team.irpo. (

...

)

IN NS hq-srv.au-team.irpo.

IN A 192.168.20.2

hq-rtr IN A 192.168.20.1

br-rtr IN A 192.168.20.65

hq-srv IN A 192.168.20.2

hq-cli IN A 192.168.20.98

br-srv IN A 192.168.20.66

moodle IN CNAME hq-rtr.

wiki IN CNAME hq-rtr.

&& настройка DNS

cp au-team 20.in-addr.arpa

vim 20.in-addr.arpa => @ IN SOA 20.168.192.in-addr.arpa. root.20.168.192.in-addr.arpa. (

...

)

IN NS 20.168.192.in-addr.arpa.

IN A 192.168.20.2

1 IN PTR hq-rtr.au-team.irpo.

2 IN PTR hq-srv.au-team.irpo.

98 IN PTR hq-cli.au-team.irpo.

&& настройка DNS

cd /var/lib/bind/etc/

rndc-confgen > /var/lib/bind/etc/rndc.key

sed -i '6,$d' rndc.key

chgrp -R named zone/

named-checkconf

named-checkconf -z =>

zone au-team.irpo/IN: loaded serial 2024092400

zone 20.168.192.in-addr.arpa/IN: loaded serial 2024092400

systemctl enable --now bind

# **ДЕЛАЕМ НА ВСЕХ МАШИНАХ**:

vim /etc/net/ifaces/ens18/resolv.conf => nameserver 192.168.20.2

domain au-team.irpo

systemctl restart network

&& делаем пинг по имени на всех машинах

###### 11 настройка времени

# Настройка клиентов синхронизации времени (HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.)

apt-get install -y chrony

vim /etc/chrony.conf => server 192.168.20.1 iburst ; + комментировать pool pool.ntp.org iburst

systemctl restart chronyd

# проверка:

&& chronyc tracking && проверка настройки времени

; vim /etc/net/ifaces/ens18/resolv.conf => nnameserver 192.168.20.2 -?

; domain au-team.irpo (исправить после настройки DNS) ######

# BRSRV: ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

root - toor

hostnamectl hostname BR-SRV.au-teame.irpo ; exec bash

##### 3 - users

&& cat /etc/passwd BR-SRV созд. Пользователь и задан hostname

ip -br a

vim /etc/net/ifaces/ens18/options ; меняем dhcp на static

echo '192.168.20.66/28' >> /etc/net/ifaces/ens18/ipv4address

echo 'default via 192.168.20.65' >> /etc/net/ifaces/ens18/ipv4route

echo 'nameserver 8.8.8.8' >> /etc/net/ifaces/ens18/resolv.conf

vim /etc/net/sysctl.conf =>

...

net.ipv4.ip\_forward = 0 => net.ipv4.ip\_forward = 1

...

systemctl restart network

ping 192.168.20.65

&& ping 8.8.8.8 && сквозная связанность на BR-SRV

##### 5. Настройка безопасного удаленного доступа на серверах HQ-SRV и BR-SRV (ssh):

apt-get install openssh-server

cd /etc/openssh

cp ssh\_config ssh\_config.back

vim sshd\_config => port 2024

MaxAuthTries 2

banner /etc/openssh/banner

AllowUsers sshuser

vim /etc/openssh/banner =>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \* Authorized access only \* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

systemctl restart sshd

&& ssh sshuser@192.168.20.2 -p 2024 && проверка ssh

###### 11 настройка времени

# Настройка клиентов синхронизации времени (HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.)

apt-get install -y chrony

vim /etc/chrony.conf => server 192.168.20.1 iburst ; + комментировать pool pool.ntp.org iburst

systemctl restart chronyd

# проверка:

&& chronyc tracking && проверка настройки времени

; vim /etc/net/ifaces/ens18/ipv4address => 192.168.20.66/28

; vim /etc/net/ifaces/ens18/ipv4route => default via 192.168.20.65 // прописываем шлюз

; vim /etc/net/ifaces/ens18/resolv.conf => nameserver 192.168.20.2 -?

; domain au-team.irpo (если DNS настроился)

# HQCLI: ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

user passwd: 'resu'

su -- => password 'toor'

hostnamectl hostname HQ-CLI.au-team.irpo ; exec bash

ip -br a

# ЕСЛИ ЕСТЬ проверяем пинги и переходим к yandex

# ЕСЛИ НЕТ :

vim /etc/net/ifaces/ens18/options => меняем dhcp на static

echo '192.168.20.98/28' >> /etc/net/ifaces/ens18/ipv4address

echo 'default via 192.168.20.97' >> /etc/net/ifaces/ens18/ipv4route

echo 'nameserver 8.8.8.8' >> /etc/net/ifaces/ens18/resolv.conf

# комментируем host в vim /etc/dhcp/dhcpd.conf на HQ-RTR проверяем инет и ставим Yandex

systemctl restart network

ip -br a

# ping 192.168.200.1

ping 192.168.20.97

&& ПРОВЕРКА НАСТРОЙКИ DHCP

cat /etc/net/ifaces/ens18/options # стоит dhcp

# под root:

rm -f /etc/net/ifaces/ens18/ipv4address

systemctl restart network

&& ping 192.168.20.97

###### 9

ip -br a #+ можно посмотреть option и ipv4address там д.б. dhcp и ipv4address можно удалить и dhcp все равно прилетит

###### установка yandex (2.9)

apt-get update

apt-get install yandex-browser-stable

&& Установка Yandex

###### 11 настройка времени

;Настройка клиентов синхронизации времени (HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.)

apt-get install -y chrony

vim /etc/chrony.conf => server 192.168.20.1 iburst ; + комментировать pool pool.ntp.org iburst

systemctl restart chronyd

;проверка:

&& chronyc tracking && проверка настройки времени

; vim /etc/net/ifaces/ens18/resolv.conf => nameserver 192.168.20.2 -?

; domain au-team.irpo (исправить на 8.8.8.8 при не скачивании пакeтов) ######

# ЮЗЕРЫ

##### 3

Создайте пользователя net\_admin на РОУТЕРАХ **HQ-RTR И BR-RTR**/////////////////////////////////////////////////////////////////////////////////////////

useradd -m -u 1010 net\_admin

passwd net\_admin => P@ssw0rd

vim /etc/sudoers => WHEEL\_USERS ALL = (AL:AL) ALL #раскомментируем

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

Root ALL = (AL:AL) ALL

net\_admin ALL = (AL:AL) ALL

# раскомментируем

vim /etc/group => # Вписать ТОЛЬКО нового пользователя (net\_admin) в группу wheel (она уже СУЩЕСТВУЕТ)

&& добавление net\_admin прав

# вариант

; useradd net\_admin -m -s/bin/bash -GWheel

; passwd net\_admin => P@ssw0rd

; grep net\_admin /etc/passwd

; echo 'WHEEL\_USERS ALL = (ALL:ALL) NOPASSWORD: ALL' >> /etc/sudoers

&& grep net\_admin /etc/group

; su net\_admin

; ● Создайте пользователя sshuser на СЕРВЕРАХ х **HQ-SRV и BR-SRV**/////////////////////////////////////////////////////////////////////////////////////////

useradd -m -u 1010 sshuser

passwd sshuser => P@ssw0rd

vim /etc/sudoers => WHEEL\_USERS ALL = (AL:AL) ALL ;раскомментируем

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

Root ALL = (AL:AL) ALL

sshuser ALL = (AL:AL) ALL

vim /etc/group => ;Вписать ТОЛЬКО нового пользователя (sshuser) в группу wheel (она уже СУЩЕСТВУЕТ)

&& добавление sshuser прав

&& grep sshuser /etc/group

; su sshuser

;вариант

; groupadd sshuser -g1010

; useradd sshuser -u1010 -g1010 -m -s/bin/bash

; passwd sshuser => P@ssw0rd

; grep sshuser /etc/passwd

; usermode -aG wheel sshuser

; echo 'WHEEL\_USERS ALL = (ALL:ALL) NOPASSWORD: ALL' >> /etc/sudoers

cat /etc/passwd => проверяем

P@ssw0rd

**МОДУЛЬ 2**

######4 ANSIBLE ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

BR-SRV

apt-get install -y ansible

vim /etc/ansible/hosts =>

[all]

hq-srv ansible\_host=192.168.20.2 ansible\_connection=local

hq-cli ansible\_host=192.168.20.98 ansible\_connection=local

hq-rtr ansible\_host=192.168.20.1 ansible\_connection=local

br-rtr ansible\_host=192.168.20.65 ansible\_connection=local

&& ansible all -m ping && настройка ansible

#### 6 на маршрутизаторах сконфигурируйте статическую трансляцию портов. Внимательно читаем задание на какой машине какой порт куда бросать;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

HQ-RTR

# на HQ-SRV

iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to-destination 192.168.20.2:2024

iptables-save >> /etc/sysconfig/iptables systemctl enable iptables --now

&& iptables-save && проброс портов

; vim /etc/sysconfig/iptables

BR-RTR

# на BR-SRV

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.20.66:8080

iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to-destination 192.168.20.66:2024

iptables-save >> /etc/sysconfig/systemctl

enable iptables --now

# проверка:

&& iptables-save && проброс портов

ssh sshuser@192.168.20.1

####2 Сконфигурируйте файловое хранилище:;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

# на HQ-SRV

# делаем три диска по одному гигу

&& lsblk && проврерка дисков

apt-get install -y mdadm

&& mdadm --create --verbose /dev/md0 --level=5 --raid-devices=3 /dev/sdc /dev/sdd /dev/sdb

mdadm --detail --scan | sudo tee a /etc/mdadm.conf

mkfs.ext4 /dev/md0

mkdir -p /raid5

blkid /dev/md0 >> /etc/fstab

vim /etc/fstab =>

&& /dev/md0: UUID="2adc065f-48d6-4fc1-b74d-6de80026d63c" /raid5 ext4 defaults 0 0

# nolock вместо defaults если не будет монтироваться ?

# проверяем, что пространство монтируется:

&& mount -a && проверка монтирования дисков

apt-get install -y nfs-server

mkdir /raid5/nfs

vim /etc/exports => &&

/srv/public -ro,insecure,no\_subtree\_check,fsid=1 \*

#/srv/share -rw,insecure,fsid=0,sec=krb5 \*

/raid5/nfs 192.168.20.98(rw,sync,no\_subtree\_check) ; адрес HQ-CLI

export fs -a

systemctl restart nfs-server.service

; на HQ-CLI:

mkdir -p /mnt/nfs

vim /etc/fstab => &&

192.168.20.2:/raid5/nfs /mnt/nfs nfs defaults 0 0

# адрес HQ-SRV

apt-get install -y nfs-utils nfs-common

systemctl start rpc-statd

systemctl start rpcbind

&& mount -a && проверка монтирования дисков

#######3 - time в первом модуле

###### 1. Настройте доменный контроллер Samba на машине BR-SRV;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

apt-get update

apt-get install -y task-samba-dc

rm -f /etc/samba/smb.conf

rm -rf /var/lib/samba/

rm -rf /var/cache/samba/

mkdir -p /var/lib/samba

mkdir -p /var/lib/samba/sysvol

;(пароль для администратора используем – P@ssw0rd)

samba-tool domain provision

systemctl enable --now samba.service

cp /var/lib/samba/private/krb5.conf /etc/krb5.conf ;overright - y

cd /opt

visudo krb5.conf => %hq ALL=(ALL) NOPASSWD: /bin/cat, /bin/grep, /usr/bin/id

vim users.csv => user1.hq, P@ssw0rd

user2.hq,P@ssw0rd

user3.hq,P@ssw0rd

user4.hq,P@ssw0rd

user5.hq,P@ssw0rd

mkdir smbscript

cd smbscript/

vim import.sh => #! bin/bash

while IFS=' ,' read -r username password; do

sudo samba-tool user create "$username" "$password"

sudo samba-tool group addmembers hq "$username"

done < /opt/users.csv

chmod +x import.sh

samba-tool group create hq

./import.sh

;Переходим на ВМ HQ-CLI;;;;;;;;;;;;;;;;;;;;;;

cat /etc/resolv.conf => search au-team.irpo

nameserver 192.168.20.2 ;br-srv

;Открываем центр управления

;Выбираем центр управления системой или через поиск ищем acc:

;пароль toor

;В разделе Users выбираем аутентификацию:

Active directory domain : au-team.irpo

workgroup: au-team

comp name: HQ-CLI

;Листаем вниз и нажимает «Apply» - Administrator пароль P@ssw0rd

;Если все правильно сработало, то должно появиться приветственное окно:

;Делаем reboot, после заходим в терминал -

;Проверяем, что работает домен на CLI-HQ:

wbinfo --ping-dc

;Возвращаемся на ВМ BR-SRV (пароль P@ssw0rd) dir smbscript;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

samba-tool dns add br-srv.au-team.irpo au-team.irpo hq-rtr A 192.168.20.1 Administrator

samba-tool dns add br-srv.au-team.irpo au-team.irpo wiki CNAME hq-rtr.au-team.irpo -U Administrator

samba-tool dns add br-srv.au-team.irpo au-team.irpo modle CNAME hq-rtr.au-team.irpo -U Administrator

####5. Развертывание приложений в Docker на сервере BR-SRV;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; на BR-SRV

iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.20.66:8080

iptables -A FORWARD -p tcp -d 192.168.20.66 --dport 8080 -j ACCEPT

iptables-save >> /etc/sys

iptables-save >> /etc/sysconfig/iptables

systemctl enable —nou iptables.service

apt-get install -y docker-io docker-compose

touch wiki.yml

vim wiki.yml =>

version: '3'

services:

wiki: image: mediawiki container \_name: wiki restart: always

ports: - 8080:80

links: - mariadb

volumes:

- images:/var/www/html/inages

#- ./LocalSettings.php:/var/wuw/html/LocalSettings.php

mariadb:

image: mariadb

container\_name: mariadb hostname: mariadb restart: always

environment:

MYSQL DATABASE: mediawiki

MYSQL USER: wiki

MYSQL\_PASSWORD: WikiP@ssuBrd MYSQL\_RANDOM\_ROOT\_PASSWORD: 1

volumes:

- db:/var/lib/mysql

volumes:

images:

db:

"wiki.yml" 30L, 571B

docker-compose -f wiki.yml up -d

; графическая установка

/home/user/LocalSettings.php root@192.168.0.10:~/

vim wiki.yml =>

version: '3'

services:

wiki: image: mediawiki

container\_name: wiki restart: always

ports: - 8080:80

links: - mariadb

volumes:

- images:/var/www/html/images

/LocalSettings.php:/var/wuw/html/LocalSettings.php

mariadb:

image: mariadb

container\_name: mariadb hostname: mariadb restart: always

environment:

MYSOL DATABASE: mediawiki

MYSOL USER: wiki

MYSOL PASSWORD: WikiPesswürd

MYSQL\_RANDON\_ROOT\_PASSHORD: 1

volumes:

- db:/var/lib/mysql

volumes:

images:

db :

"wiki.yml" 3AL, 569B

#### 8 установка nginx

; на HQ\_RTR

apt-get install -y nginx

cd /etc/nginx/sites-available.d/

vim proxy.conf =>

listen 80;

server\_name moodle.au-team.irpo

proxy\_pass http://192.168.20.2;

listen 80;

server\_name wiki.au-team.irpo

proxy\_pass http://192.168.20.66

ln -s /etc/nginx/sites-available.d/proxy.conf /etc/nginx/sites-led.d/

nginx -t

systemctl restart nginx.service

systemctl enable --now nginx.service

Задание 2

Задание 3

Задание 4

Задание 5

Задание 6

Задание 7

Задание 8

Задание 9

Задание 10

Задание 11

**Модуль 2**

Задание 1

Задание 2

Задание 3

Задание 4

Задание 5

Задание 6

Задание 7

Задание 8

Задание 9