1. Создала VDS "Witty Macaw" в аккаунте otparch2 в своем проекте a.tereschenko

---

2. Пользователи и доступ

1) Создаю нового пользователя:

useradd user

2) Задаю пароль для пользователя 2Kptest4w

passwd user

3) Добавляю возможность переключение на суперпользователя:

usermod -aG wheel user

Проверяю, что работает:

[user@spb-3-vm-96r5 ~]$ sudo -i

[sudo] password for user:

[root@spb-3-vm-96r5 ~]#

4) Запрещаю доступ по SSH от root:

В файле /etc/ssh/sshd_config запрещаю подключение от root PermitRootLogin no

Побуждаю сервис перечитать конфиг:

systemctl reload sshd

Проверяю:

$ ssh root@176.124.209.119

root@176.124.209.119's password:

Permission denied, please try again.

---

3. Работа с сетью:

1) Добавила IP адрес 87.249.44.127 в ПУ

2) Добавила на интерфейс статический IP:

sudo nmcli con mod ens3 +ipv4.addresses 87.249.44.127/24

3) Применила настройки:

sudo nmcli con up ens3

ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

link/ether 5a:bc:cb:15:9b:56 brd ff:ff:ff:ff:ff:ff

altname enp0s3

altname enx5abccb159b56

inet **87.249.44.127/24** brd 87.249.44.255 scope global noprefixroute ens3

valid_lft forever preferred_lft forever

inet **176.124.209.119/24** brd 176.124.209.255 scope global dynamic noprefixroute ens3

valid_lft 86398sec preferred_lft 86398sec

inet6 fe80::58bc:cbff:fe15:9b56/64 scope link noprefixroute

valid_lft forever preferred_lft forever

Вижу, что они записаны в конфиге

/etc/NetworkManager/system-connections/ens3.nmconnection:

[ipv4]

address1=87.249.44.127/24

method=auto

Для проверки перезагрузила вдску, и доп. IP пропал. Перепробовала всевозможные настройки NetworkManager для автоматической загрузки конфига с доп. IP после перезапуска сервиса. Например, nmcli connection modify ens3 connection.autoconnect yes

Пробовала и по этой инструкции https://timeweb.cloud/docs/unix-guides/adding-ip-addresses

Но ничего не сработало. После перезагрузки у меня либо только статический IP, если я указываю в конфиге method=manual, либо только выдаваемый по DHCP, если я указываю method=auto.

В итоге обратилась за помощью. Проблему решил Артем, определив, что сетевое подключение создавалось через cloud-init.

В логах на самом деле это было видно:

Mar 24 22:41:17 spb-3-vm-96r5 NetworkManager[833]: <info> [1774381277.9736] policy: **auto-activating connection 'cloud-init ens3'** (fbc49833-4cdb-548b-a293-c38b39836fdb)

Но я не придала этому значение, а зря...

Решение:

Удаление профиля cloud-init:

nmcli con delete "cloud-init ens3"

nmcli con delete "cloud-init ens8"

Привязка и активация автоподключения профиля соединения ens3 к интерфейсу:

nmcli con modify ens3 connection.interface-name ens3

nmcli con modify ens3 connection.autoconnect yes

Добавление статического IP:

nmcli con modify ens3 ipv4.method auto

nmcli con modify ens3 +ipv4.addresses 87.249.44.127/24

Поднятие интерфейса:

nmcli con up ens3

---

4. Настрой DNS:

Проверила, что нет процессов, слушающих порт 53:

sudo ss -nlp | grep 53

Значит systemd-resolved тут не используется.

В /etc/resolv.conf указано, что DNS сервера задаются NetworkManager:

[root@spb-3-vm-96r5 ~]# cat /etc/resolv.conf

Generated by NetworkManager

nameserver 1.1.1.1

nameserver 1.0.0.1

Добавила DNS сервера в конфиг NetworkManager:

nmcli connection modify ens3 ipv4.dns 8.8.8.8

nmcli connection modify ens3 +ipv4.dns 8.8.4.4

$ cat /etc/resolv.conf

Generated by NetworkManager

nameserver 8.8.8.8

nameserver 8.8.4.4

Убедилась, что запросы действительно идут к DNS серверу с IP 8.8.8.8:

tcpdump -i ens3 -nnv port 53

21:47:00.696949 IP (tos 0x0, ttl 64, id 41104, offset 0, flags [DF], proto UDP (17), length 51)

176.124.209.119.47715 > **8.8.8.8**.53: 19861+ A? ya.ru. (23)

---

5. Firewall (firewalld)

Установила, запустила сервис и добавила в автозагрузку:

yum install firewalld

systemctl enable firewalld --now

---

6. Nginx

Установила, запустила сервис и добавила в автозагрузку:

yum install nginx

systemctl enable nginx --now

Проверила, что TCP SYN запрос на подключение к порту 80 приходит, но, судя по всему, по правилам nft отправляется ICMP-пакет с ошибкой:

tcpdump -i ens3 -nnve host 92.100.37.98 and not port 22

22:52:34.137071 9e:ce:ed:e6:73:40 > 5a:bc:cb:15:9b:56, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 57, id 9356, offset 0, flags [DF], proto TCP (6), length 60)

92.100.37.98.47388 > 176.124.209.119.80: Flags [S], cksum 0x6f2e (correct), seq 1871229806, win 64240, options [mss 1452,sackOK,TS val 2932952825 ecr 0,nop,wscale 7], length 0

22:52:34.137191 5a:bc:cb:15:9b:56 > 9e:ce:ed:e6:73:40, ethertype IPv4 (0x0800), length 102: (tos 0xc0, ttl 64, id 22088, offset 0, flags [none], proto ICMP (1), length 88)

176.124.209.119 > 92.100.37.98: **ICMP host 176.124.209.119 unreachable - admin prohibited filter**, length 68

nft list ruleset

chain filter_INPUT {

reject with icmpx admin-prohibited

}

Добавила разрешающие правила для подключения по порту 80:

firewall-cmd --add-port=80/tcp --permanent

firewall-cmd --add-port=80/udp --permanent

firewall-cmd --reload

firewall-cmd --list-ports

80/tcp 80/udp

Проверила, что доступ есть:

kostushka@laptop:~$ **nc -v 176.124.209.119 80**

Connection to 176.124.209.119 80 port [tcp/http] succeeded!

kostushka@laptop:~$ **curl -LI 176.124.209.119:80**

HTTP/1.1 200 OK