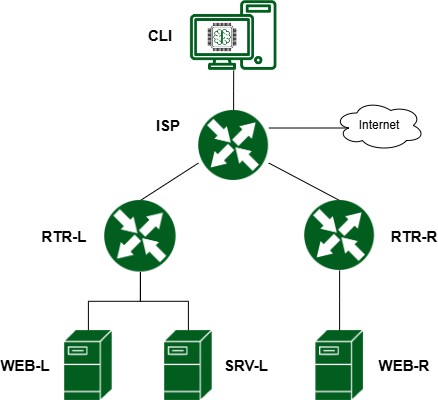
Задание экзамена «Администрирование сетей передачи информации»



1. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.

Адресация должна быть выполнена в соответствии с Таблицей 1.

Таблица 1

|  |  |
| --- | --- |
| Имя ВМ | IP-адрес |
| RTR-L | 100.100.100.10/28 – для подсети в сторону ISP 10.10.10.1/24 – для подсети офиса LEFT |
| RTR-R | 150.150.150.10/28 – для подсети в сторону ISP 20.20.20.1/24 – для подсети офиса RIGHT |
| SRV-L | 10.10.10.100/24 |
| WEB-L | 10.10.10.110/24 |
| WEB-R | 20.20.20.100/24 |
| ISP | 100.100.100.1/28 – для подсети в сторону RTR-L 150.150.150.1/28 – для подсети в сторону RTR-R 35.35.35.1/28 – для подсети в сторону CLI DHCP -для выхода в общественную сеть |
| CLI | 35.35.35.10/28 |

**RTR-L:**

hostnamectl set-hostname rtr-l.au.team; exec bash

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

vim /etc/net/ifaces/ens18/ipv4address 100.100.100.10/28

cp -r /etc/net/ifaces/ens18/ /etc/net/ifaces/ens19/

vim /etc/net/ifaces/ens19/ipv4address10.10.10.1/24

reboot

**RTR-R:**

hostnamectl set-hostname rtr-r.au.team; exec bash

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

vim /etc/net/ifaces/ens18/ipv4address150.150.150.10/28

cp -r /etc/net/ifaces/ens18/ /etc/net/ifaces/ens19/

vim /etc/net/ifaces/ens19/ipv4address20.20.20.1/24

reboot

**SRV-L:**

hostnamectl set-hostname srv-l.au.team; exec bash

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

vim /etc/net/ifaces/ens18/ipv4address10.10.10.100/24

reboot

**WEB-L:**

hostnamectl set-hostname web-l.au.team; exec bash

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

vim /etc/net/ifaces/ens18/ipv4address10.10.10.110/24

reboot

**WEB-R:**

hostnamectl set-hostname web-r.au.team; exec bash

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

vim /etc/net/ifaces/ens18/ipv4address20.20.20.100/24

reboot

**ISP:**

hostnamectl set-hostname isp.au.team; exec bash

cp -r /etc/net/ifaces/ens18 /etc/net/ifaces/ens19/

vim /etc/net/ifaces/ens19/options меняем на static

cp -r /etc/net/ifaces/ens19 /etc/net/ifaces/ens20/

cp -r /etc/net/ifaces/ens19 /etc/net/ifaces/ens21/

vim /etc/net/ifaces/ens19/ipv4address 100.100.100.1/28

vim /etc/net/ifaces/ens20/ipv4address 150.150.150.1/28

vim /etc/net/ifaces/ens21/ipv4address 35.35.35.1/28

reboot

**CLI:**

hostnamectl set-hostname cli.au.team; exec bash

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

vim /etc/net/ifaces/ens18/ipv4address 35.35.35.10/28

reboot

1. Настройка динамической трансляции адресов на всех роутерах.
   * Настройте динамическую трансляцию адресов для обоих офисов сторону ISP и с ISP в сторону общественной сети.
   * Все устройства в офисах должны иметь доступ к сети Интернет

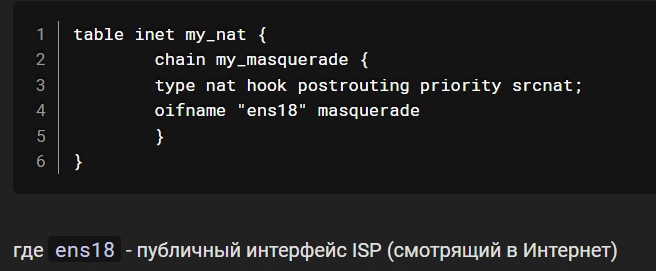
**ISP:**

apt-get update

apt-get install nftables -y

vim /etc/nftables/nftables.nft

В конфиге прописать ниже после всего:

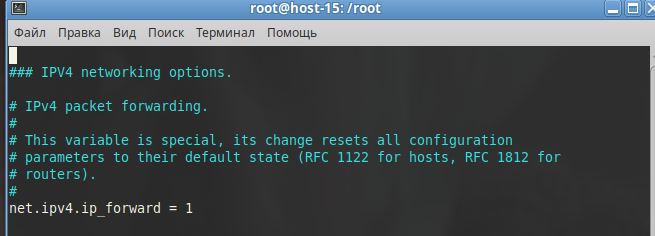


systemctl start nftables

[если не запускается проверить на ошибки командой nft -f /etc/nftables/nftables.conf]

systemctl enable nftables

vim /etc/net/sysctl.conf



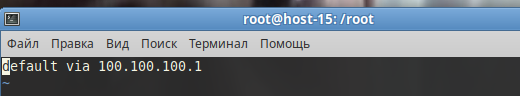


reboot

**RTR-L:**

vim /etc/net/ifaces/ens18/ipv4route

Шлюз по умолчанию в сторону ISP:



reboot

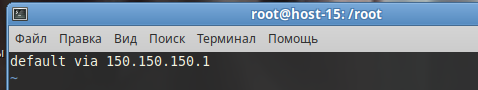
Далее скачать и настроить nftables точь-в-точь как на ISP, не забыть net.ipv4.ip\_forward = 1

reboot

**RTR-R:**

vim /etc/net/ifaces/ens18/ipv4route

Шлюз по умолчанию в сторону ISP:



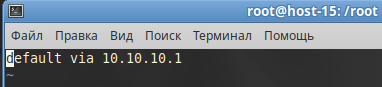
reboot

Далее скачать и настроить nftables точь-в-точь как на ISP, не забыть net.ipv4.ip\_forward = 1

reboot

**SRV-L:**

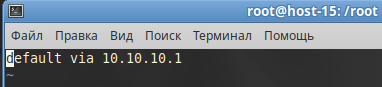
vim /etc/net/ifaces/ens18/ipv4route



Reboot

**WEB-L:**

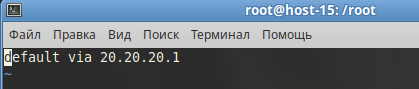
vim /etc/net/ifaces/ens18/ipv4route



reboot

**WEB-R:**

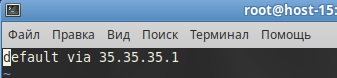
vim /etc/net/ifaces/ens18/ipv4route



reboot

**CLI:**

vim /etc/net/ifaces/ens18/ipv4route



reboot

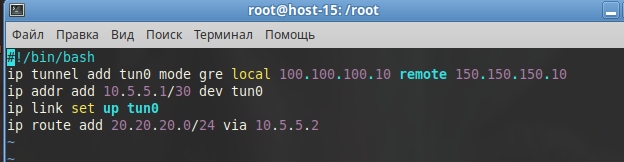
1. Между офисами должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.
   * Трафик, проходящий по данному туннелю, должен быть защищен:
   * Платформа ISP не должна иметь возможности просматривать содержимое пакетов, идущих из одной внутренней сети в другую.
   * Туннель должен позволять защищенное взаимодействие между офисами управления трафиком по их внутренним адресам
   * Взаимодействие по внешним адресам должно происходит без применения туннеля и шифрования.
   * Трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.

**Создание gre-тоннеля:**

**RTR-L:**

vim /etc/gre.up

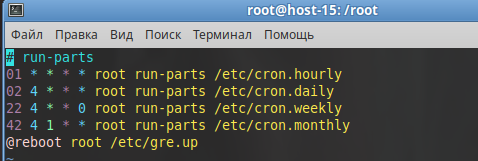
Пишем:

Сохраняем файл

chmod +x /etc/gre.up

sh /etc/gre.up

vim /etc/crontab

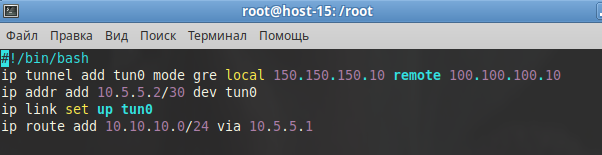




**RTR-R:**

vim /etc/gre.up

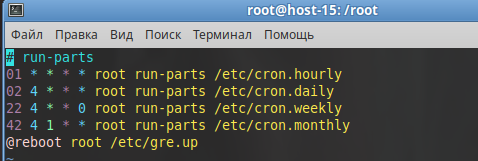
Пишем:

Сохраняем файл

chmod +x /etc/gre.up

sh /etc/gre.up

vim /etc/crontab



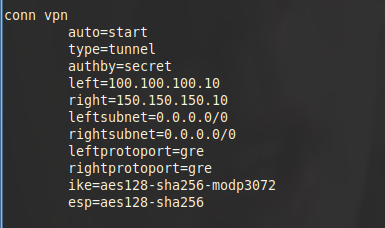


**Создание ip-sec соединения:**

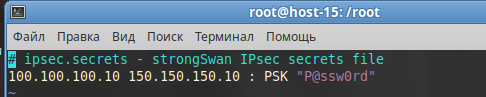
**RTR-L:**

apt-get install strongswan

vim /etc/strongswan/ipsec.conf



vim /etc/strongswan/ipsec.secrets



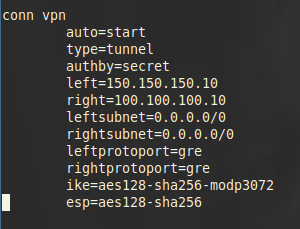
systemctl start strongswan-starter.service

systemctl enable strongswan-starter.service

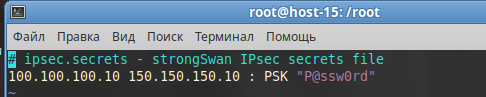
**RTR-R:**

apt-get install strongswan

vim /etc/strongswan/ipsec.conf



vim /etc/strongswan/ipsec.secrets



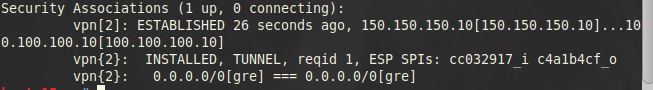
systemctl start strongswan-starter.service

systemctl enable strongswan-starter.service

Команда для проверки:

ipsec status

Должно быть так:



Если не так, то пробуем

ipsec update

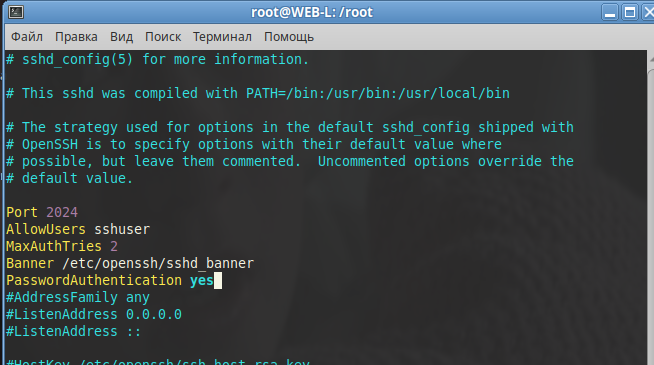
ipsec restart

1. Настройка безопасного удаленного доступа на серверах WEB-L и WEB-R:
   * Для подключения используйте порт 2024
   * Разрешите подключения только пользователю sshuser
   * Ограничьте количество попыток входа до двух
   * Настройте баннер «Authorized access only»

**WEB-L и WEB-R:**

apt-get install openssh-server

vim /etc/openssh/sshd\_config



echo “Authorized access only” > /etc/openssh/sshd\_banner

systemctl enable --now sshd

useradd sshuser

passwd sshuser

1. Настройка DNS для офисов HQ и BR.
   * Основной DNS-сервер реализован на SRV-L. Дочерний сервер DNS на WEB-R.
   * Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
   * В качестве DNS сервера пересылки используйте 94.232.137.104 DNS сервер.
   * Для устройств офиса RIGHT DNS сервер WEB-R, для устройств офиса LEFT DNS сервер SRV-L

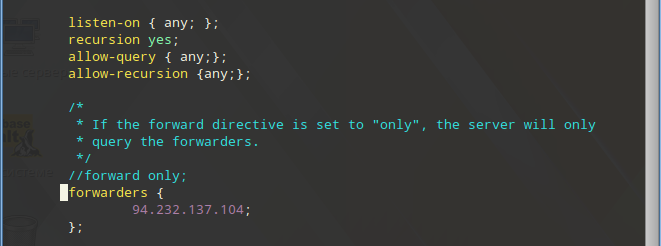
Таблица 2

|  |  |  |
| --- | --- | --- |
| Имя ВМ | Запись | Тип |
| RTR-L | rtr-l.au.team | A,PTR |
| RTR-R | rtr-r.au.team | A,PTR |
| SRV-L | srv-l.au.team | A,PTR |
| WEB-L | web-l.au.team | A,PTR |
| WEB-R | web-r.au.team | A,PTR |
| ISP | isp.au.team | A,PTR |
| CLI | cli.au.team | A,PTR |

**SRV-L:**

**apt-get update && apt-get install bind bind-utils**

**vim /etc/bind/options.conf**



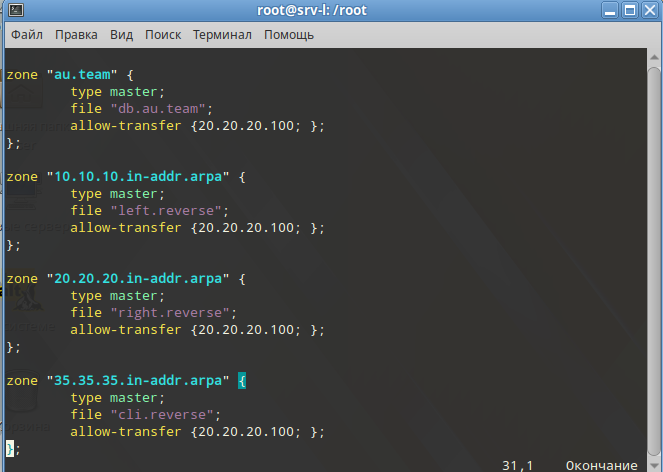
В качестве DNS-сервера для самого себя должен быть 127.0.0.1:

vim /etc/resolv.conf

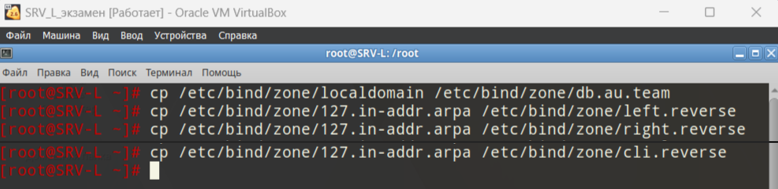


В конфигурационном файле /etc/bind/local.conf описываем необходимые зоны согласно требованию задания:

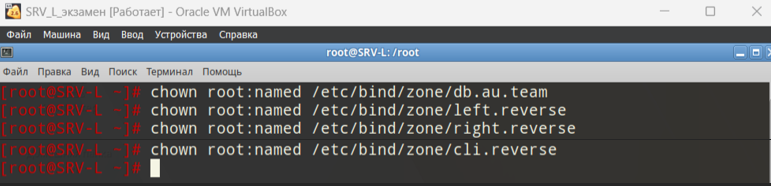
**vim /etc/bind/local.conf**



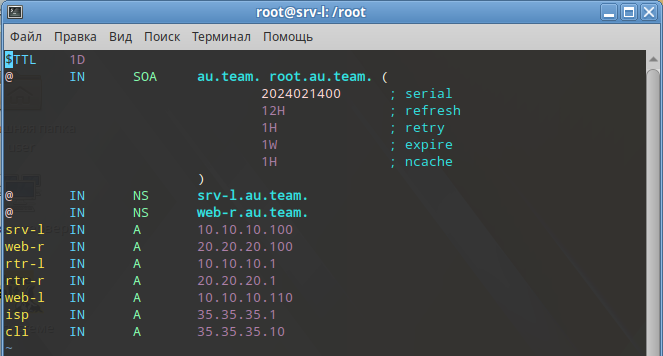
Примеры файлов зон прямого и обратного просмотра расположены по пути /etc/bind/zone. Копируем их:



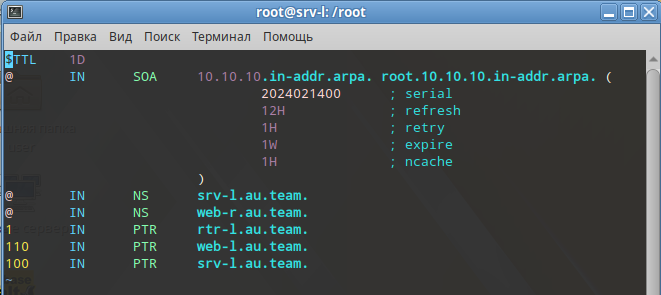
Задаём необходимые права:



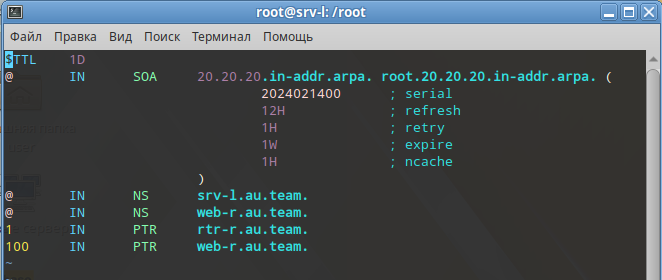
vim /etc/bind/zone/db.au.team



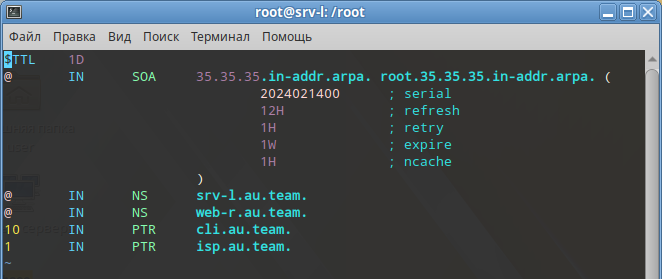
vim /etc/bind/zone/left.reverse



vim /etc/bind/zone/right.reverse



vim /etc/bind/zone/cli.reverse

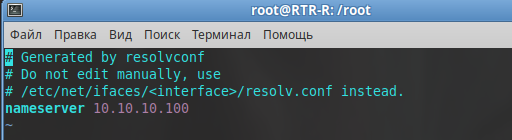


**systemctl restart bind**

**named-checkconf**

**named-checkconf -z**

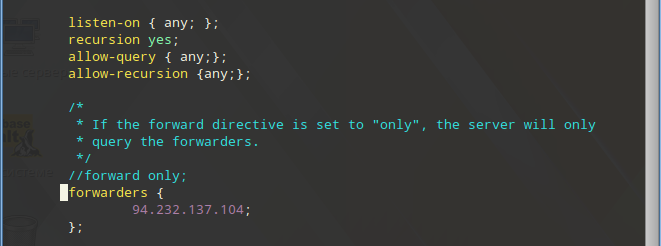
НА ВСЕХ МАШИНАХ КРОМЕ SRV-L и WEB-R: поменять /etc/resolv.conf



**WEB-R:**

**apt-get update && apt-get install bind bind-utils**

**vim /etc/bind/options.conf**

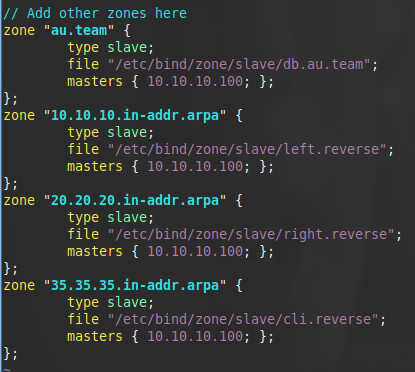


В качестве DNS-сервера для самого себя должен быть 127.0.0.1:

vim /etc/resolv.conf



**vim /etc/bind/local.conf**



chown named:named /var/lib/bind/zone/slave/ **ВАЖНО!!!**

systemctl restart bind

systemctl enable –now bind

systemctl status bind

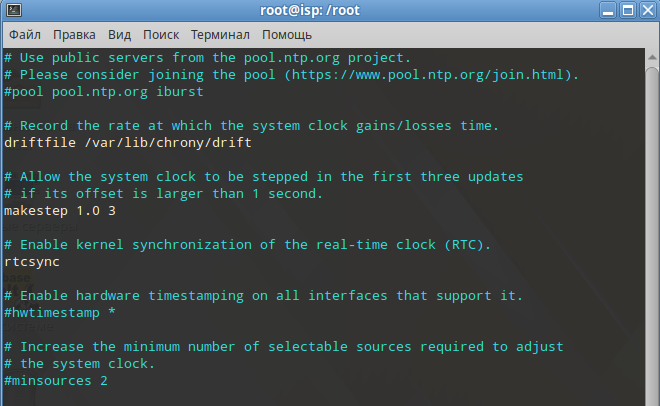
Левая подсеть обращается к SRV-L (10.10.10.100), правая к WEB-R (20.20.20.100) – конфиг resolv.conf

1. Настройте службу сетевого времени на базе сервиса chrony
   * В качестве сервера выступает ISP
   * На ISP настройте сервер chrony, выберите стратум 5
   * В качестве клиентов настройте RTR-L, RTR-R, SRV-L, WEB-L, WEB-R, CLI

Настройка на ISP

Открываем файл /etc/chrony.conf

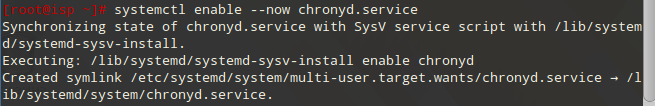
Комментим строчку **pool pool.ntp.org iburst**

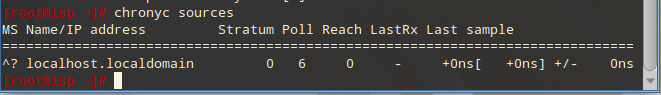


В конце файла пишем



Сохраняем его



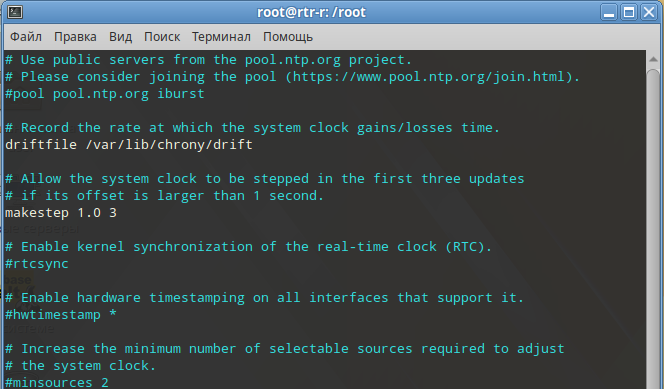


На всех остальных машинах

В файле /etc/chrony.conf комментируем строчки

**pool pool.ntp.org iburst**

**rtcsync (не обязательно, как я понял)**



**На RTR-R**

В конце файла пишем server 150.150.150.1

**На RTR-L**

В конце файла пишем server 100.100.100.1

**На CLI**

В конце файла пишем server 35.35.35.1

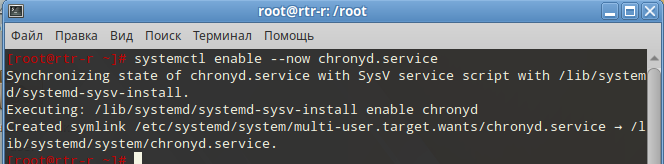
**На SRV-L и WEB-L**

В конце файла пишем server 100.100.100.1

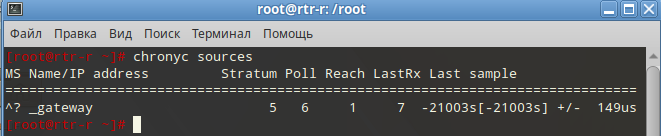
**На WEB-R**

В конце файла пишем server 150.150.150.1

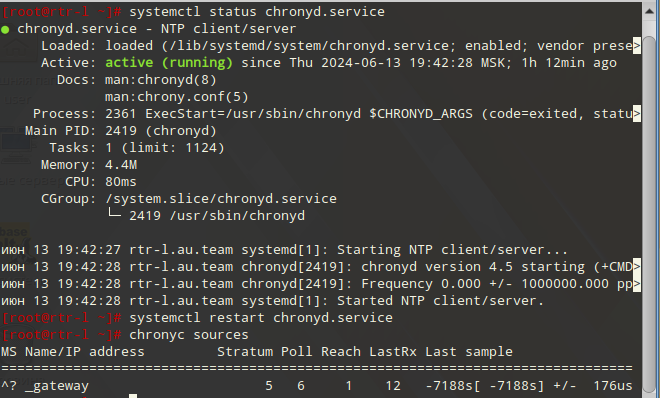
Сохраняем и выходим из файла



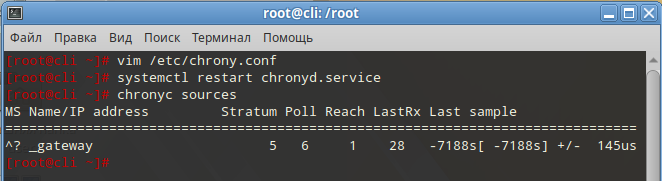
Для RTR-R



Для RTR-L



Для CLI



1. Сконфигурируйте файловое хранилище:
   * При помощи четырёх дополнительных дисков, размером 1Гб каждый, на SRV-L сконфигурируйте дисковый массив уровня 5
   * Имя устройства – md0, конфигурация массива размещается в файле

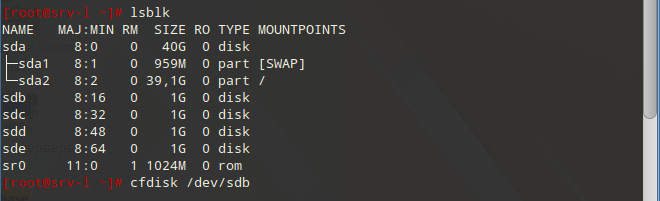
/etc/mdadm.conf

* + Обеспечьте автоматическое монтирование в папку /raid5
  + Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4
  + Настройте сервер сетевой файловой системы(nfs), в качестве папки общего

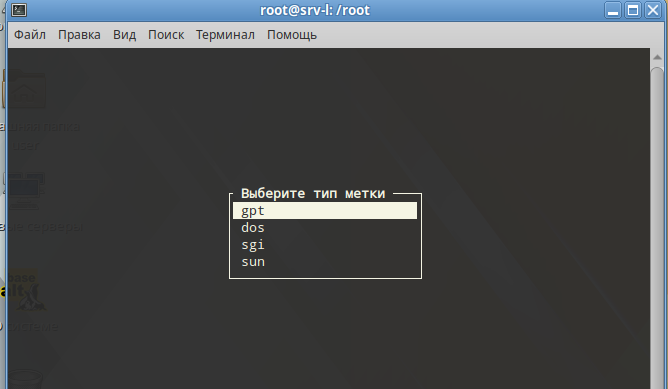
доступа выберите /raid5/nfs, доступ для чтения и записи для всей сети в сторону WEB-L, WEB-R.

* + На WEB-L, WEB-R настройте автомонтирование в папку /mnt/nfs

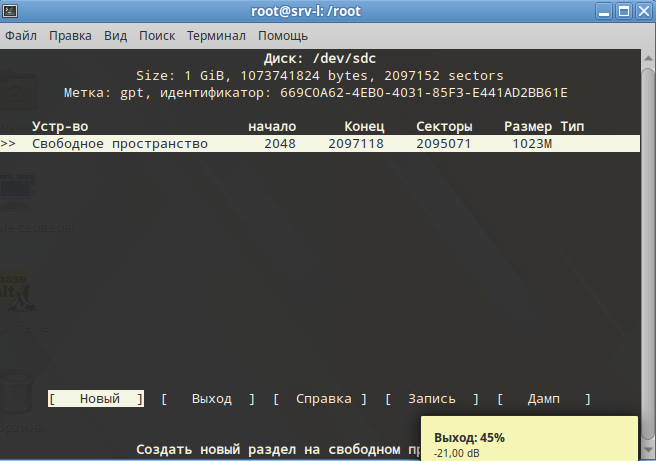
Пишем lsblk, смотрим диски



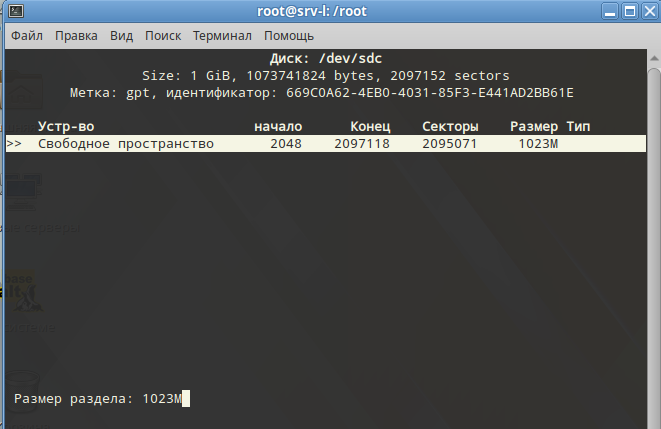
Команда: cfdisk /dev/sdс



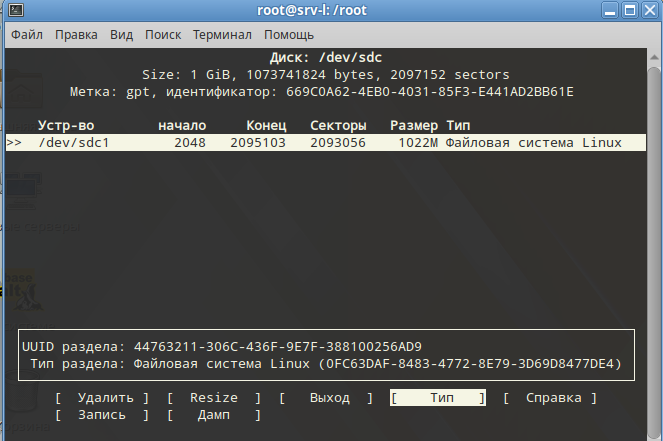
Нажимаем enter



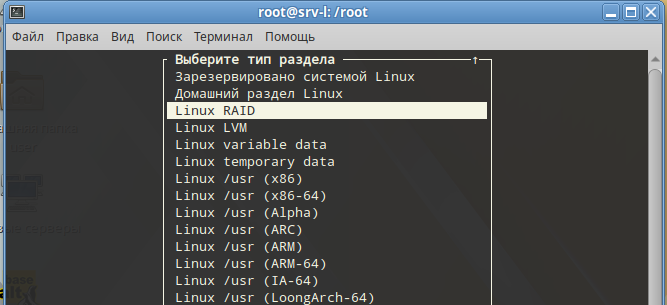
Выбираем Новый



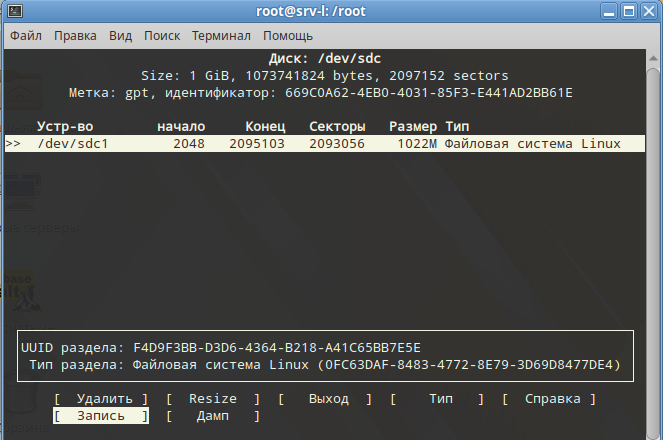
Нажимаем enter



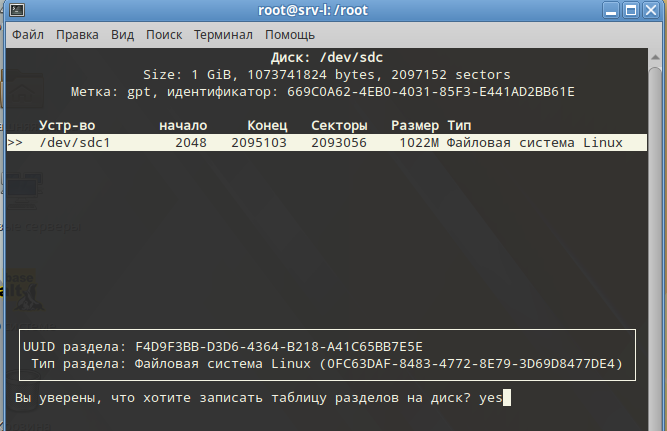
Нажимаем Тип



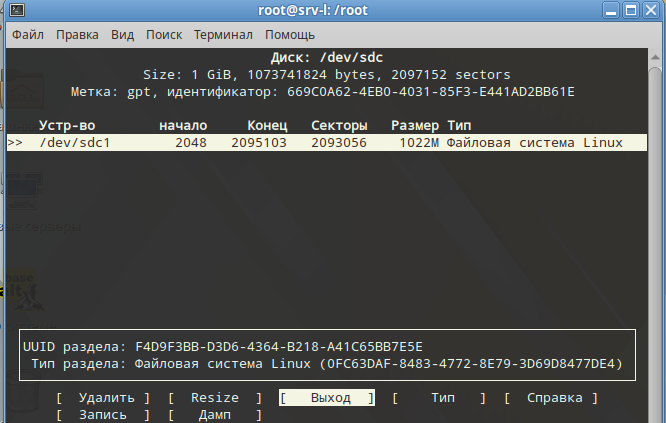
Выбираем Linux Raid, нажимаем enter



Выбираем Запись



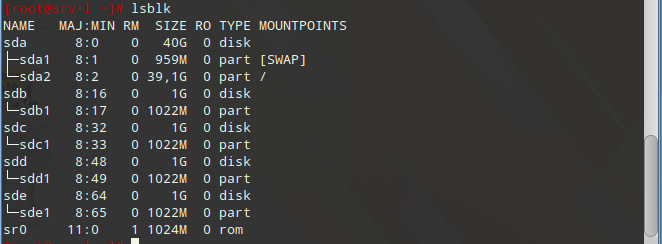
Пишем yes

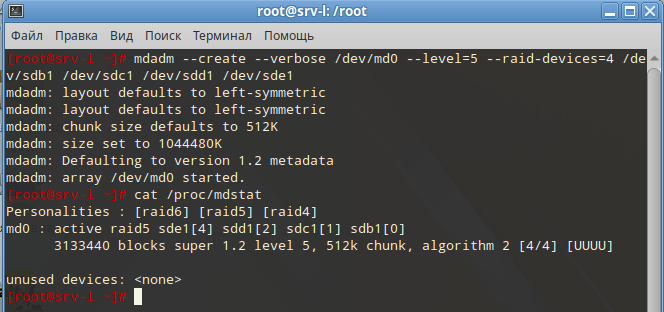


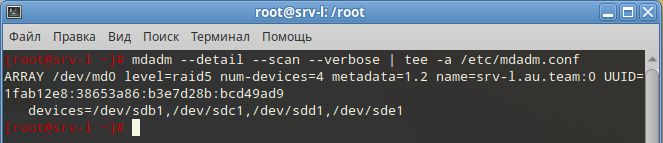
Выбираем Выход и нажимаем enter

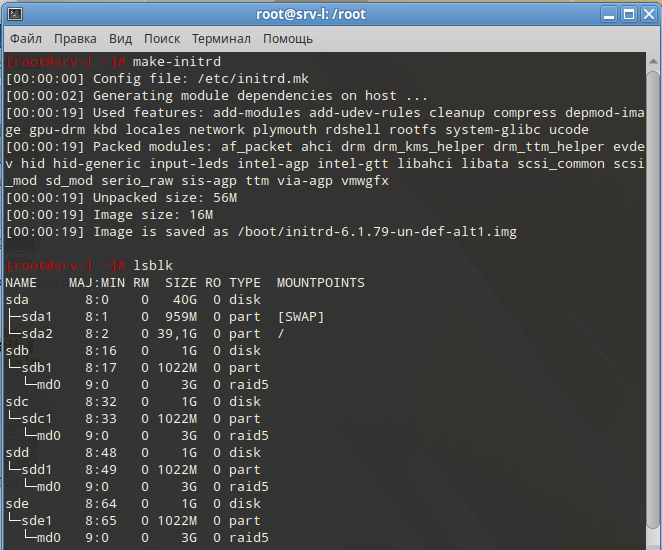
То же самое делаем для /dev/sdb /dev/sdd /dev/sde

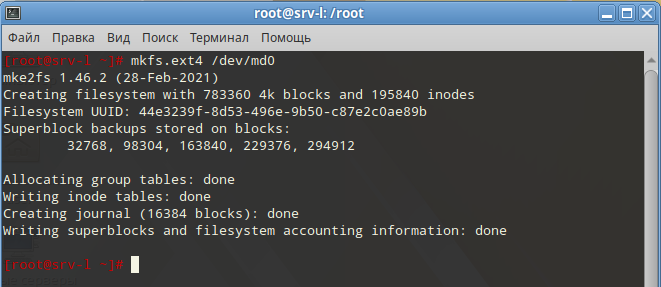
Получилось

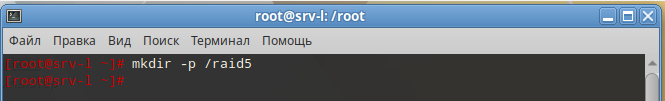




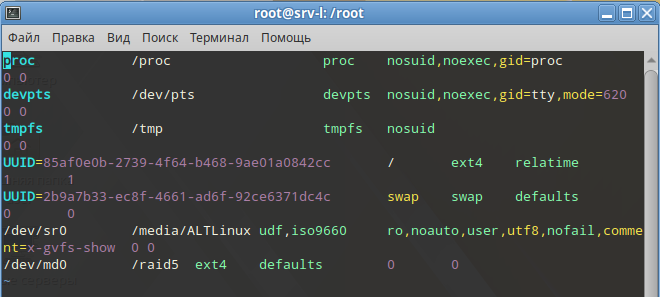




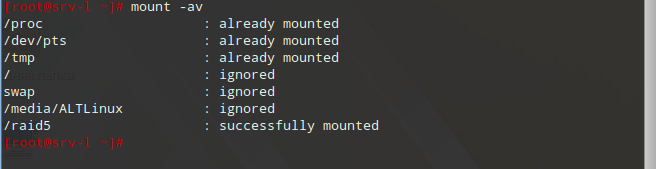




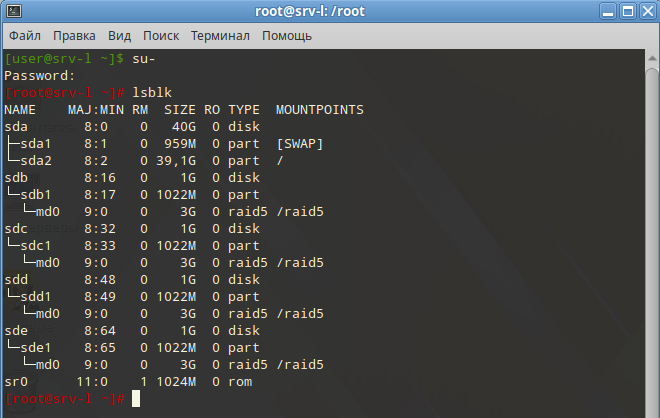
Открываем файл /etc/fstab

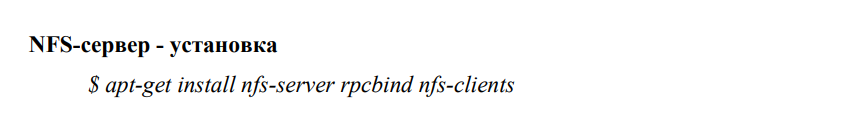


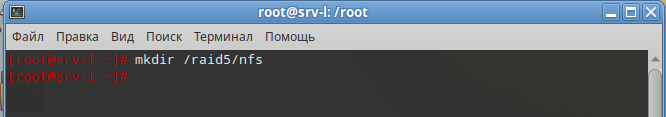
(последняя строчка)



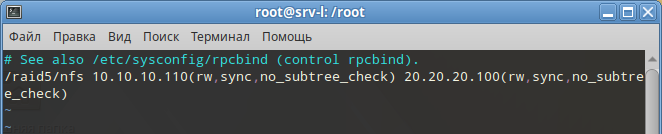
Перезагружаем машину reboot





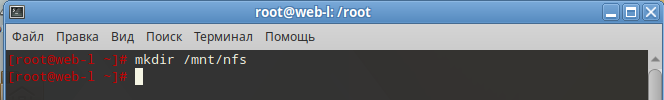


vim /etc/exports

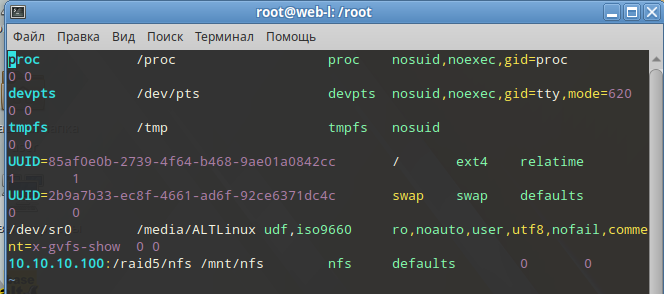


На web-l и web-r прописываем

apt-get install nfs-clients



vim /etc/fstab



(последняя строчка)

В конце прописываем mount -a

1. Запустите сервис MediaWiki используя docker на сервере WEB-L.
   * Установите Docker и Docker Compose.
   * Создайте в домашней директории пользователя файл wiki.yml для приложения MediaWiki:
   * Средствами docker compose должен создаваться стек контейнеров с приложением MediaWiki и базой данных
   * Используйте два сервиса;
   * Основной контейнер MediaWiki должен называться wiki и использовать образ mediawiki;
   * Файл LocalSettings.php с корректными настройками должен находиться в домашней папке пользователя и автоматически монтироваться в образ;
   * Контейнер с базой данных должен называться db и использовать образ mysql;
   * Он должен создавать базу с названием mediawiki, доступную по стандартному порту, для пользователя wiki с паролем DEP@ssw0rd;
   * База должна храниться в отдельном volume с названием dbvolume.
   * MediaWiki должна быть доступна с WEB-R по порту 8080 и имени midiawiki.au.team
2. Удобным способом установите приложение Яндекс Браузере для организаций на CLI

На cli   
apt-get update

apt-get install yandex-browser-stable