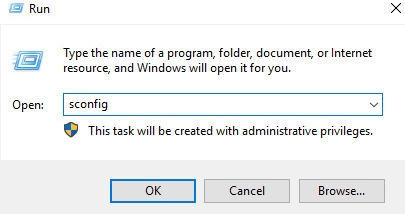
**Методичка по выполнению демонстрационного экзамена СИСА 2023г**

**Настройка ip-адресации**

CLI настраиваем первым и после этого этапа переходим к SRV



После доустановки SRV он включается почти мгновенно. Не теряя времени нажимаем комбинацию клавиш Win+R и вводим sconfig



Мы переходим в синюю панель sconfig, где можем настроить всё, что нужно.

- Нажимаем 4 (Пункт Configure Remote Management), далее 1 (Enable Remote Manegement) – подтверждаем, далее 3 ( Configure Server Response) – подтверждаем

Так мы настраиваем разрешение на ответ эхо-запросов для SRV.

- Нажимаем 4 (Return to main menu), что возвращает нас обратно в главную панель

- Нажимаем 8 (Network Settings), далее 1 (выбираем единственный интерфейс), переходим в панель настройки адаптера.

Нажимаем 1 (Set Network Adapter Address). На вопрос о выборе метода настройки интерфейса выбираем статическую (Пишем S)



Вводим нужный нам ip адрес



Далее нам предлагают ввести маску. Нажимаем enter так как маска по умолчанию 24, которая нам и нужна



Вводим шлюз по умолчанию



- Нажимаем 2 пункт (Set DNS Servers)

Вводим локальный ip, так как SRV является DNS сервером



Далее нам предлагается ввести альтернативный DNS сервер. Просто жмём enter



- Вводим 4 и выходим в главное меню. Последнее что нам нужно это изменить имя компьютера.

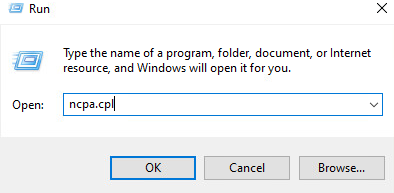
- Нажимаем 2 (Computer Name) и меняем его на SRV



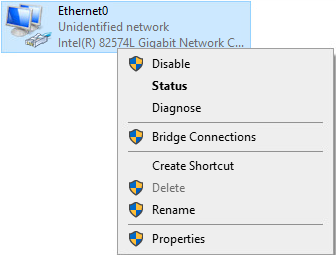
И соглашаемся на перезапуск

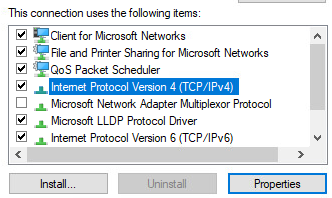
Переходим обратно к CLI и теперь будем настраивать ip ему.

Нажимаем комбинацию клавиш Win+R и вводим ncpa.cpl. Это действие перекинет нас в меню настроек адаптеров

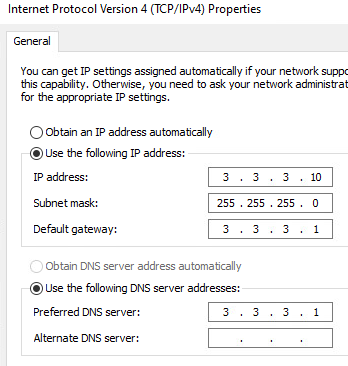


Переходим в настройки нашего адаптера/настройки ipv4





И вводим нужную нам адресацию



**Переходим к машинкам на Debian**

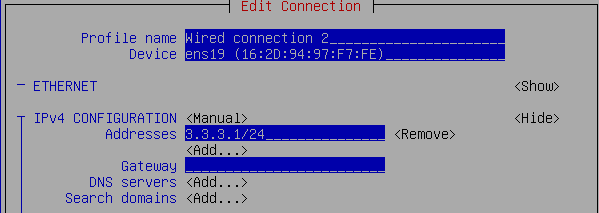
Устанавливаем Network Manager

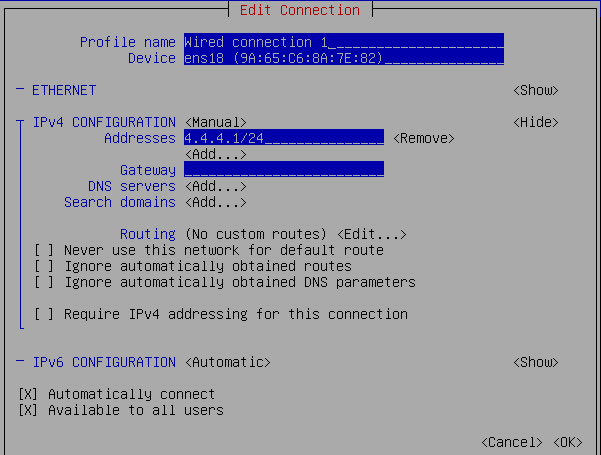
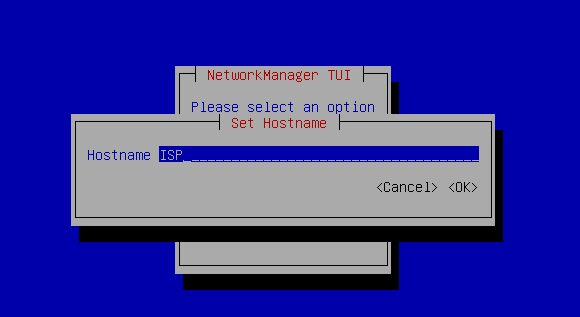


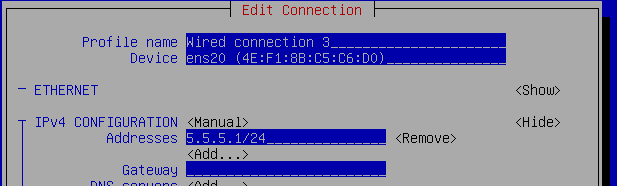
Настроим ip и hostname согласно топологии с помощью nmtui

- Сверяем наши MAC-Адреса интерфейсов с MAC-адресами интерфейсов с панели настроек виртуальных машин

- После сверки переходим к настройке

ISP

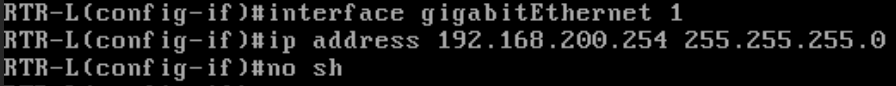
nmtui

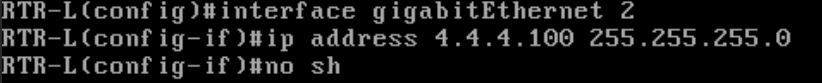
Необходимо произвести эти действия на WEB-L, WEB-R, ISP.

**Переходим к машинам cisco**

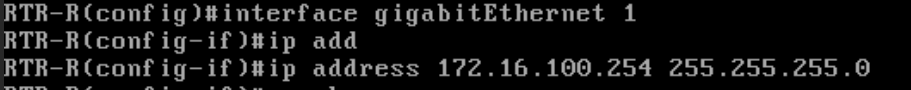
RTR-L

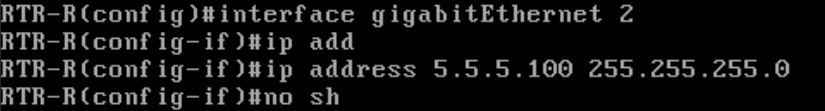
Ставим hostname

Настройка gi1 (Смотрит в сторону зоны LEFT)

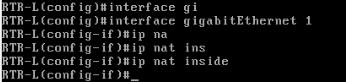
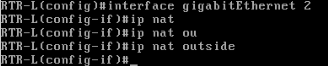
Настройка gi2 (Смотрит в сторону ISP)

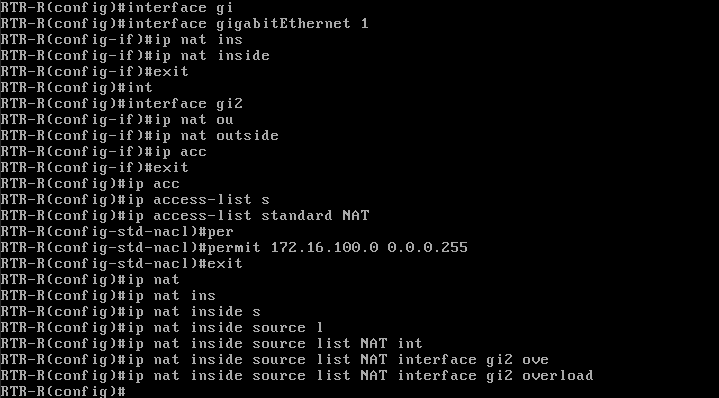
RTR-R

Настройка gi1 (Смотрит в сторону зоны RIGHT)

Настройка gi2 (Смотрит в сторону ISP)

Настроим PAT

RTR-L

RTR-R

**Сетевая связность.**

На ISP нужно настроить пересылку пакетов.

Открываем файл с помощью нано



Ищем данную строку и разкомментируем её





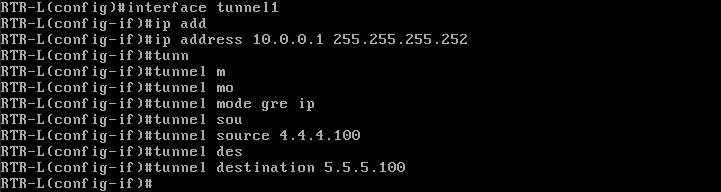
Сохраняем файл и применяем изменения следующей командой



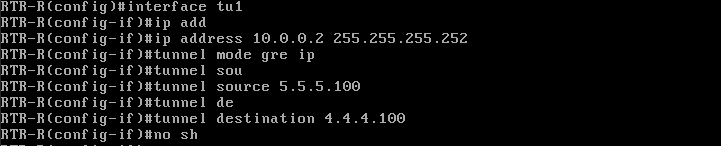
Указываем статический маршрут

**Тунель gre**

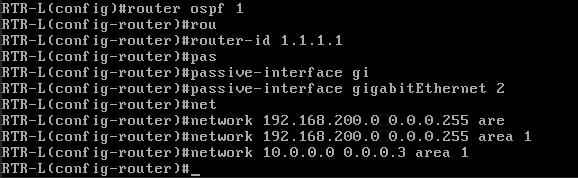
RTR-L

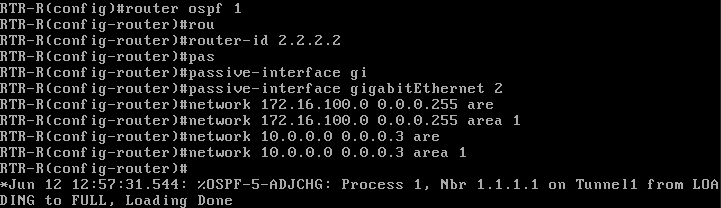


RTR-R



Настройка OSPF

RTR-L

RTR-R

**Настройка SSH**

На устройствах WEB-L, WEB-R требуется настроить ssh.

На каждой машинке повторяем следующие действия:

Открываем файл настроек ssh с помощью нано



Ищем следующую строку



Разкомментриуем и поставим атрибут yes



И сохраняем файл

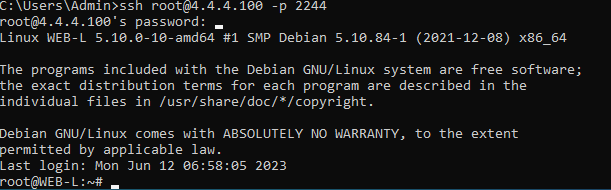
Перезапускаем службы ssh

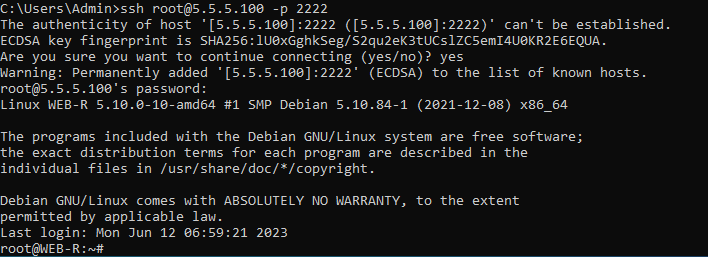


Эти действия провести на каждой машине, указанной выше

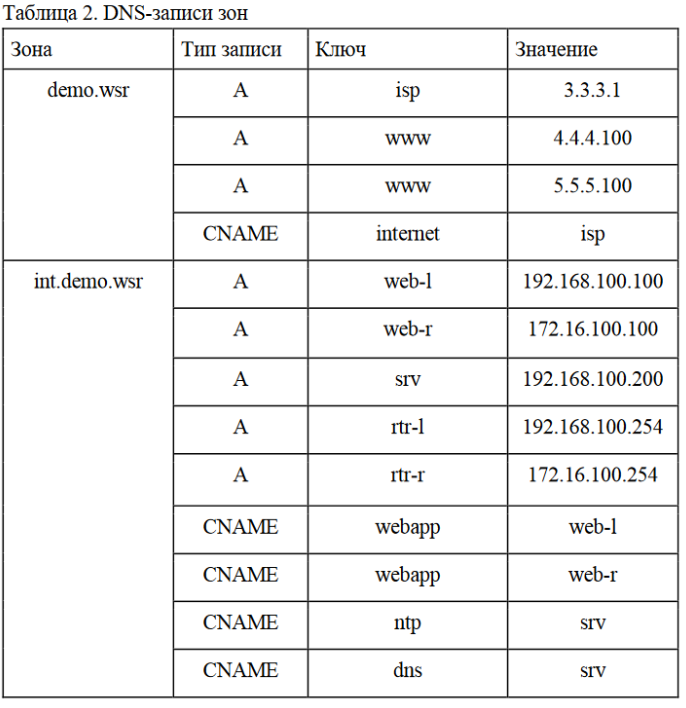
На RTR-L и RTR-R пробросим порты 2244 на WEB-L и 2222 на WEB-R.

Проверяем работу перенаправления ssh с CLI

Подключение к WEB-L. Нужно отправлять запрос на 4.4.4.100, он перенаправляет запрос на WEB-L

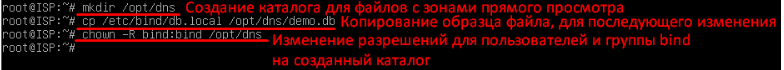
Также и с WEB-R

Настройка DNS



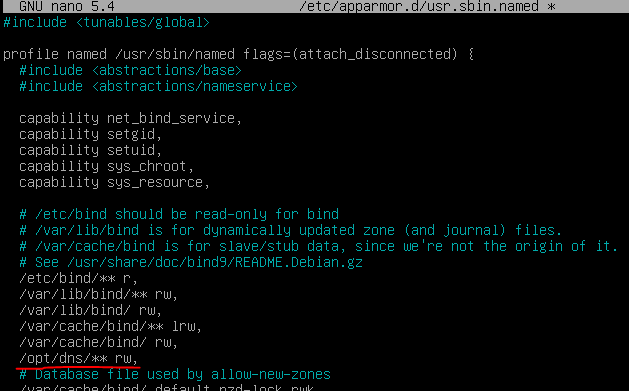
На ISP установим bind9





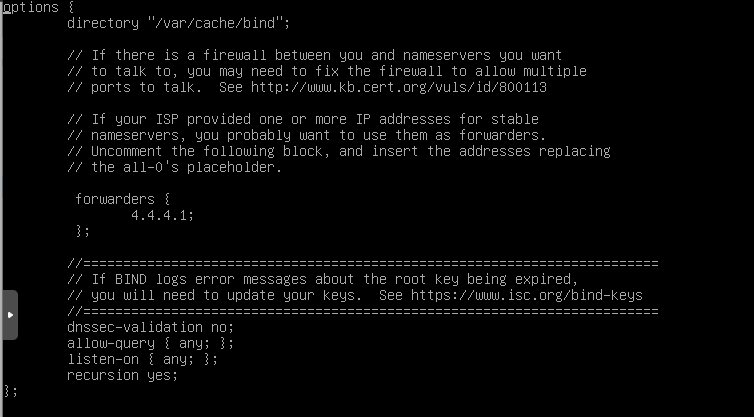
Разрешим беспрепятственную работу файлам из каталога /opt/dns





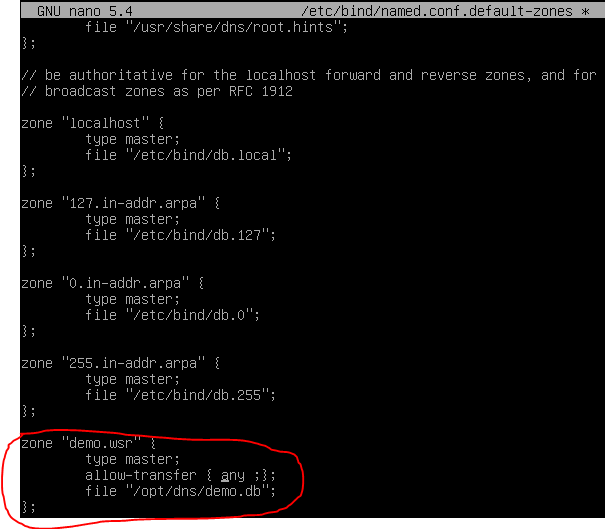
Настроим конфигурацию dns



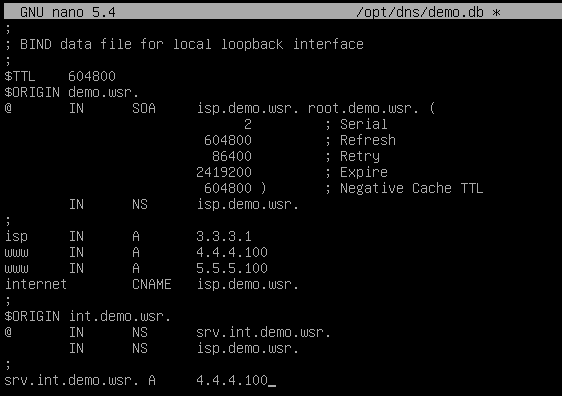


Настроим зоны dns







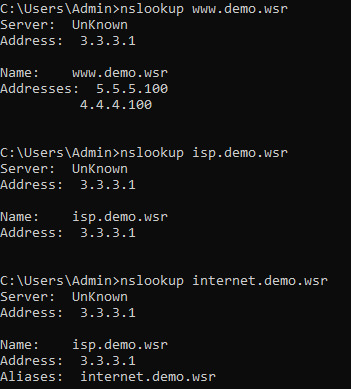
Отредактируйте файл, чтобы он выглядел следующим образо

На RTR-L добавим перенаправления dns трафика на srv

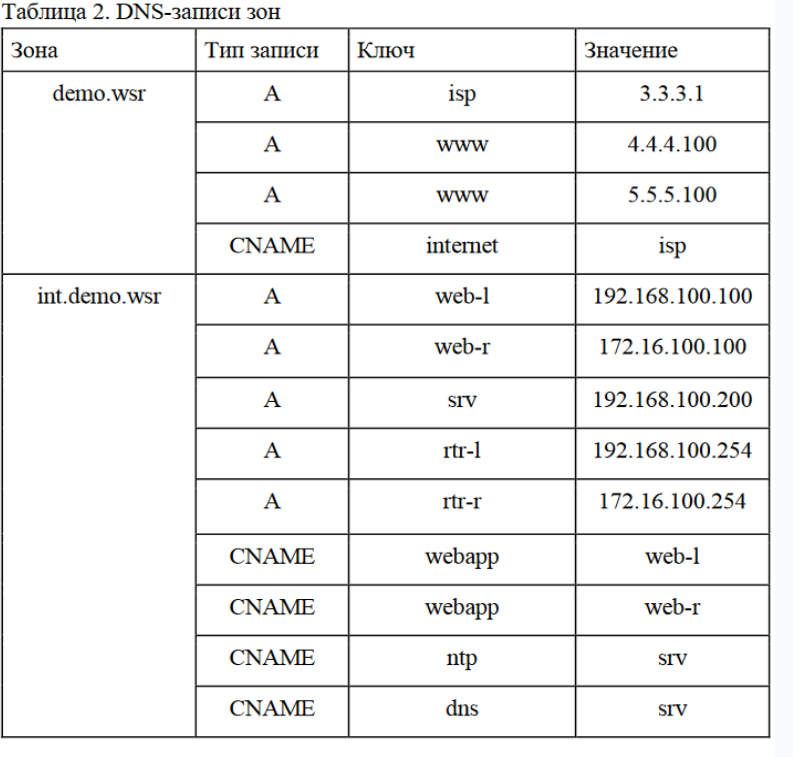
Перезагрузим службы на ISP

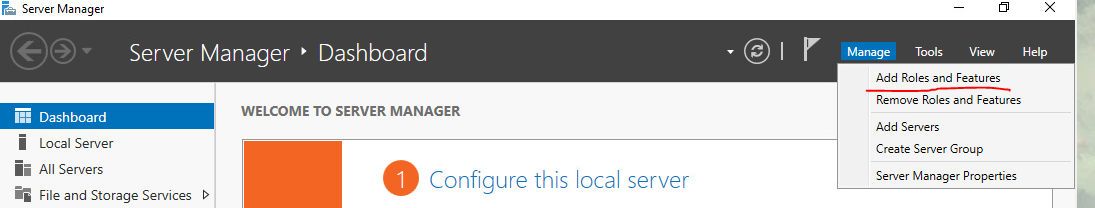


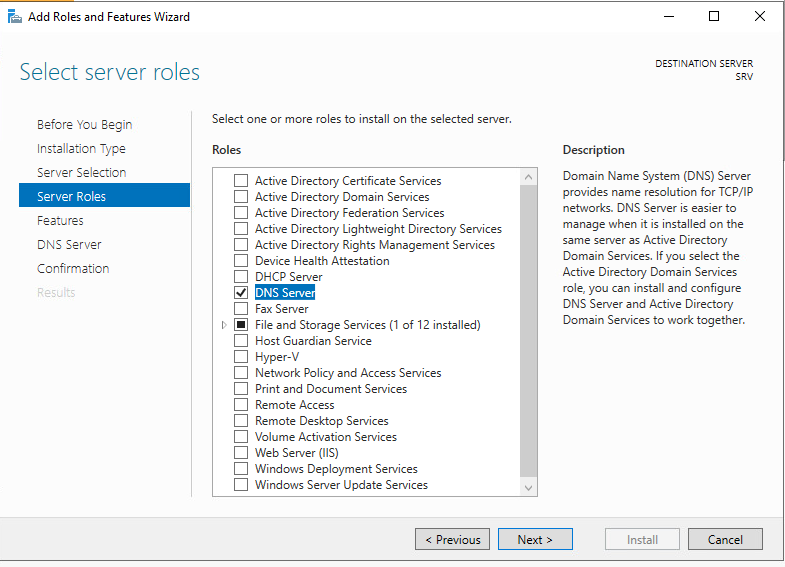
Проверим работу dns с CLI (может потребоваться перезагрузка CLI и ISP)

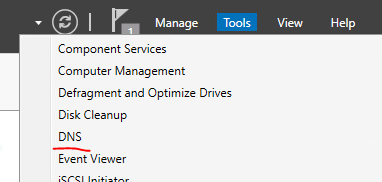


**Настроим dns на SRV**

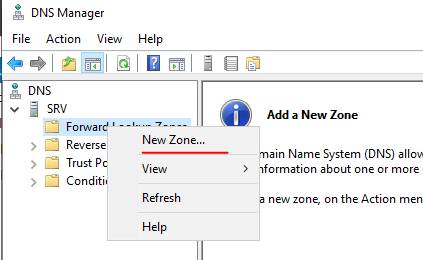


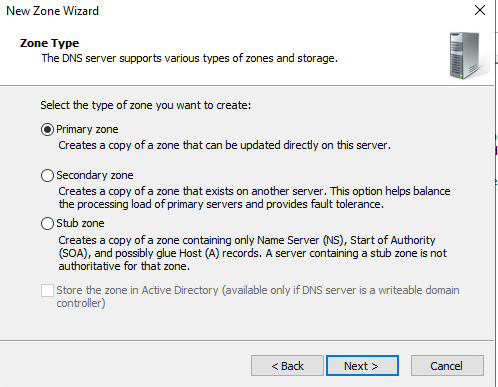


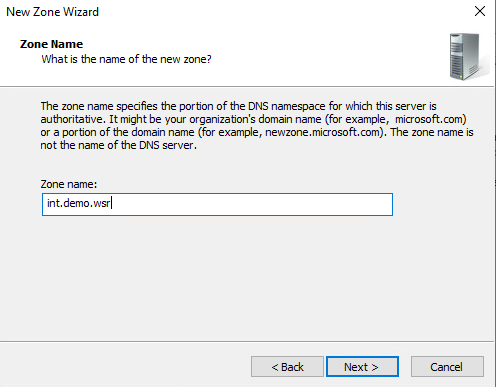


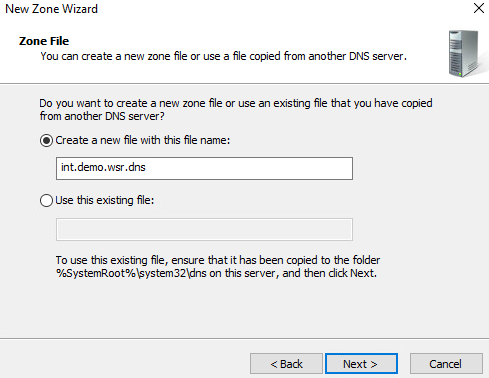


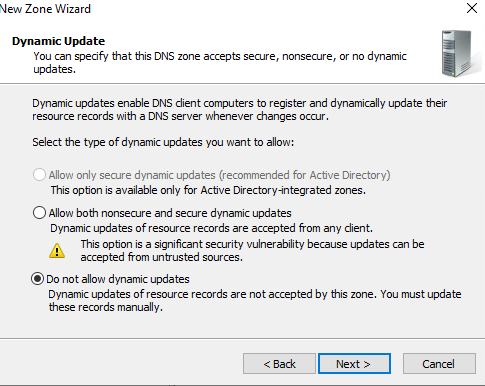
Создадим прямую зону



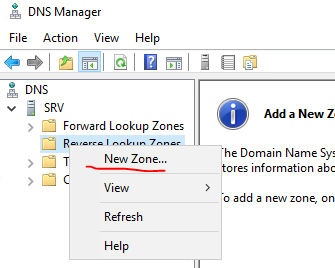


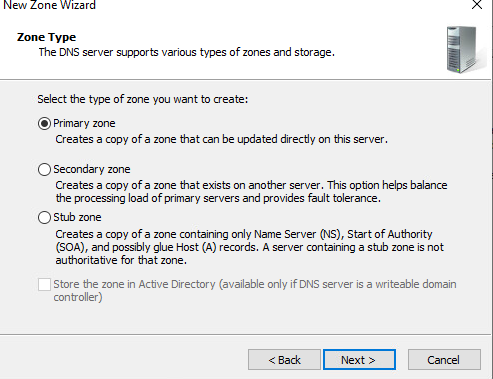


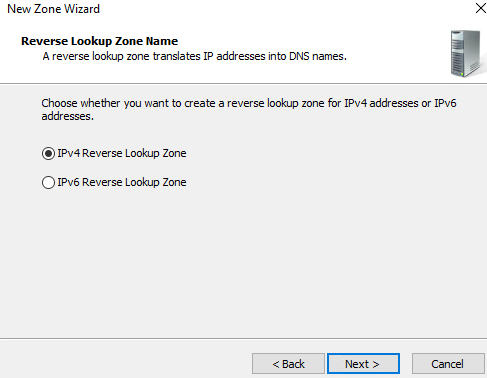


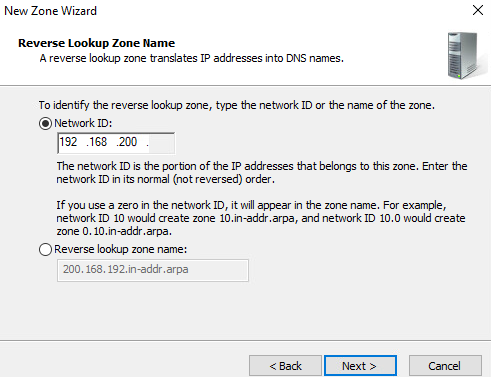


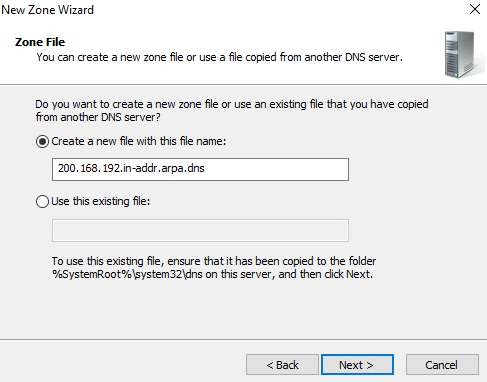
Создадим обратную зоны

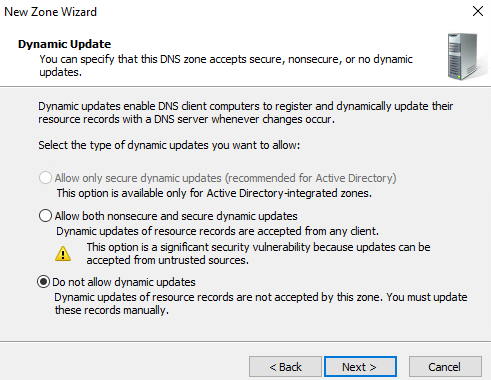


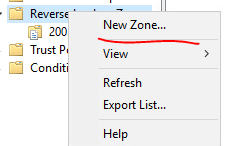


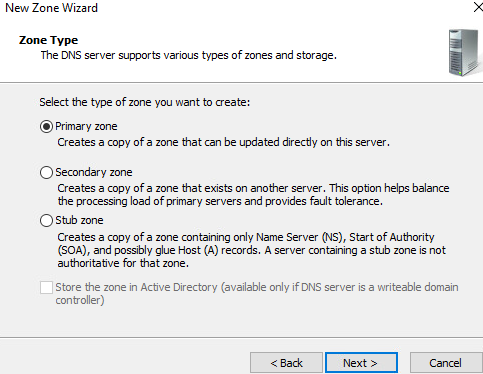


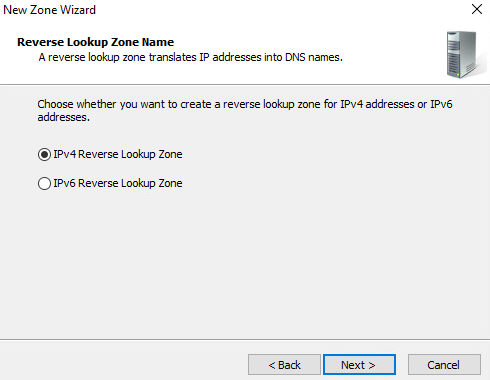


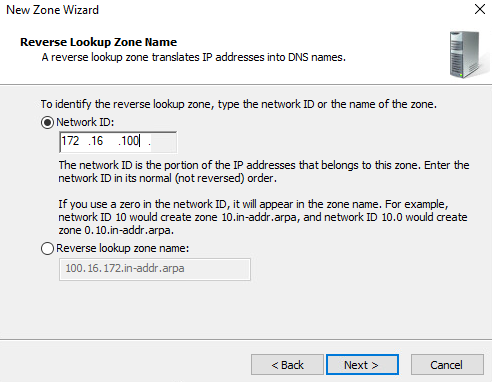


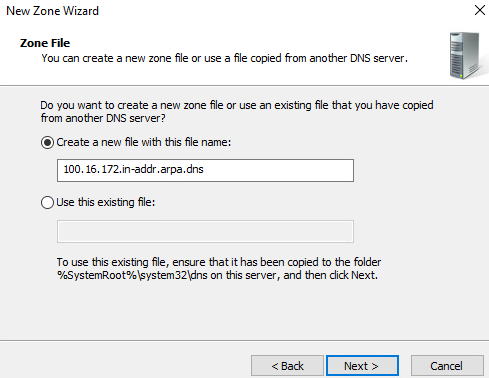


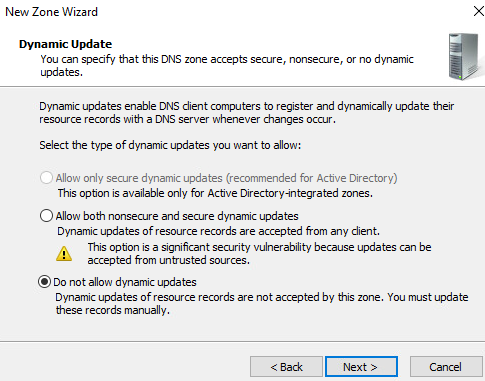




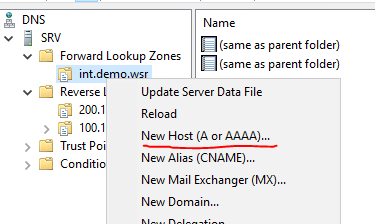


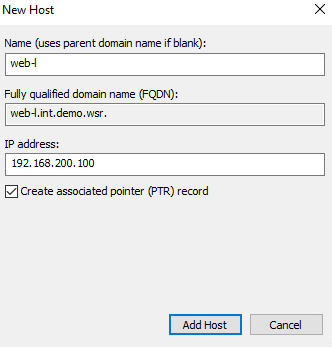


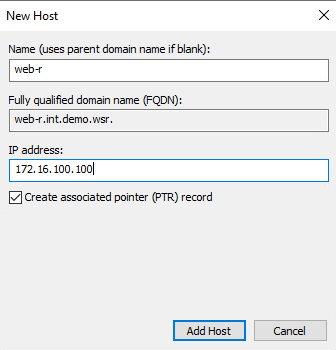


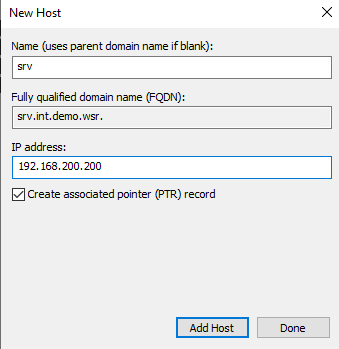


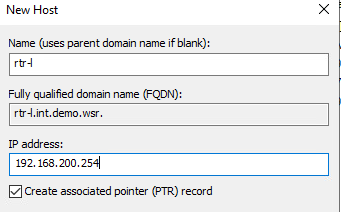
Создадим записи из таблицы 2 задания ДЭ

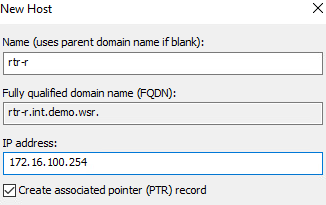


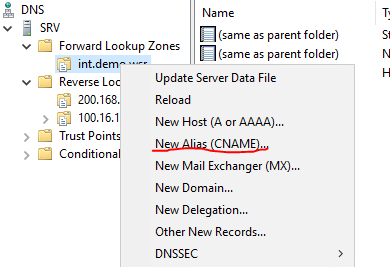


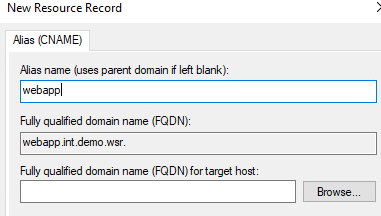




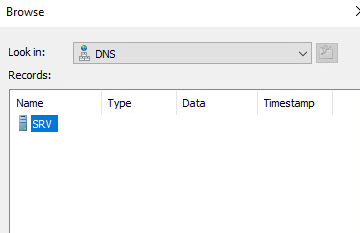


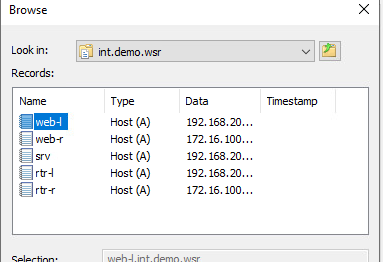


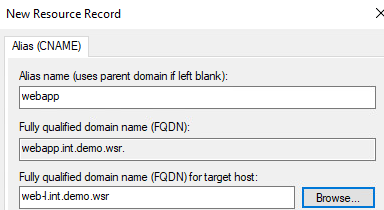


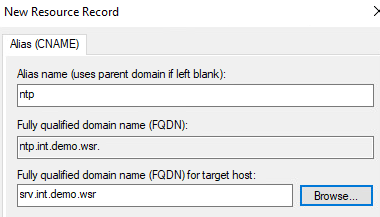


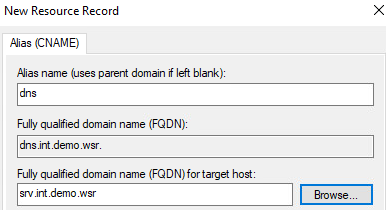
Тыкаем два раза на SRV и пробегаем по папкам



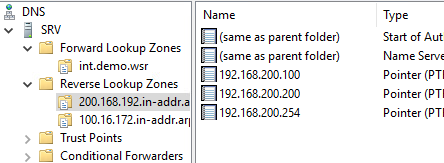


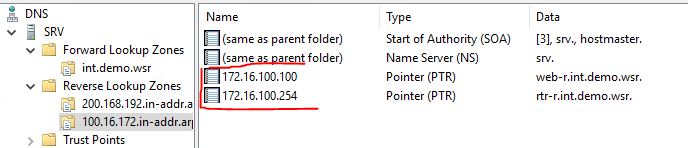




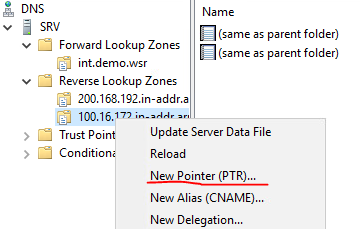


Проверяем следующие записи (если нету, попробуйте правой кликнуть и refresh)

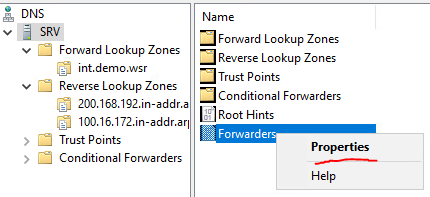


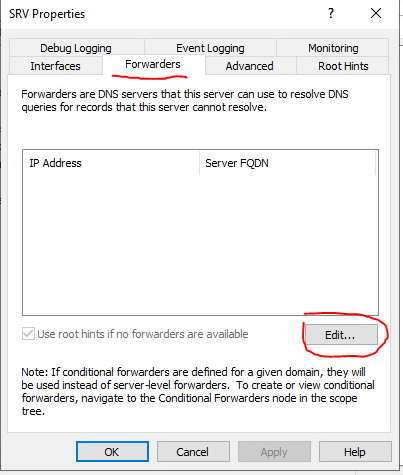


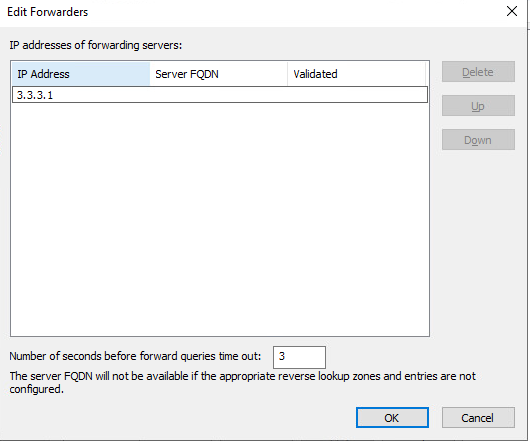
Если нету записей, создаём их так

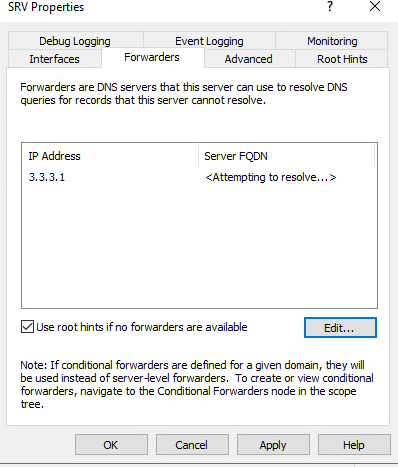


Настраиваем пересылку запросов





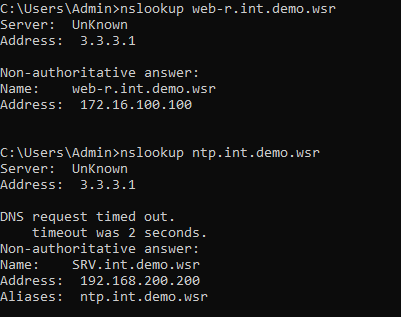
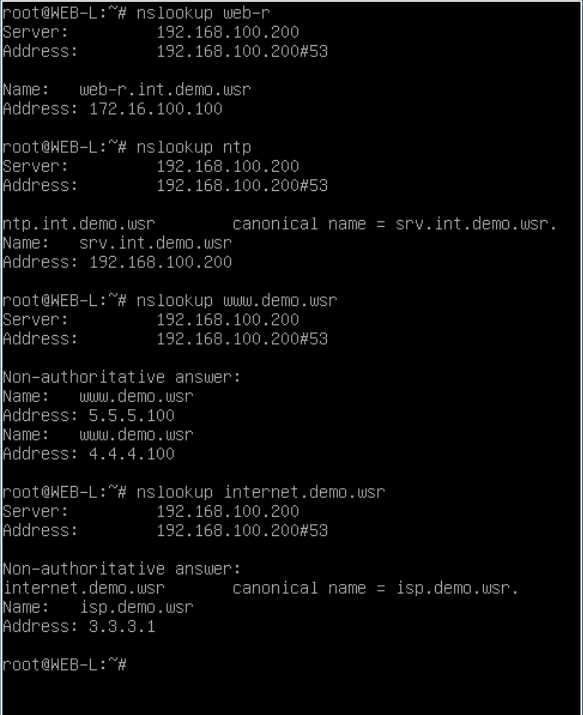


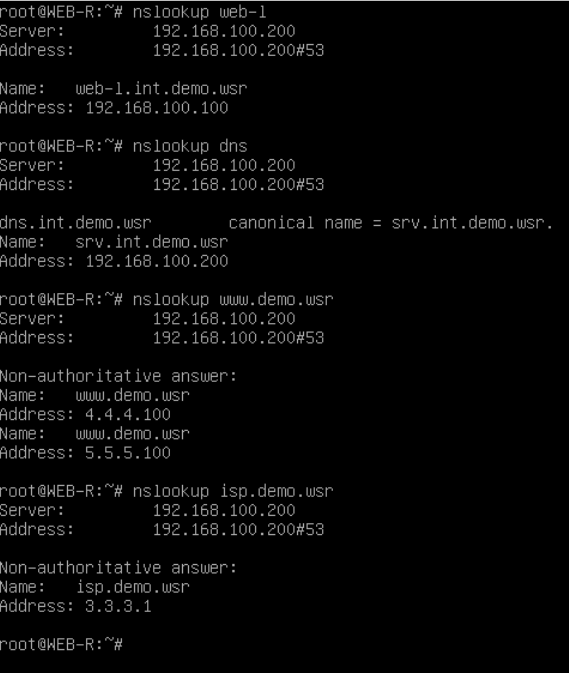


Прокинем порты для работы DNS



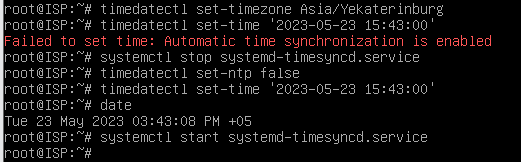
Проверка dns





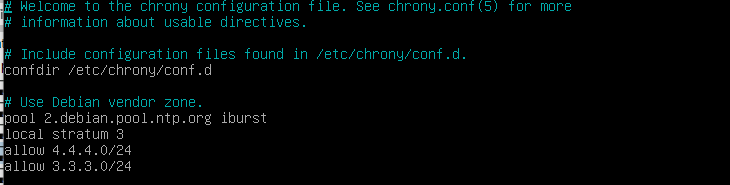
**Настройка ntp**

На ISP устанавливаем время



Скачаем пакет хрони



Отредактируем файл настроек

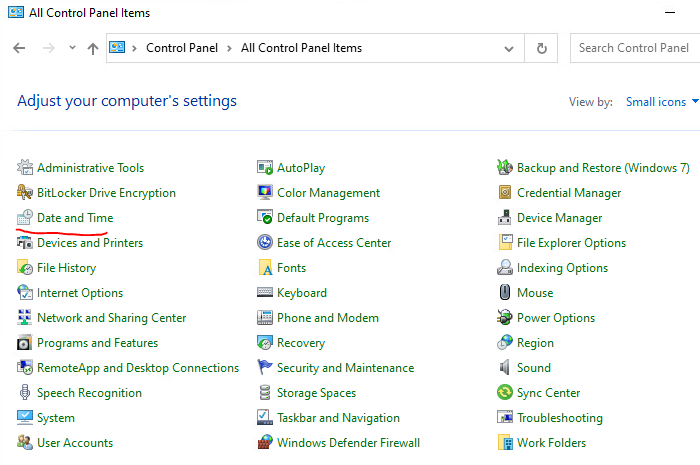
Узнаем время на isp



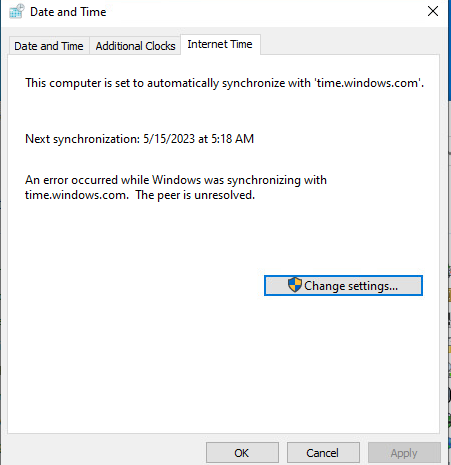
Перезагружаем ntp



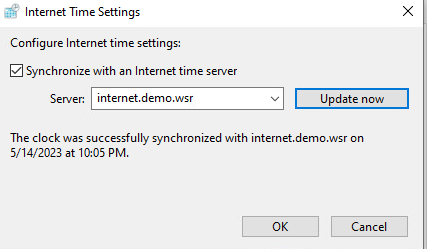
Далее переходим на CLI



Видим, что время неправильное, меняем настройки



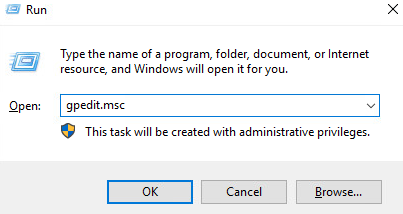
Синхронизируем время пока не появился уведомление об успешной синхронизации



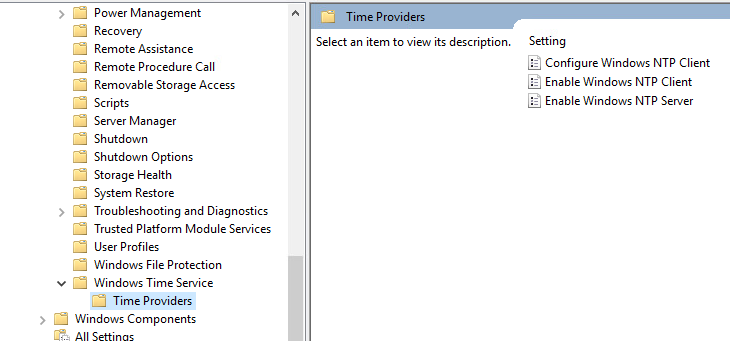
Пробрасываем NTP порт на SRV

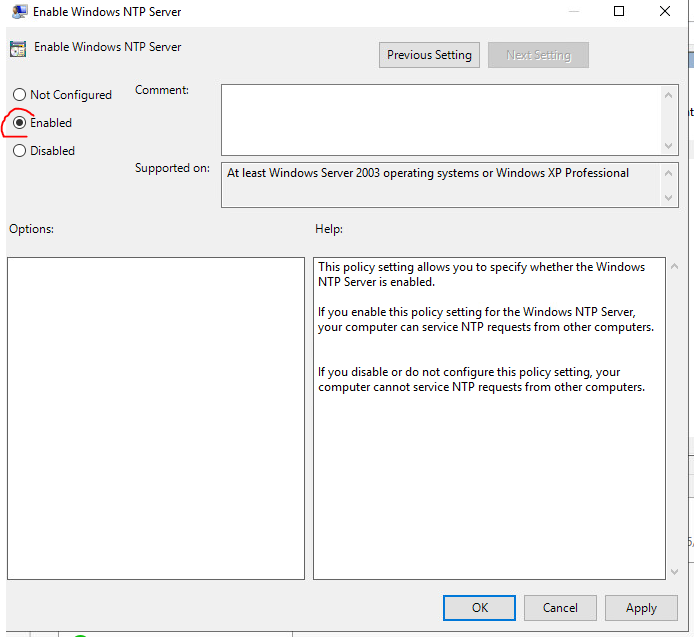
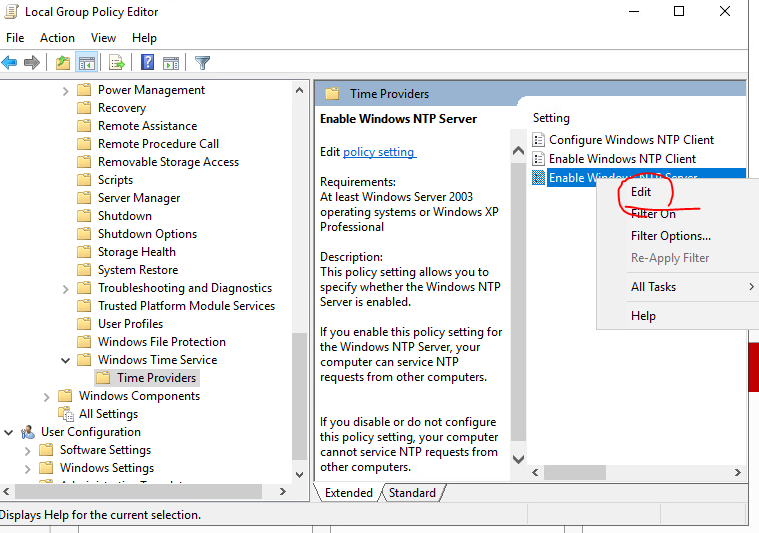
Далее переходим на SRV

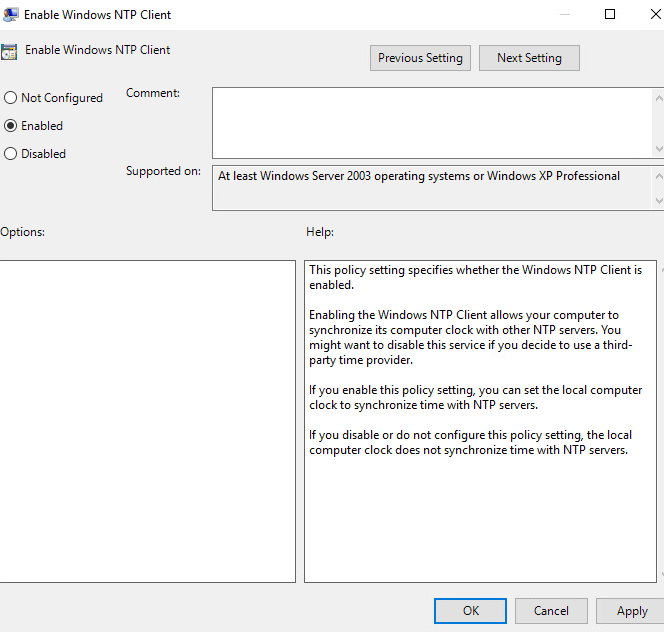
Жмякаем Win+R и прописываем следующее

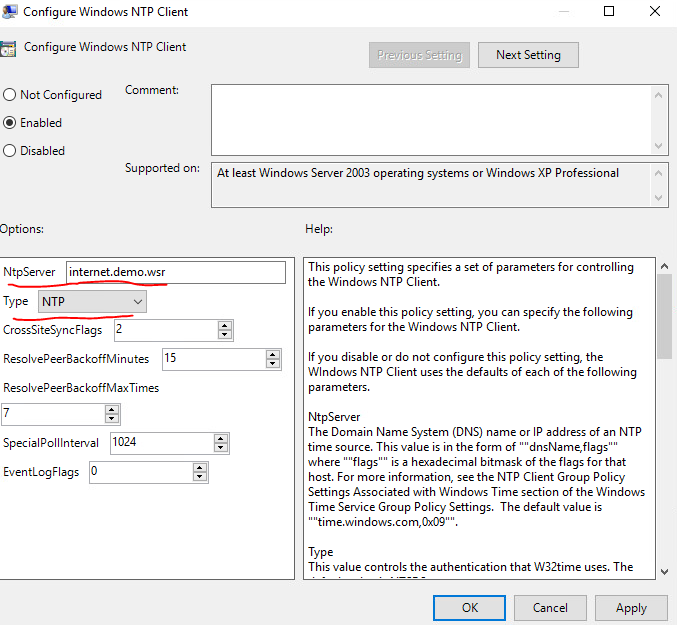


Переходим по пути Computer Configuration > Administrative Templates > System > Windows Time Service > Time Providers



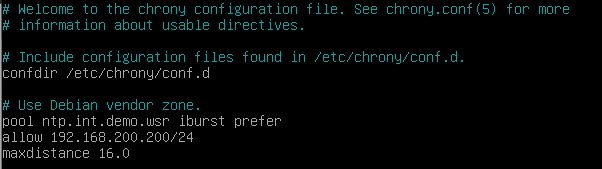






Синхронизируем время на WEB-L и WEB-R

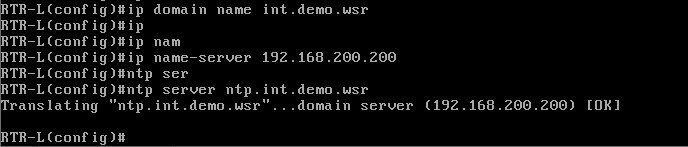
Устанавливаем хрони

Редактируем файл настроек

Перезагружаем ntp



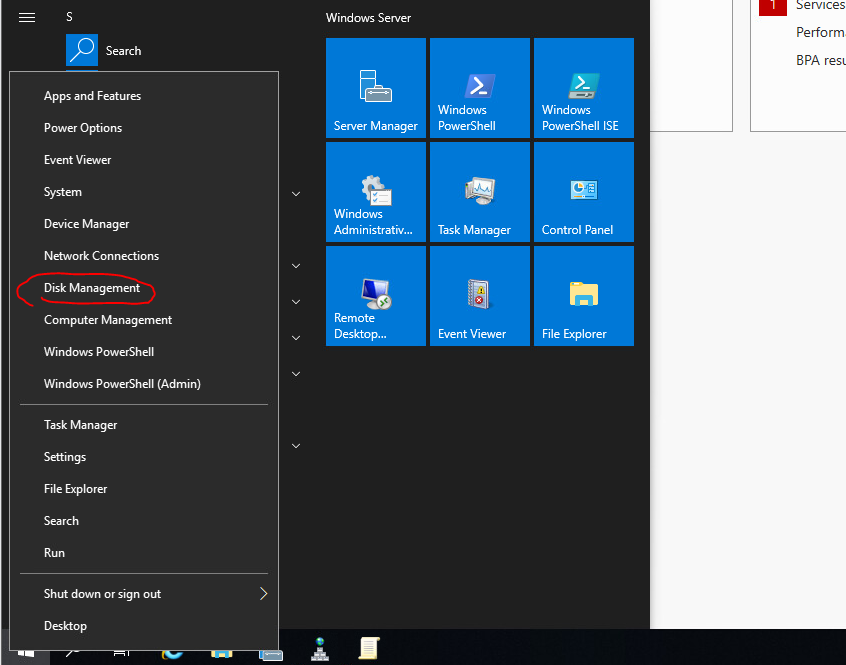
Синхронизируем время и сразу же пропишем DNS на RTR-L и RTR-R

Повторить на RTR-R

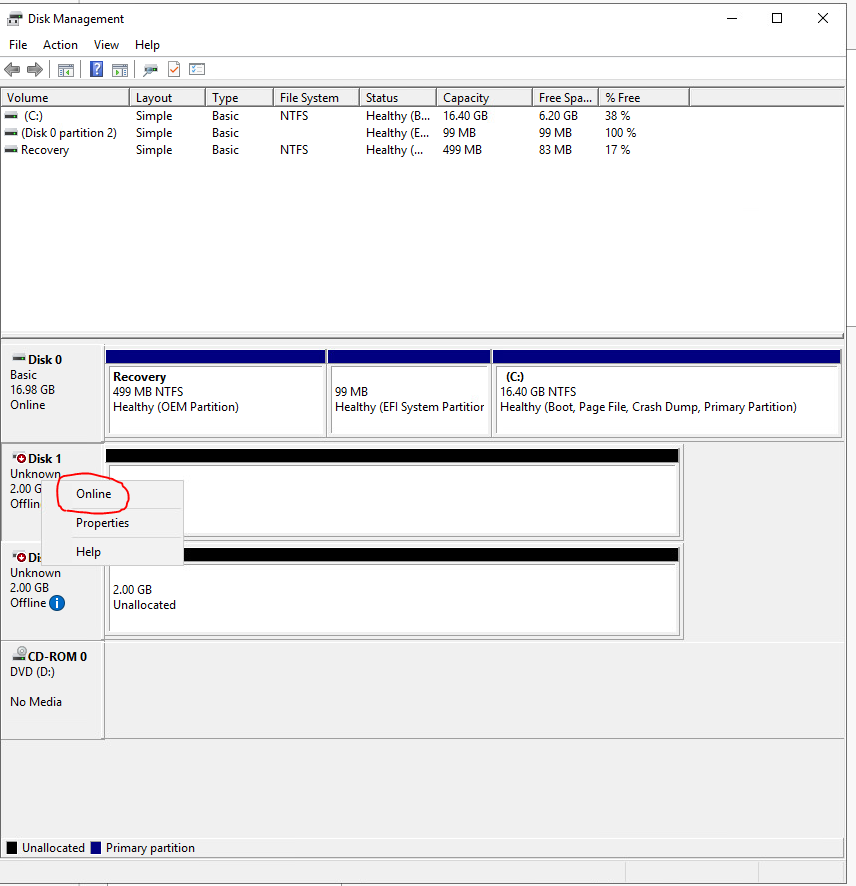
**Файловый smb сервер**

Настроим файловый сервер на SRV

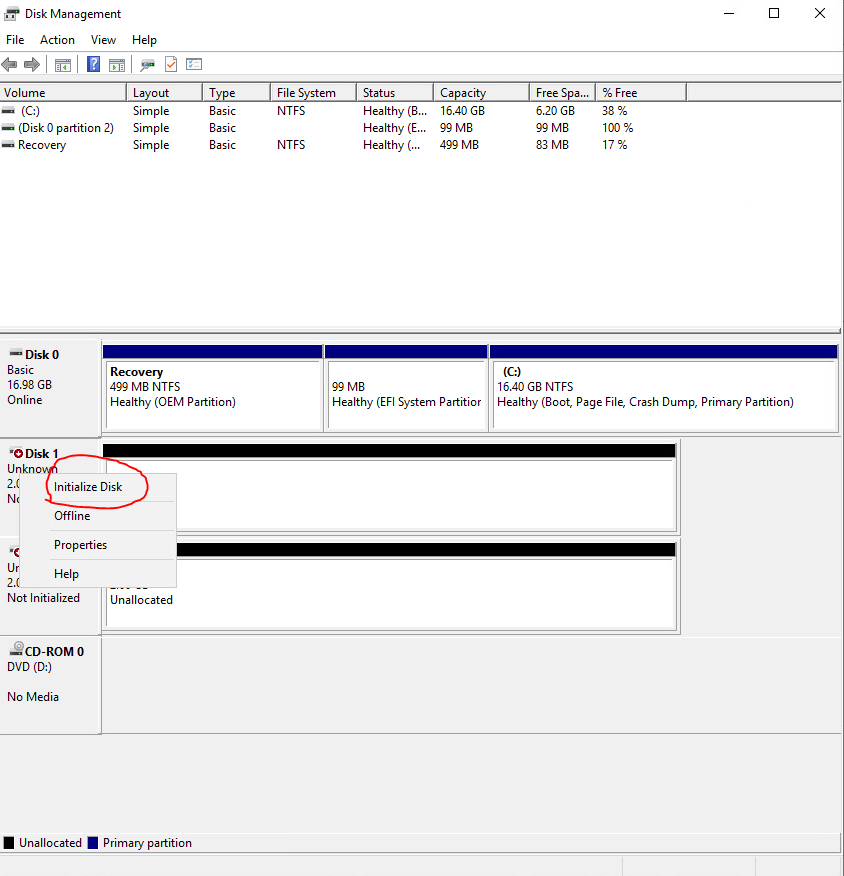
Жмякнем правой на кнопочку виндоуса и перейдем в disk management

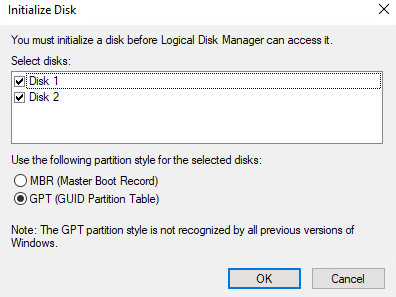


Подключаем оба диска. Тыкаем правой кнопкой и online

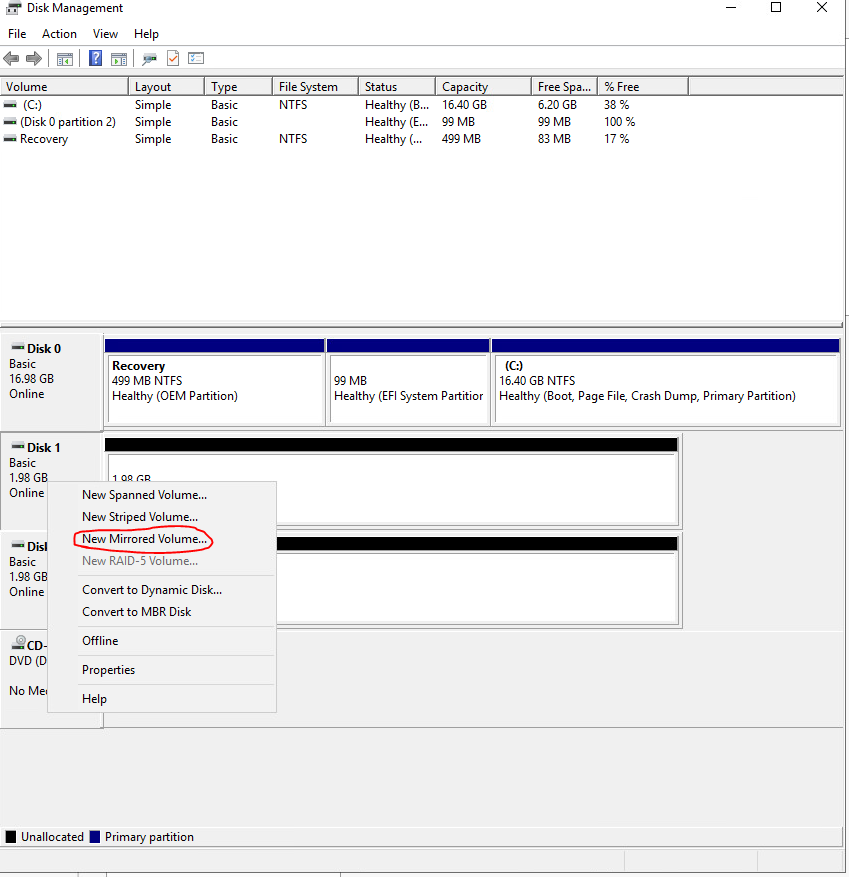


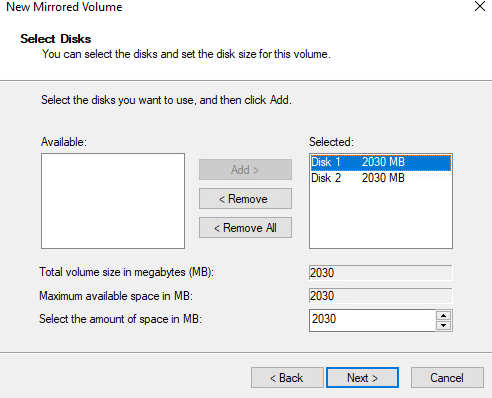
Инициализируем диски

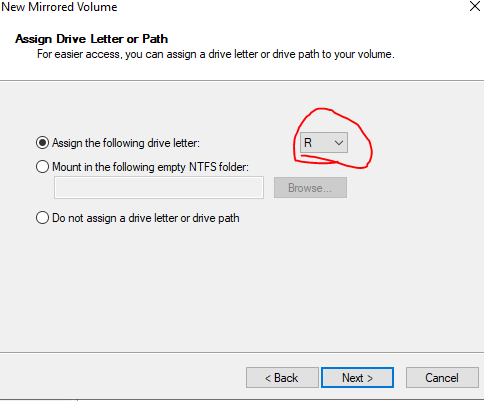


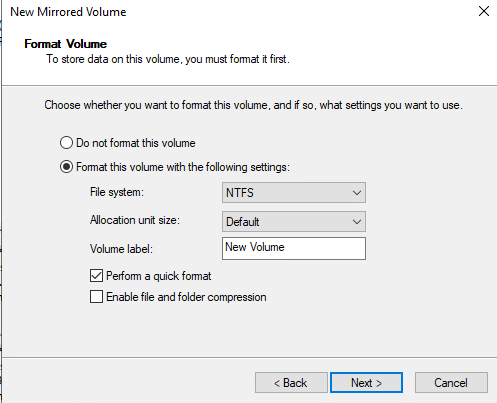


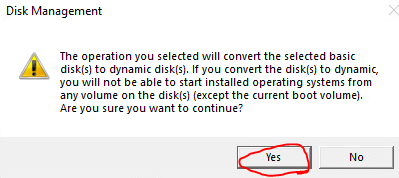
Запускаем мастер создания RAID-1 (смотрим в задание, может попасться другой рейд)



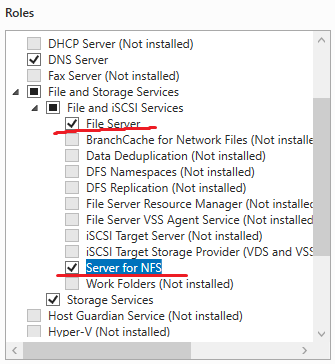
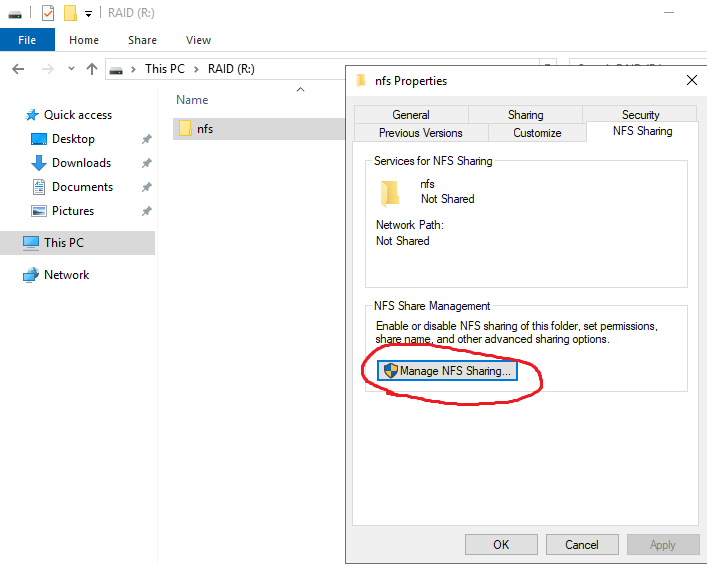


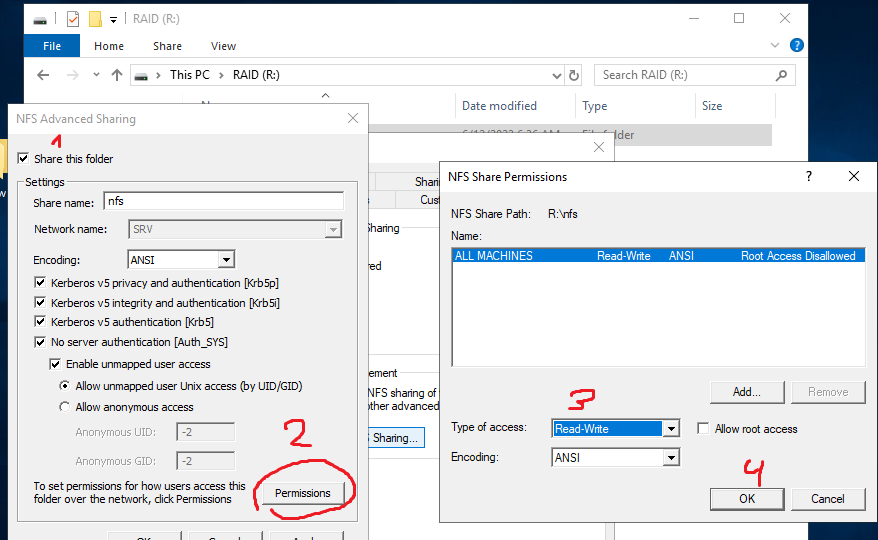






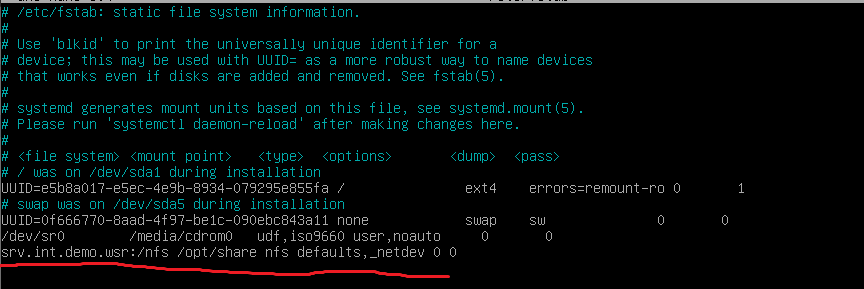
Установим nfs

После установки создаём папку и нажимаем по ней ПКМ, выбираем NFS Sharing



На WEB-L и WEB-R установим nfs-common

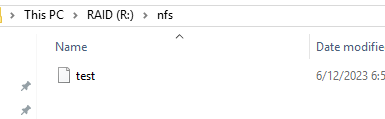
Создадим папку

И отредактируем файл /etc/fstab

Примонтируем

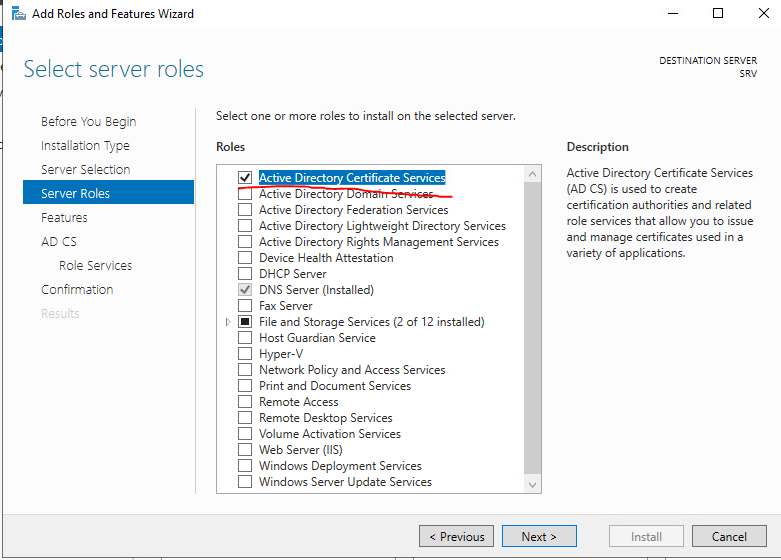
Попробуем создать файл

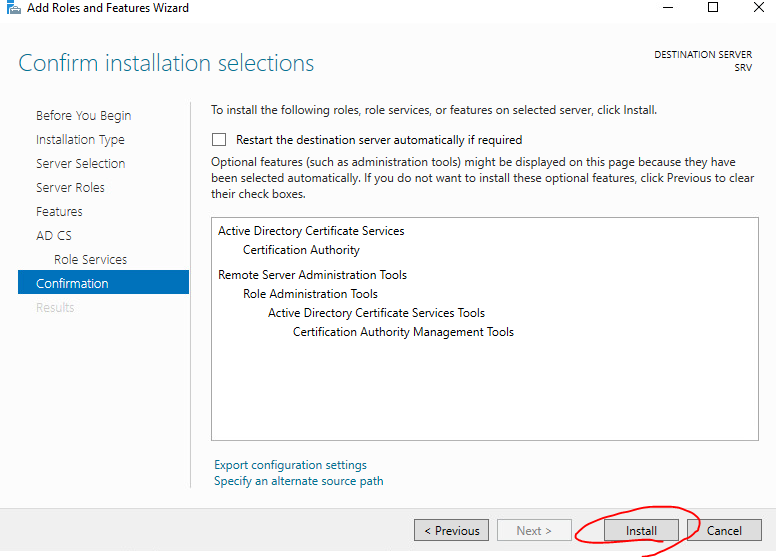
И смотрим на SRV

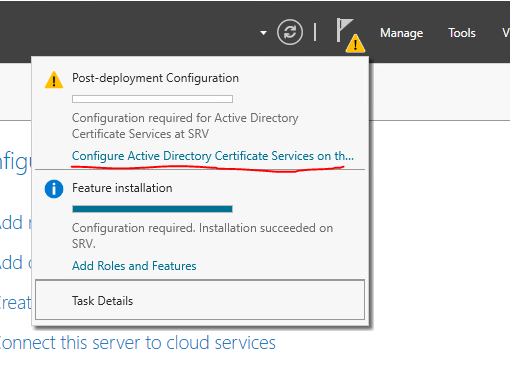


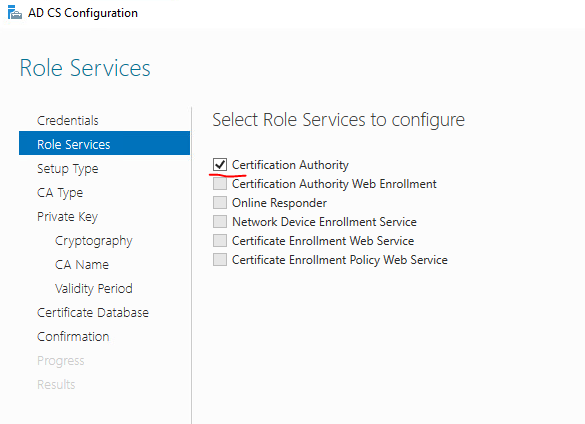
**Центр сертификации**

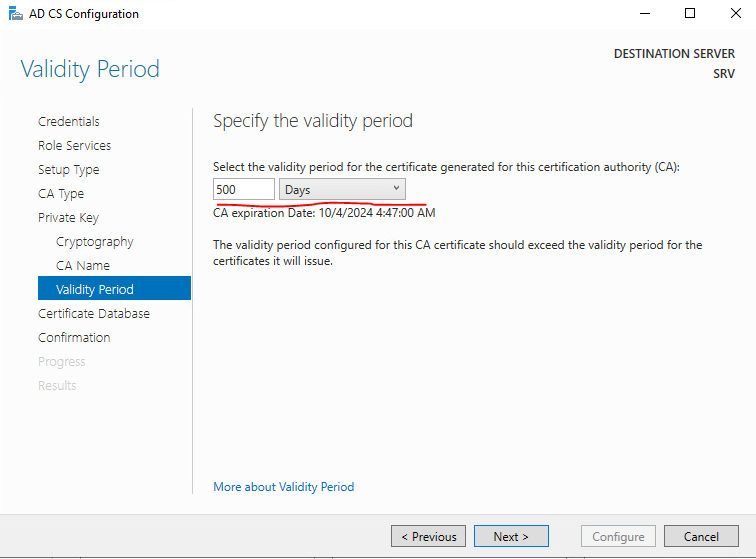
Настроим центр сертификации на SRV

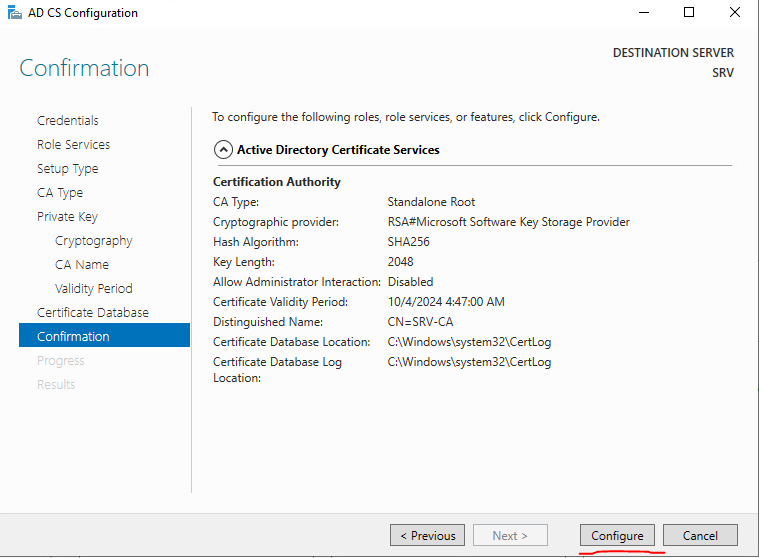


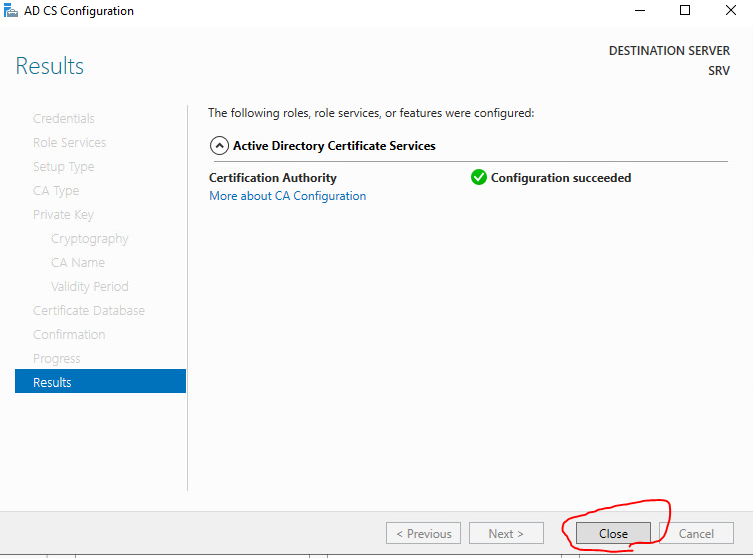




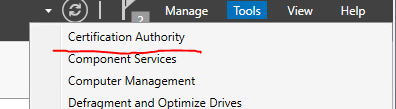


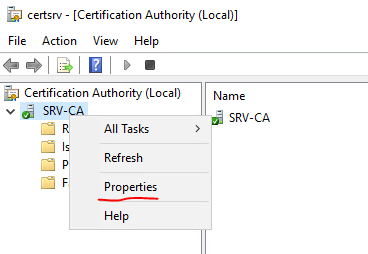


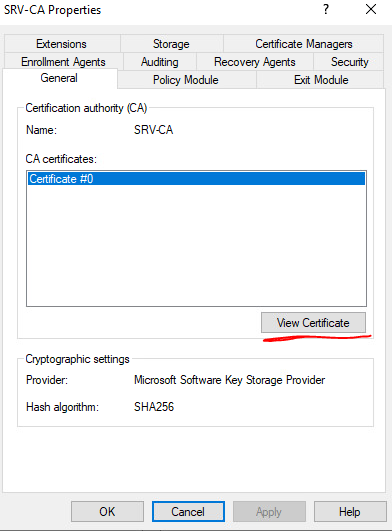


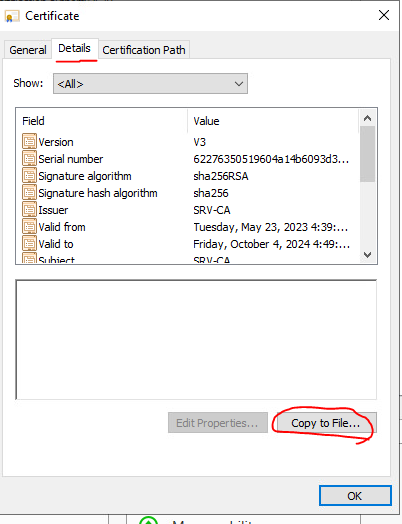


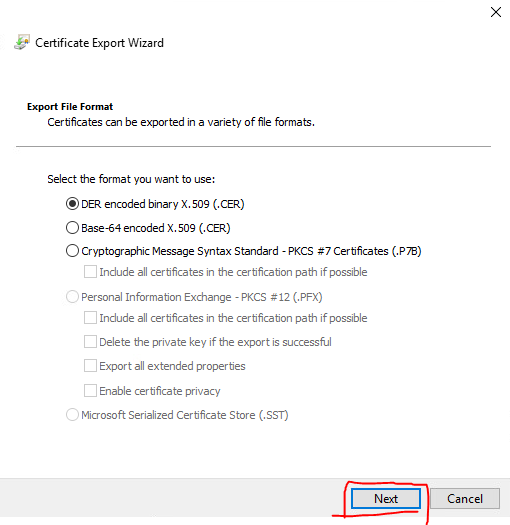
Настроим наш центр

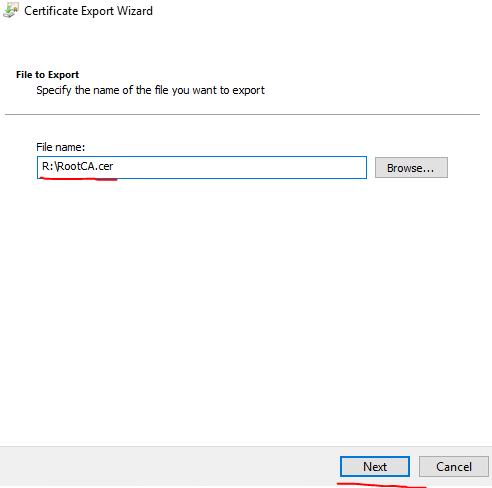


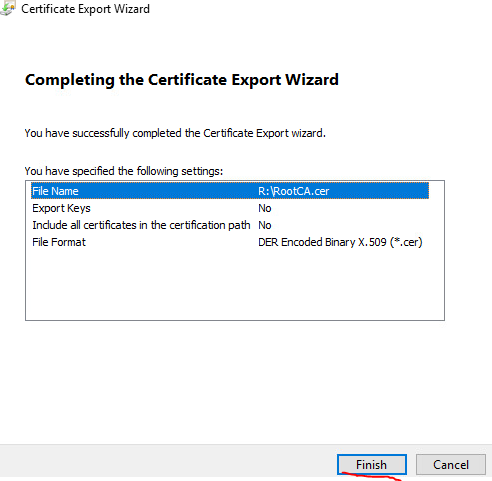


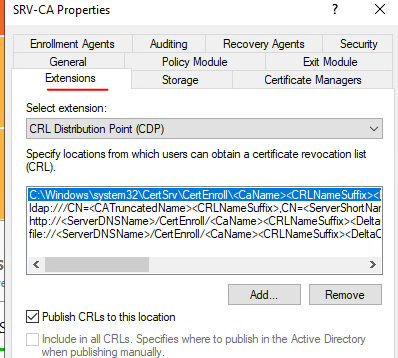


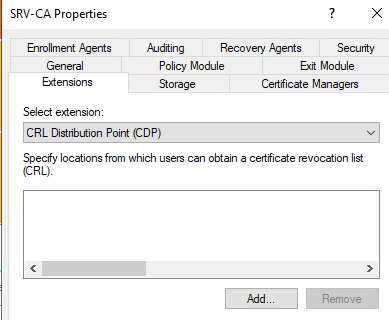


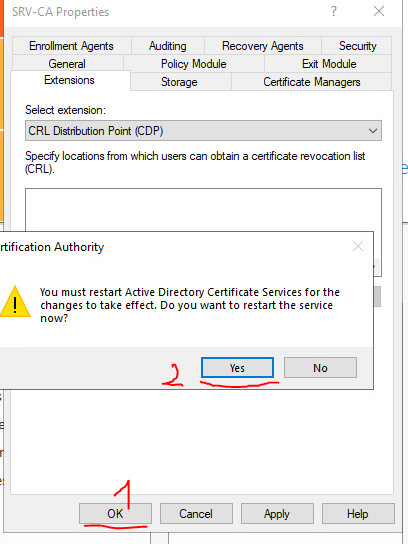


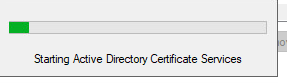




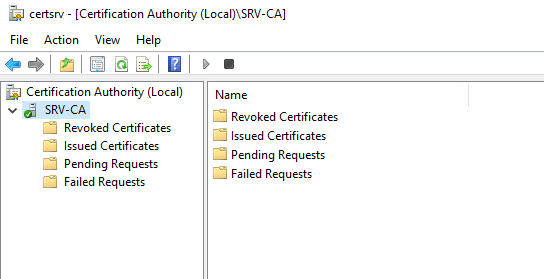








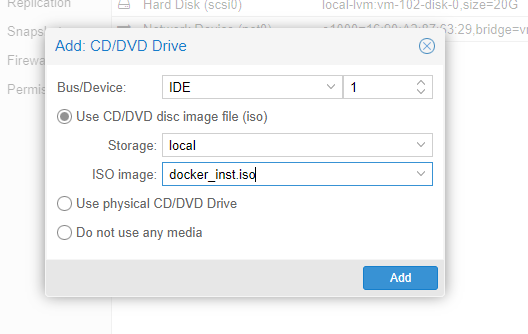
Если нет никаких ошибок, то всё должно быть так



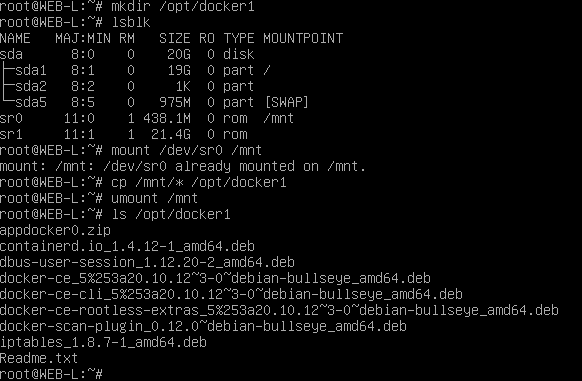
**Установим Докер**

**ВЫПОЛНЯЕМ НА WEB-L и WEB-R (ЗА ЭТО МОЖНО ПОЛУЧИТЬ МНОГО БАЛЛОВ)**

Выключаем Web-L/R и добавляем на эти машины новый диск

Выбираем в качестве образа ISO/docker

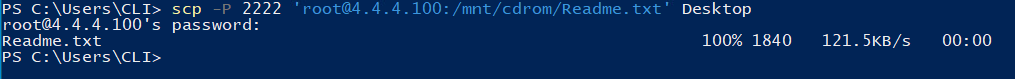
Далее запускаем машину создаём папку, монтируем наш диск и копируем с него всё в созданную папку (Если добавили сразу же, то он должен быть /dev/sr0 или /dev/sr1)



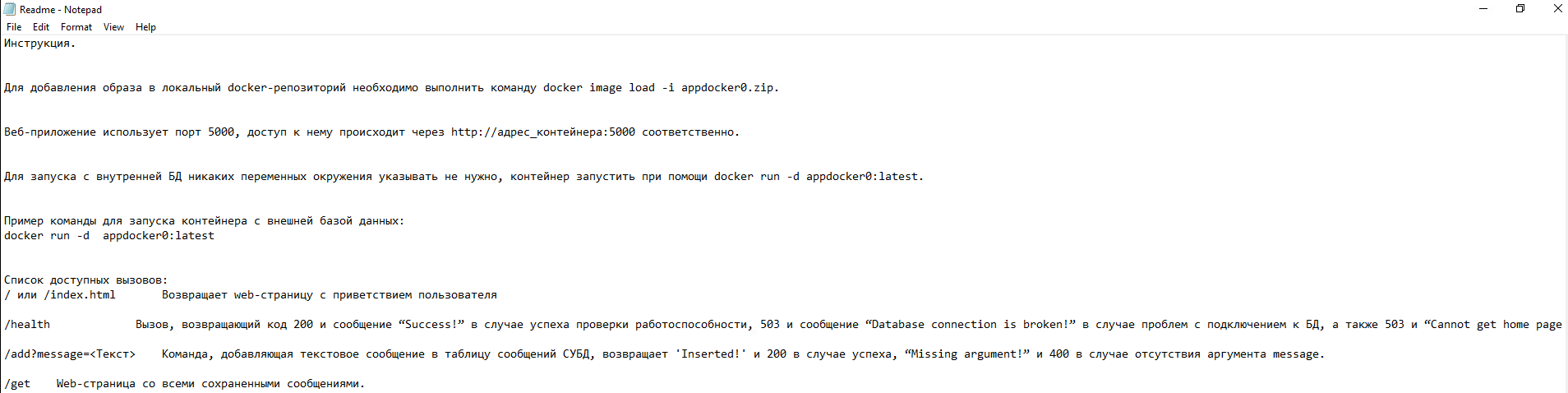
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Можно скопировать инструкцию на CLI, вдруг что-то будет другое

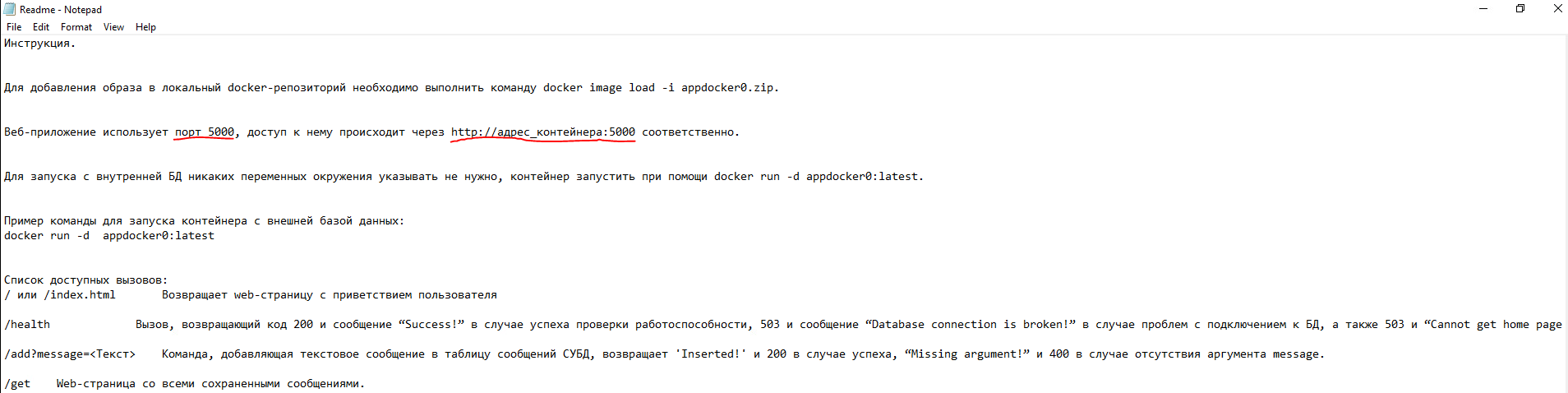
На CLI заходим в powershell и копируем инструкцию с Web-L себе на рабочий стол



Теперь можно её посмотреть

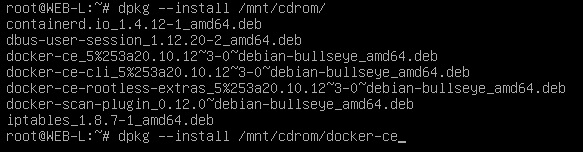


Смотрим в инструкции на порт и адрес



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Далее установим пакеты для докера



Устанавливаем следующие (Смотрим на список и просто нажимая tab добавляем)



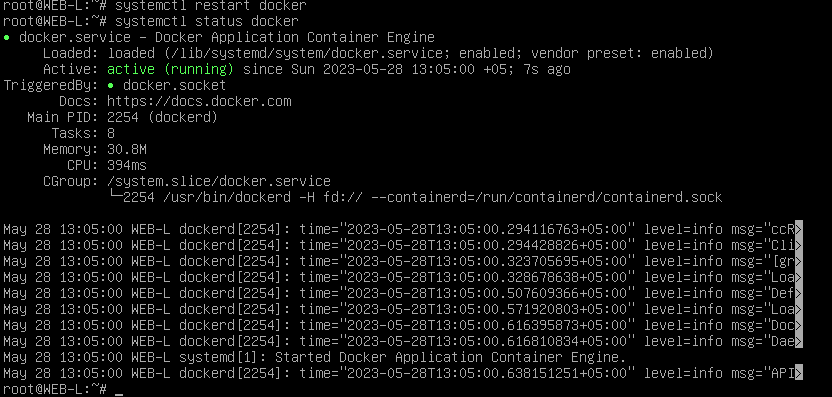




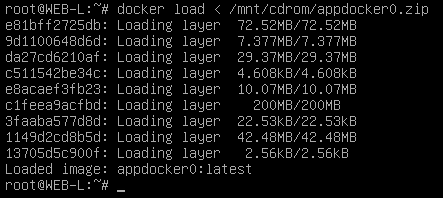
Добавим докер в автозагрузку



Перезапустим его и посмотрим статус



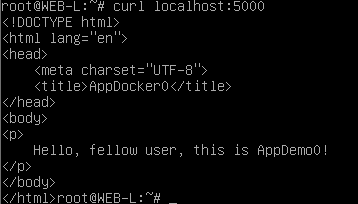
Загрузим образ докера appdocker0.zip(смотрим название в инструкции или через ls)



Создадим контейнер из образа (Смотрим на второй порт в ключе –p. Этот порт из инструкции перенаправляется на 8080)

Проверим

Теперь проверим работу докера.

Установим curl

**Настроим балансировку нагрузки через nginx**

Установим nginx на WEB-R и WEB-L



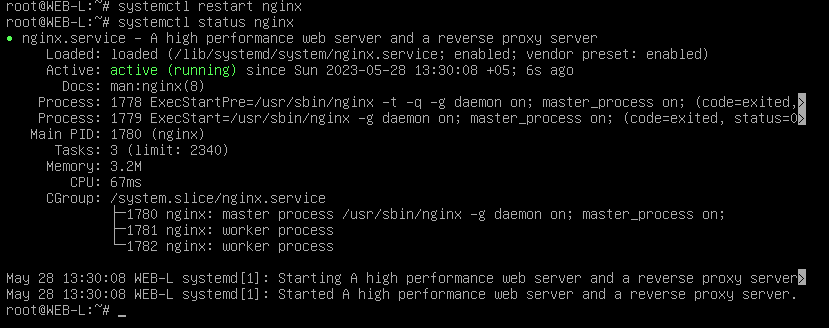
Настроим файлы nginx на WEB-L



Закомментируем все остальные строчки и добавим свои



Проверим работоспособность

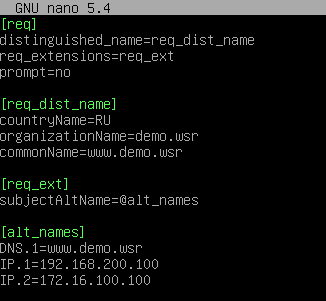


**Настроим сертификацию**

Создаём ключ на WEB-L



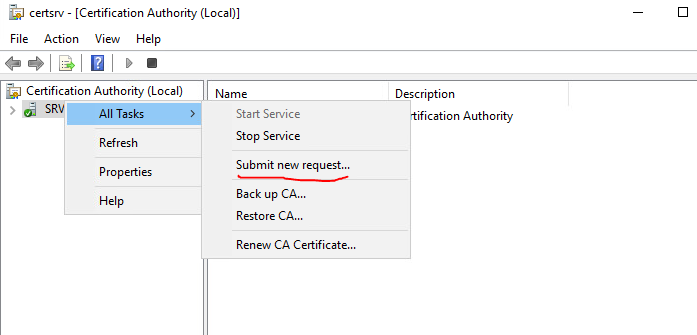
Создаём файл [www.conf](http://www.conf) и пишем следующее

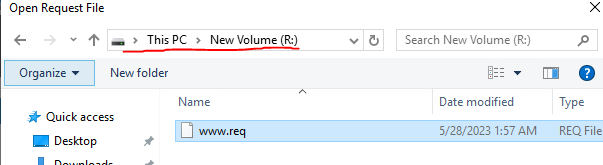


Генерируем запрос сертификата

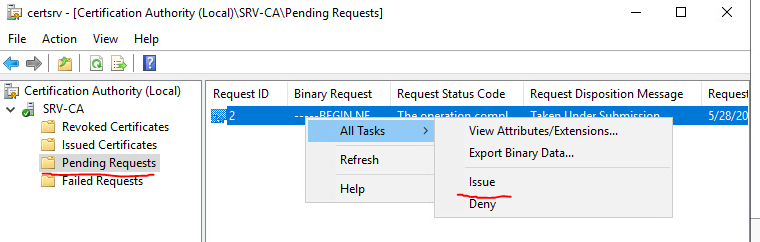


В центре сертификации на SRV настроим запрос на сертификат

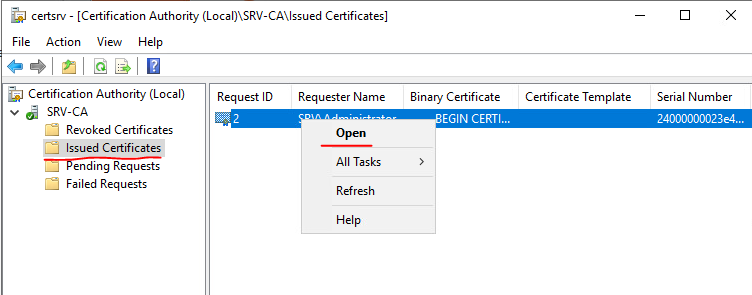


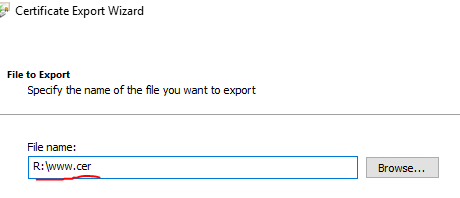
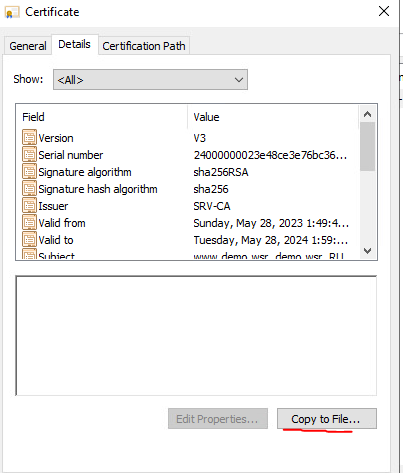


Подтвердим запрос сертификата



Сохраним новый сертификат в сетевую папку





На WEB-L конвертируем формат сертификата



Копируем приватный ключ и сертификат в папку веб сервера



Отредактируем данный файл



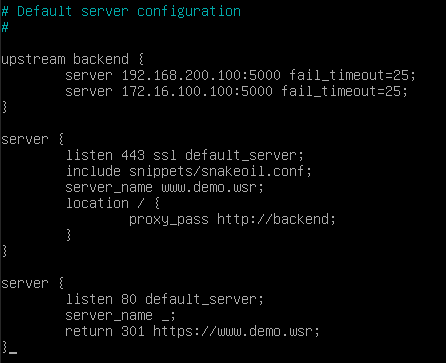
Отредактируйте его, чтобы он выглядел следующим образом



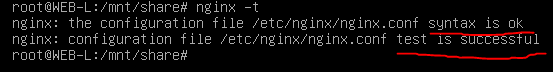
Отредактируем данный файл



Отредактируйте его, чтобы он выглядел следующим образом



Проверяем работу сервера nginx



Перезапустим nginx



Копируем файлы конфигурации в сетевую папку

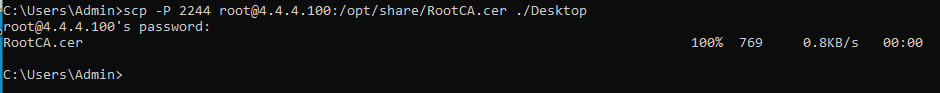


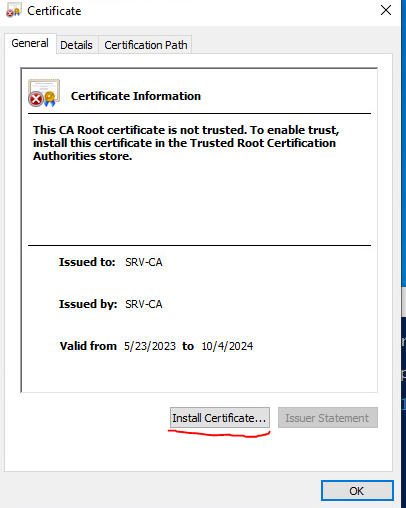
Далее переходим на WEB-R и копируем эти файлы конфигурации заместо файлов в /etc/nginx

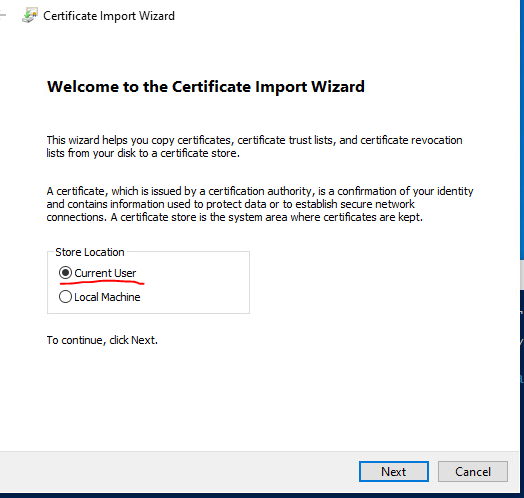


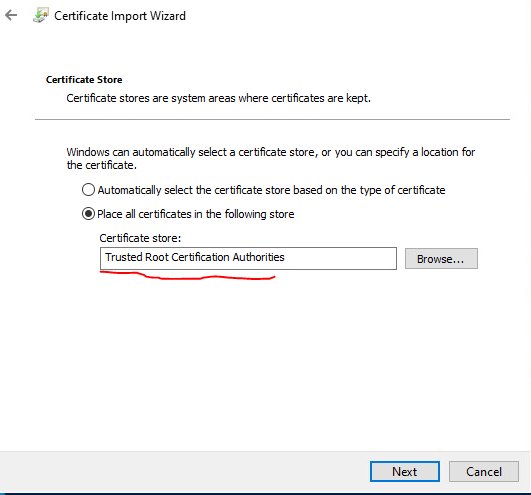
Добавим в центр сертификации SRV-CA в список доверенных на CLI

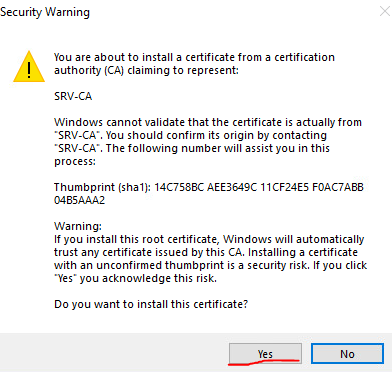
В cmd вводим следующее



Откроем его и установим сертификат







**Настройка IPSEC**

RTR-L

Вводим следующие команды:

crypto isakmp policy 1

encr aes

authentication pre-share

hash sha256

group 14

exit

crypto isakmp key cisco address 5.5.5.100

crypto isakmp nat keepalive 5

crypto ipsec transform-set SET esp-aes 256 esp-sha256-hmac

mode tunnel

exit

crypto ipsec profile VTI

set transform-set SET

interface Tunnel1

tunnel mode ipsec ipv4

tunnel protection ipsec profile VTI

RTR-R

crypto isakmp policy 1

encr aes

authentication pre-share

hash sha256

group 14

exit

crypto isakmp key cisco address 4.4.4.100

crypto isakmp nat keepalive 5

crypto ipsec transform-set SET esp-aes 256 esp-sha256-hmac

mode tunnel

exit

crypto ipsec profile VTI

set transform-set SET

interface Tunnel1

tunnel mode ipsec ipv4

tunnel protection ipsec profile VTI

**Списки контроля доступа**

RTR-L

Создадим новый список

И пропишем туда

permit tcp any any established

permit tcp any host 4.4.4.100 eq 53

permit udp any host 4.4.4.100 eq 53

permit tcp any host 4.4.4.100 eq 80

permit tcp any host 4.4.4.100 eq 443

permit tcp any host 4.4.4.100 eq 2244

permit ucp any host 4.4.4.100 eq 123

permit tcp 4.4.4.0 0.0.0.255 eq 53 any

permit udp 4.4.4.0 0.0.0.255 any eq 53 any

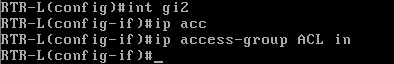
permit gre host 5.5.5.100 host 4.4.4.100

permit udp host 5.5.5.100 host 4.4.4.100 eq 500

permit esp any any

permit icmp any any

Привяжем его к интерфейсу



RTR-R

Создаём такой же список

И вводим

permit tcp any any established

permit tcp any host 5.5.5.100 eq 80

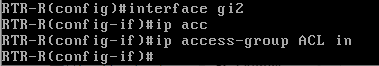
permit tcp any host 5.5.5.100 eq 443

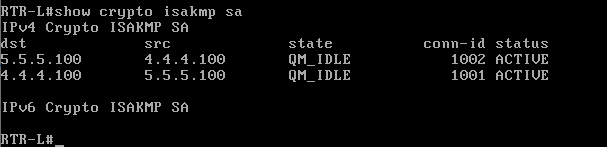
permit tcp any host 5.5.5.100 eq 2244

permit udp host 5.5.5.100 host 4.4.4.100 eq 500

permit gre host 4.4.4.100 host 5.5.5.100

permit esp any any

permit icmp any any

Проверим работу ipsec

**Проверка**

Проверим работу сертификата на CLI

Нас должно перекинуть на https

