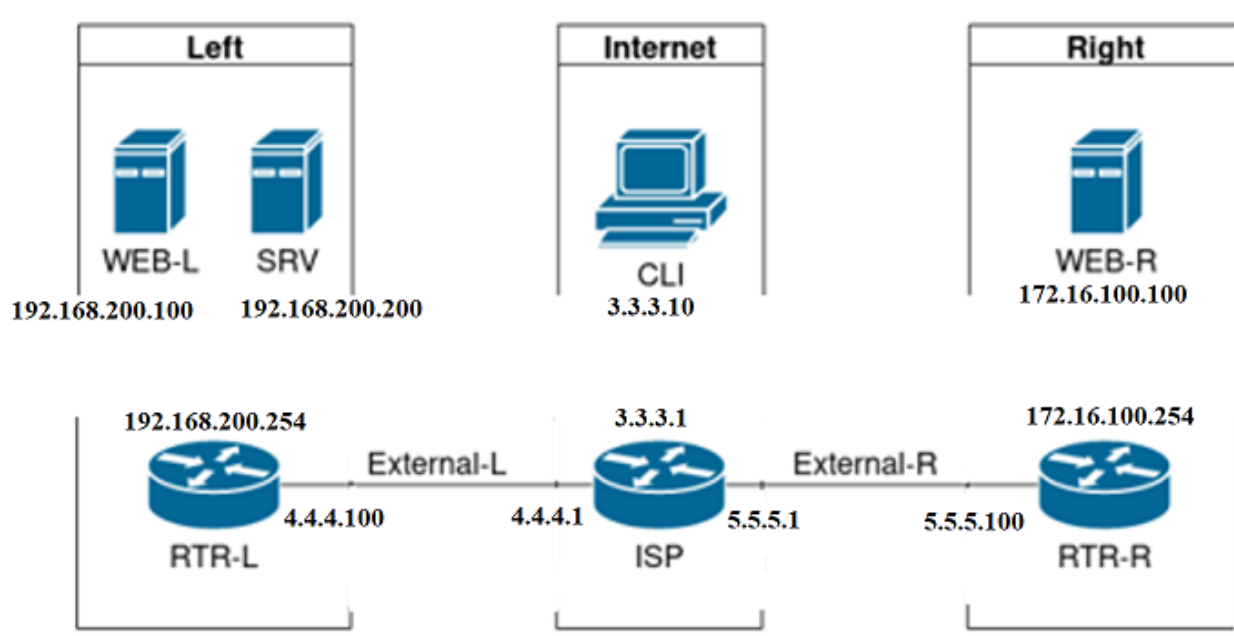


Схема



Имя ВМ	ОС	ОЗУ	Кол- во ядер	IP-адреса	Дополнительно
RTR- L	Debian 11	2 Гб	2	4.4.4.100/24 192.168.200.254/ 24	
	Cisco CSR		4		
RTR- R	Debian 11	2 Гб	2	5.5.5.100/24 172.16.100.254/2 4	
	Cisco CSR	4 Гб	4		
SRV	Debian 11	2 Гб	2		
	Windows Server 2019	4 Гб	4	192.168.200.200/ 24	Дополнительные диски: 2 шт по 2 Гб
WEB- L	Debian 11	2 Гб	2	192.168.200.100/ 24	
WEB- R	Debian 11	2 Гб	2	172.16.100.100/2 4	
ISP	Debian 11	2 Гб	2	4.4.4.1/24 5.5.5.1/24 3.3.3.1/24	
CLI	Windows 10	4	4	3.3.3.10/24	

SRV-deb в самом конце

Возможность пропускать через себя пакеты

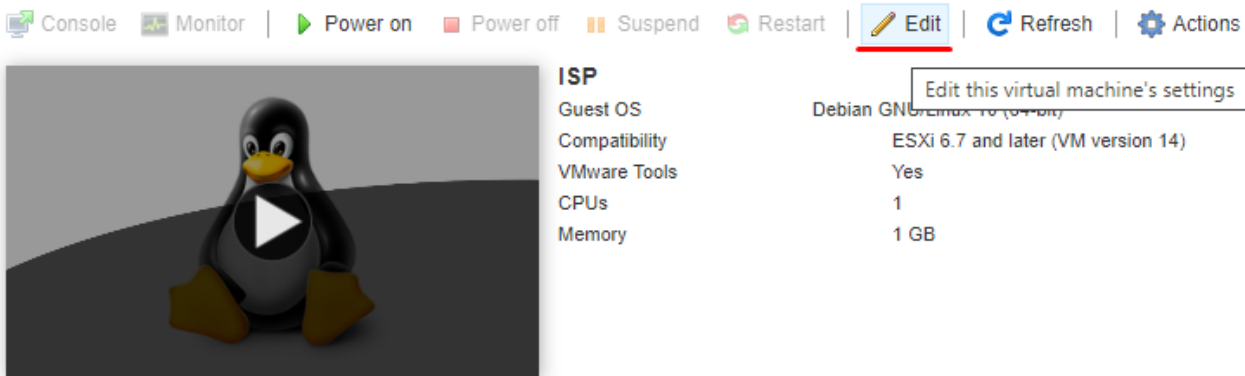
- nano /etc/sysctl.conf
 - раскомментировать (удалить #) строку net.ipv4.ip_forward 1

Доступ по ssh для рута

- apt install openssh-server **установка ssh или проверка того что он уже установлен**
- nano /etc/ssh/sshd_config
 - раскомментировать (удалить #) строку PermitRootLogin yes
- systemctl restart sshd

Добавление диска в репозитории

Жмем Edit



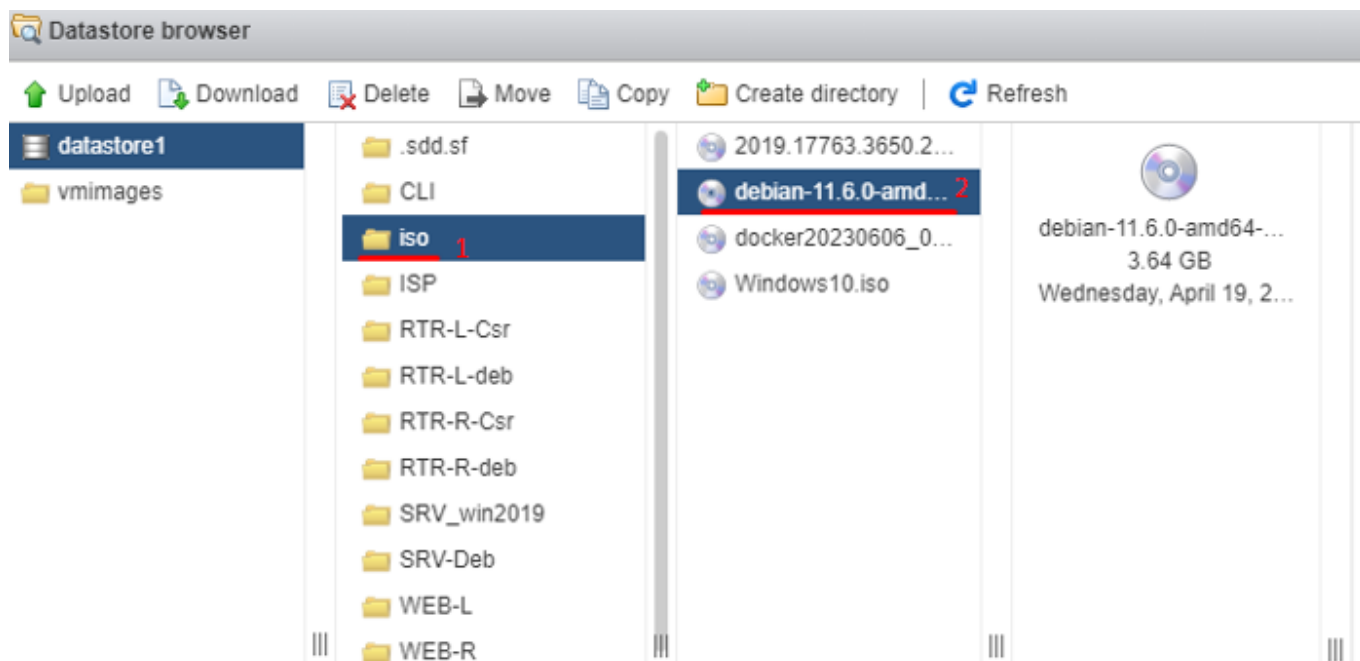
The screenshot shows the VMware Workstation interface. At the top, there is a toolbar with buttons for Console, Monitor, Power on, Power off, Suspend, Restart, Edit (highlighted with a red line), Refresh, and Actions. Below the toolbar, there is a preview window showing a penguin icon. To the right of the preview, the virtual machine's name 'ISP' is displayed, along with its Guest OS (Debian GNU/Linux 10 (64-bit)), Compatibility (ESXi 6.7 and later (VM version 14)), VMware Tools (Yes), CPUs (1), and Memory (1 GB). A tooltip 'Edit this virtual machine's settings' is visible over the 'Edit' button.

Below the main interface, the 'Edit settings - ISP (ESXi 6.7 virtual machine)' window is open. It shows a list of hardware components and their settings:

Component	Setting	Connect
USB controller 1	USB 2.0	
Network Adapter 1	VM Network	<input type="checkbox"/>
Network Adapter 2	ISP	<input checked="" type="checkbox"/>
Network Adapter 3	Left-ISP	<input checked="" type="checkbox"/>
Network Adapter 4	Right-ISP	<input checked="" type="checkbox"/>
CD/DVD Drive 1	Datastore ISO file	
Status	<input checked="" type="checkbox"/> Connect at power on	
CD/DVD Media	[datastore1] iso/debian-11.6.0-amd64-DVD-1.iso	
Controller location	SATA controller 0, SATA (0:0)	
Video Card	Specify custom settings	

At the bottom of the window, there are 'Save' and 'Cancel' buttons.

Дальше выбираем диск, для большинства пакетов нужен диск BD 1. (debian.....BD_1.iso)



[datastore1] iso/debian-11.6.0-amd64-DVD-1.iso

3

Select

Cancel

Если спросит то йес

Answer question - ISP



The guest operating system has locked the CD-ROM door and is probably using the CD-ROM, which can prevent the guest from recognizing media changes. If possible, eject the CD-ROM from inside the guest before disconnecting. Disconnect anyway and override the lock?

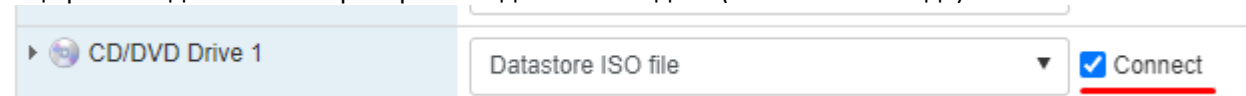
☒ Yes

☐ No

Answer

Cancel

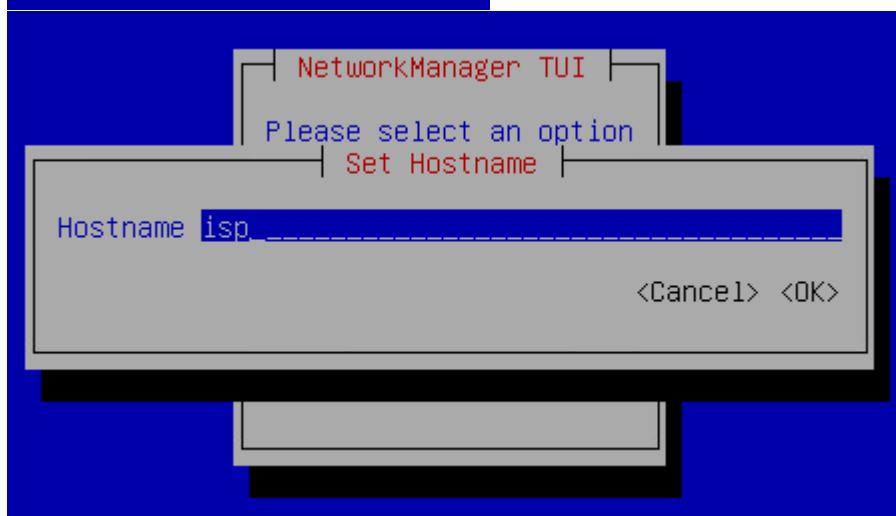
Ещё раз заходим в Edit и проверяем подключен ли диск (стоит галочка = да).



- apt-cdrom add
- apt update

Настройка имени

в nmtui



После перезагрузки применится и будет показываться в консоли

```
root@isp:~#
```

или

- `hostnamectl set-hostname %имя%` + поменять в `/etc/hosts`

Адресация

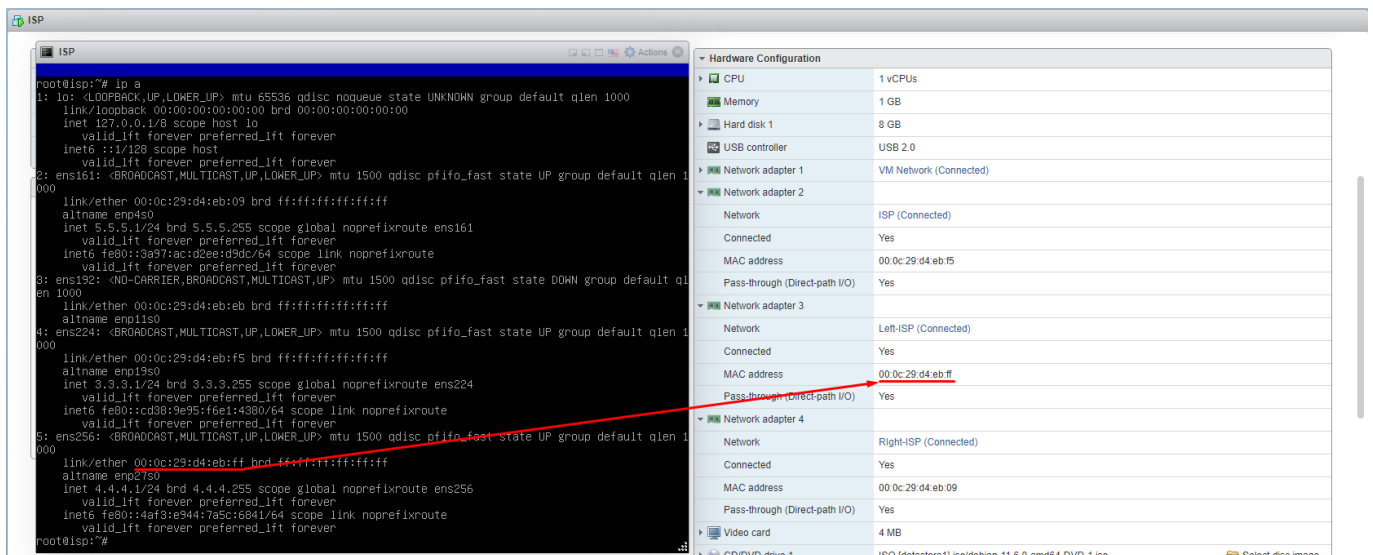
Для начала проверить имена интерфейсов.

Для этого нужно ввести `ip a` на линуксе.

- `ip a >` показывает интерфейсы

Смотрим MAC-адрес интерфейса

Сверяемся с `esxi` (нажимаем на интерфейс сетевой карты и смотрим мак адрес)



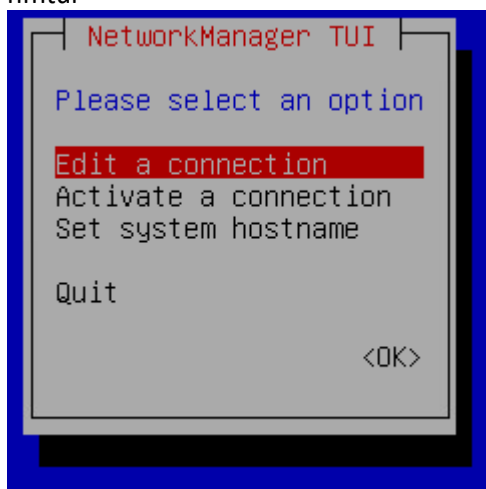
Сопоставляем мак адреса и смотрим в том же esxi название сегмента локальной сети (left, left-isp и т.д.)
В смотрим в таблицу в задании с ip адресами и запоминаем какому интерфейсу (**ens256**) дать ip.

Если нет соединений в nmtui, то надо добавить их командой

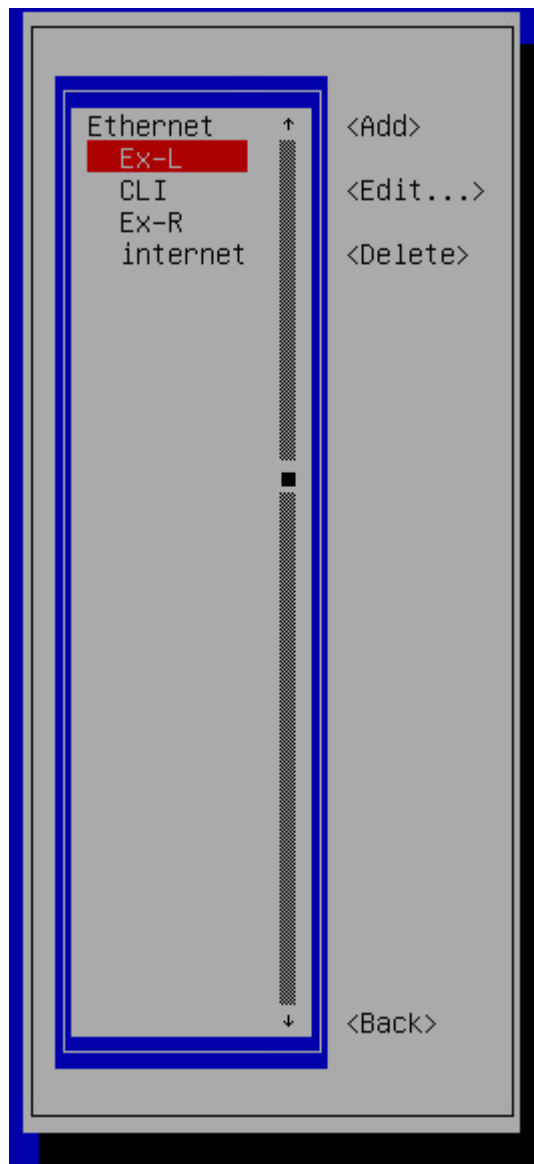
- nmcli connection add type Ethernet ifname ens000

Дальше настраиваем соединения

- nmtui



Выбираем соединение и настраиваем адресацию



WEB-L

Profile name L_____

Device ens192 (00:0C:29:23:87:D6)_____

ETHERNET

CONFIGURATION <Manual>

Addresses 192.168.200.100/24_____ <Remove>

<Add...>

Gateway 192.168.200.254_____

DNS servers 192.168.200.200_____ <Remove>

WEB-R

Profile name	R_____	
Device	ens192 (00:0C:29:32:DE:DB)_____	
ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	172.16.100.100/24_____	<Remove>
	<Add...>	
Gateway	172.16.100.254_____	
DNS servers	4.4.4.100_____	<Remove>
	<Add...>	

RTR-R

Добавить статический маршрут по умолчанию через 5.5.5.1 в nmtui (то, как это сделать показано в rtr-l)

Profile name	Ex-R_____	
Device	ens224 (00:0C:29:42:B0:3A)_____	
ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	5.5.5.100/24_____	<Remove>
	<Add...>	
Gateway	5.5.5.1_____	
DNS servers	4.4.4.100_____	<Remove>
	<Add...>	
Profile name	To-R_____	
Device	ens192 (00:0C:29:42:B0:30)_____	
ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	172.16.100.254/24_____	<Remove>
	<Add...>	
Gateway	_____	
DNS servers	<Add...>	

RTR-L

Добавить статический маршрут по умолчанию через 4.4.4.1 в nmtui

Edit Connection

Profile nameEx-L
Deviceens256 (00:0C:29:D4:EB:FF)

- ETHERNET

Show

IPv4 CONFIGURATIONManual

Hide

Addresses4.4.4.100/24RemoveAdd...
Gateway
DNS serversAdd...
Search domainsAdd...
Routing (No custom routes) Edit...
[] Never use this network for default route
[] Ignore automatically obtained routes
[] Ignore automatically obtained DNS parameters
[] Require IPv4 addressing for this connection

- IPv6 CONFIGURATIONAutomatic

Show

[X] Automatically connect
[X] Available to all users

CancelOK

Destination/Prefix	Next Hop	Metric
No custom routes are defined.		
Add...		
CancelOK		

Destination/Prefix	Next Hop	Metric
0.0.0.0/0	4.4.4.1	Remove
Add...		
CancelOK		

Profile name	To-L_____	
Device	ens192 (00:0C:29:0D:95:AE)_____	
ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	192.168.200.254/24_____	<Remove>
	<Add...>	
Gateway	_____	
DNS servers	<Add...>	

ISP

Profile name	Ex-L_____	
Device	ens256 (00:0C:29:D4:EB:FF)_____	
ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	4.4.4.1/24_____	<Remove>
	<Add...>	
Gateway	_____	
DNS servers	<Add...>	

Profile name	CLI_____	
Device	ens224 (00:0C:29:D4:EB:F5)_____	
ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	3.3.3.1/24_____	<Remove>
	<Add...>	
Gateway	_____	
DNS servers	3.3.3.1_____	<Remove>
Profile name	Ex-R_____	
Device	ens161 (00:0C:29:D4:EB:09)_____	

ETHERNET		
IPv4 CONFIGURATION	<Manual>	
Addresses	5.5.5.1/24_____	<Remove>
	<Add...>	
Gateway	_____	
DNS servers	<Add...>	

SRV

ДНС должен прописаться сам, когда поднимется днс, но лучше самому добавить 192.168.200.200

☒ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Firewalld

RTR-L

- apt install firewalld
- firewall-cmd --get-active-zones - **просмотр зон**

удаляем из зоны public все интерфейсы

- firewall-cmd --zone=public --remove-interface=ens**123**
- firewall-cmd --list-all-zones | less

добавляем в зоны trusted и external все интерфейсы

- firewall-cmd --zone=trusted --add-interface=ens**123** **внутр.**
- firewall-cmd --zone=external --add-interface=ens**123** **внеш.**
- firewall-cmd --zone=external --list-all - **просмотр правил**
- firewall-cmd --zone=external --add-service=**http**
- firewall-cmd --zone=external --add-service=**https**
- firewall-cmd --zone=external --add-service=**dns**
- firewall-cmd --zone=external --add-service=**ssh**
- firewall-cmd --zone=external --add-forward-port=port=**2244**:proto=**tcp**:toport=**22**:toaddr=192.168.200.100
- firewall-cmd --zone=external --add-forward-port=port=**80**:proto=**tcp**:toport=**80**:toaddr=192.168.200.100
- firewall-cmd --zone=external --add-forward-port=port=**53**:proto=**udp**:toport=**53**:toaddr=192.168.200.**200**
- firewall-cmd --zone=external --add-port=12345/udp
- firewall-cmf --runtime-to-permanent **сохранение правил**
- firewall-cmd --reload

```

root@rtr-1:~# firewall-cmd --zone=external --list-all
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens224
  sources:
  services: dns http https ssh
  ports: 12345/udp
  protocols:
  forward: no
  masquerade: yes
  forward-ports:
    port=2244:proto=tcp:toport=22:toaddr=192.168.200.100
    port=80:proto=tcp:toport=80:toaddr=192.168.200.100
    port=53:proto=udp:toport=53:toaddr=192.168.200.200
  source-ports:
  icmp-blocks:
  rich rules:

```

RTR-R

- `firewall-cmd --get-active-zones` - **просмотр зон**
- `firewall-cmd --zone=public --remove-interface=ens123`
- `firewall-cmd --list-all-zones | less`
- `firewall-cmd --zone=trusted --add-interface=ens123` **внутр.**
- `firewall-cmd --zone=external --add-interface=ens123` **внеш.**
- `firewall-cmd --zone=external --list-all` - **просмотр правил**
- `firewall-cmd --zone=external --add-service=http`
- `firewall-cmd --zone=external --add-service=https`
- `firewall-cmd --zone=external --add-service=dns`
- `firewall-cmd --zone=external --add-service=ssh`
- `firewall-cmd --zone=external --add-forward-port=port=2222:proto=tcp:toport=22:toaddr=172.16.100.100`
- `firewall-cmd --zone=external --add-forward-port=port=80:proto=tcp:toport=80:toaddr=172.16.100.100`
- `firewall-cmd --zone=external --add-port=12345/udp`
- `firewall-cmd --runtime-to-permanent` **сохранение правил**
- `firewall-cmd --reload`

```

root@rtr-r:~# firewall-cmd --zone=external --list-all
external (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens224
  sources:
  services: http https ssh
  ports: 12345/udp
  protocols:
  forward: no
  masquerade: yes
  forward-ports:
    port=2222:proto=tcp:toport=22:toaddr=172.16.100.100
    port=80:proto=tcp:toport=80:toaddr=172.16.100.100
  source-ports:
  icmp-blocks:
  rich rules:

```

Wireguard

RTR-L

- apt install wireguard wireguard-tools
- mkdir /etc/wireguard/keys
- cd /etc/wireguard/keys
- wg genkey | tee srv-sec.key | wg pubkey > srv-pub.key
- wg genkey | tee cli-sec.key | wg pubkey > cli-pub.key
- cat srv-sec.key cli-pub.key >> /etc/wireguard/wg0.conf
- nano /etc/wireguard/wg0.conf

```
RTR-L-deb
GNU nano 5.4 /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.1/30
ListenPort = 12345
PrivateKey = +EEL3UAMnhRzfQ0vUbvHkqSwNzPs0FJxB+Er/90MGkw=

[Peer]
PublicKey = PuRnALqs88Zpz0vBKDBWU12xwoDxX1eFtjUwjf91tEk=
AllowedIPs = 10.0.0.0/30, 172.16.100.0/24
```

- cat srv-sec.key
- cat cli-pub.key
- cat /etc/wireguard/wg0.conf **проверка ключей**
- systemctl enable --now wg-quick@wg0
- systemctl status wg-quick@wg0
- wg show all

сначала создаем директорию на RTR-R

- scp cli-sec.key srv-pub.key 5.5.100:/etc/wireguard/keys **передача ключей**

RTR-R

- apt install wireguard wireguard-tools
- mkdir /etc/wireguard/keys **создание директории**

после передачи ключей

- cat cli-sec.key srv-pub.key >> /etc/wireguard/wg0.conf

```
RTR-R-deb
GNU nano 5.4 /etc/wireguard/wg0.conf
[Interface]
Address = 10.0.0.2/30
PrivateKey = wDWbdjSuEFdxeF3FxpjNVcG6A63mTBGm1Ga1tu+okk=

[Peer]
PublicKey = cg4iJxuI1fi/0Zb2CM4gzR0r6oMBJI8/gnrwTF2j41w=
Endpoint = 4.4.4.100:12345
AllowedIPs = 10.0.0.0/30, 192.168.200.0/24
PersistentKeepalive = 10
```

- cat cli-sec.key
- cat srv-pub.key
- cat /etc/wireguard/wg0.conf **проверка ключей**
- systemctl enable --now wg-quick@wg0
- systemctl status wg-quick@wg0
- wg show all
- ip a

- ip r
должны появиться маршруты в подсети Left и Right

```
root@rtr-1:~# ip r
default via 4.4.4.1 dev ens224 proto static metric 101
4.4.4.0/24 dev ens224 proto kernel scope link src 4.4.4.100 metric 101
10.0.0.0/30 dev wg0 proto kernel scope link src 10.0.0.1
172.16.100.0/24 dev wg0 scope link
192.168.200.0/24 dev ens192 proto kernel scope link src 192.168.200.254 metric 100
root@rtr-1:~# _
```

DNS

ISP

- apt install bind9 bind9utils dnsutils
- systemctl status named
- nano /etc/bind/named.conf.options

```
//=====
listen-on { any; };
recursion no;
allow-query { any; };
dnssec-validation no;

listen-on-v6 { no; };
•
```

- nano /etc/binf/named.conf.local

```
zone "demo.wsr" {
    type master;
    allow-transfer { 4.4.4.100; };
    file "/opt/dns/demo.wsr.zone";
};

zone "3.3.3.in-addr.arpa" {
    type master;
    file "/opt/dns/reverse.demo.wsr.zone";
};
•
```

- mkdir /opt/dns
- cp /etc/bind/db.local /opt/dns/demo.wsr.zone
- chmod 665 /opt/dns/demo.wsr.zone
- nano /etc/apparmor.d/usr.sbin.named

```
# See /usr/share/doc/bind9
/etc/bind/* r,
/var/lib/bind/* rw,
/var/lib/bind/ rw,
/var/cache/bind/* lrw,
/var/cache/bind/ rw,
/opt/dns/* rw, _
•
```

- service apparmor restart

Зона	Тип записи	Ключ	Значение
demo.wsr	A	ISP	3.3.3.1
	A	www	4.4.4.100
	A	www	5.5.5.100
	CNAME	internet	ISP
int.demo.wsr	A	web-1	192.168.200.100
	A	WEB-R	172.16.100.100
	A	SRV	192.168.200.200

	A	rtr-l	192.168.200.254
	A	rtr-r	172.16.100.254
	CNAME	webapp-L	web-l
	CNAME	webapp-R	WEB-R
	CNAME	ntp	SRV
	CNAME	dns	SRV

-
- nano /opt/dns/demo.wsr.zone

```
ISP
GNU nano 5.4 /opt/dns/demo.wsr.zone
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA demo.wsr. root.demo.wsr. (
        2      ; Serial
        604800 ; Refresh
        86400  ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS demo.wsr.
@ IN A 3.3.3.1
isp IN A 3.3.3.1
www IN A 4.4.4.100
www IN A 5.5.5.100
internet CNAME isp
```

-
- named-checkconf -z **проверка**

SRV-Win

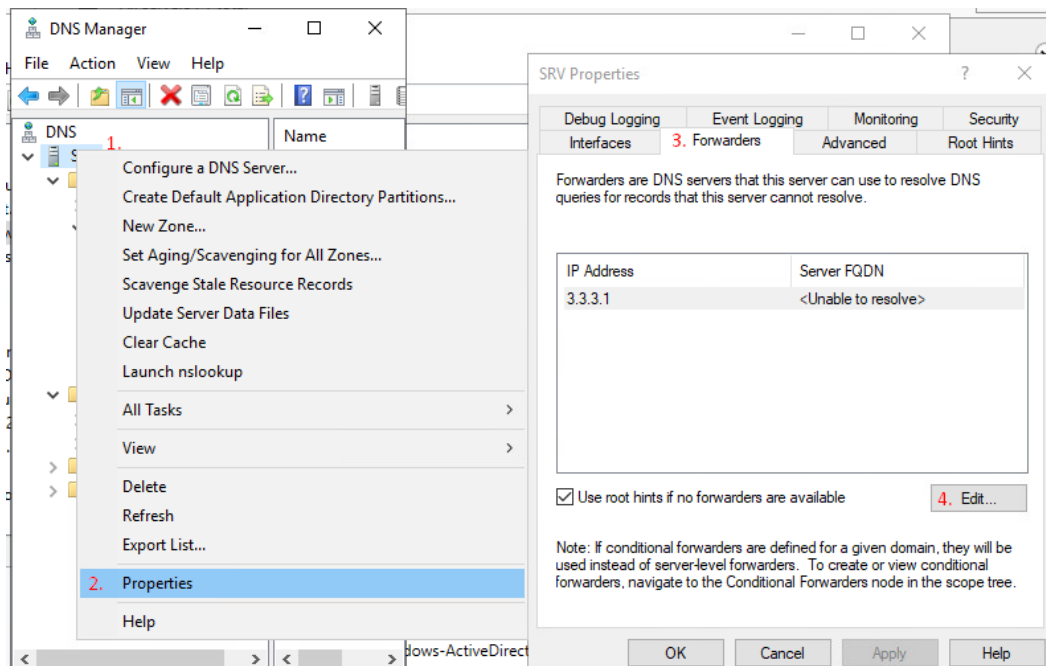
Server Manager > Tools > DNS

Добавить обратные зоны и DNS записи

	Name	Type	Data	Timestamp
DNS				
SRV				
Forward Lookup Zones				
_msdcs.int.demo.wsr				
int.demo.wsr				
_msdcs				
_sites				
_tcp				
_udp				
DomainDnsZones				
ForestDnsZones				
Reverse Lookup Zones				
200.168.192.in-addr.arpa				
100.16.172.in-addr.arpa				
Trust Points				
Conditional Forwarders				
	_msdcs			
	_sites			
	_tcp			
	_udp			
	DomainDnsZones			
	ForestDnsZones			
	(same as parent folder)	Start of Authority (SOA)	[18], srv.int.demo.wsr, ho...	static
	(same as parent folder)	Name Server (NS)	srv.int.demo.wsr.	static
	(same as parent folder)	Host (A)	192.168.200.200	6/5/2023 1:00:00 AM
	srv	Host (A)	192.168.200.200	static
	web-l	Host (A)	192.168.200.100	
	web-r	Host (A)	172.16.100.100	
	rtr-r	Host (A)	172.16.100.254	
	rtr-l	Host (A)	192.168.200.254	
	ntp	Alias (CNAME)	srv.int.demo.wsr	
	dns	Alias (CNAME)	srv.int.demo.wsr	

Добавление форвардера зон

Удалить все старые, добавить 3.3.3.1



NTP (Chrony)

ISP

- apt install chrony
- nano /etc/chrony/chrony.conf
- оставить следующие строки

```
# Include configuration files found in /etc/chrony/conf.d.
confdir /etc/chrony/conf.d

# Use Debian vendor zone.
#pool 2.debian.pool.ntp.org iburst

# Use time sources from DHCP.
#sourcedir /run/chrony-dhcp

# Use NTP sources found in /etc/chrony/sources.d.
#sourcedir /etc/chrony/sources.d

# This directive specify the location of the file containing ID/key pairs for
# NTP authentication.
#keyfile /etc/chrony/chrony.keys

# This directive specify the file into which chronyd will store the rate
# information.
driftfile /var/lib/chrony/chrony.drift

# Save NTS keys and cookies.
#ntsdumpdir /var/lib/chrony

# Uncomment the following line to turn logging on.
log tracking measurements statistics

# Log files location.
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
```

- добавляем

```
confdir /etc/chrony/conf.d
allow 3.3.3.0/24
allow 4.4.4.0/24
local stratum 3_
```

-
- Комментируем

```
#leapsectz right/UTC #maxupdateskew 100.0
```

-
- Меняем 1 на 10 и 3 на 30
- Получится

```
makestep 10 30
```

```
GNU nano 5.4 /etc/chrony/chrony.conf *
# Welcome to the chrony configuration file. See chrony.conf(5) for more
# information about usable directives.

# Include configuration files found in /etc/chrony/conf.d.
confdir /etc/chrony/conf.d
allow 3.3.3.0/24
allow 4.4.4.0/24
local stratum 3

# Use Debian vendor zone.
#pool 2.debian.pool.ntp.org iburst

# Use time sources from DHCP.
#sourcedir /run/chrony-dhcp

# Use NTP sources found in /etc/chrony/sources.d.
#sourcedir /etc/chrony/sources.d

# This directive specify the location of the file containing ID/key pairs for
# NTP authentication.
#keyfile /etc/chrony/chrony.keys

# This directive specify the file into which chronyd will store the rate
# information.
driftfile /var/lib/chrony/chrony.drift

# Save NTS keys and cookies.
#ntsdumpdir /var/lib/chrony

# Uncomment the following line to turn logging on.
log tracking measurements statistics

# Log files location.
[ Cancelled ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```



```

GNU nano 5.4 /etc/chrony/chrony.conf *
# Log files location.
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
#maxupdateskew 100.0

# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtcfile' directive.
rtcsync

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 10 30

# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smeared time.
#leapsectz right/UTC

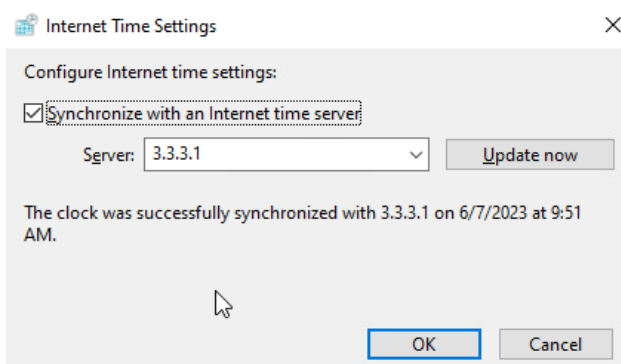
```

- systemctl restart chrony
- systemctl status chrony
- timedatectl set-timezone Asia/Novosibirsk
- date
- chronyc tracking
- chronyc clients **проверка клиентов**

CLI

Control Panel > Clock and Region > Set the time and date > Internet Time > Change Settings

Ввести 3.3.3.1

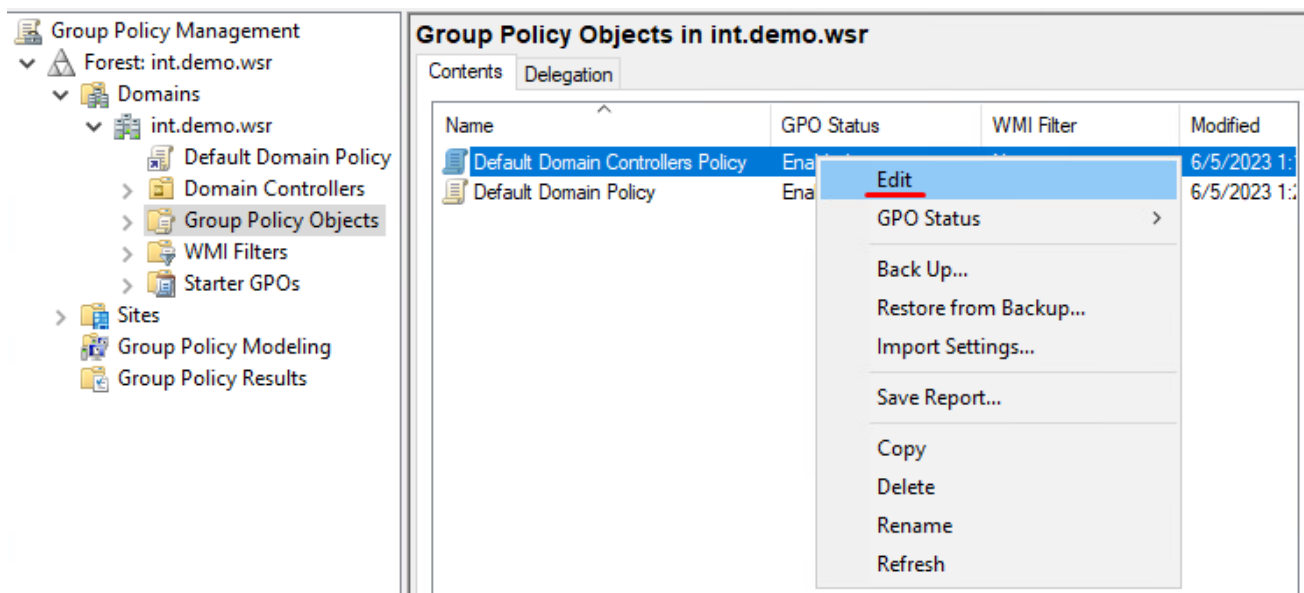


Проверяем клиентов на ISP

SRV

Отключить службу W32Time (служба времени windows time)

Server Manager > Tools > Group Policy Manager



Далее Computer Configuration > Policies > System > Windows Time Service > Time Providers
Включаем три политики, у первой прописываем NtpServer и выбираем протокол

Setting	State
Configure Windows NTP Client	Enabled
Enable Windows NTP Client	Enabled
Enable Windows NTP Server	Enabled

Configure Windows NTP Client

Previous Setting Next Setting

☐ Not Configured Comment:
☒ **Enabled**
☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

NtpServer 3.3.3.1|0x8

Type NTP

CrossSiteSyncFlags 2

ResolvePeerBackoffMinutes 15

ResolvePeerBackoffMaxTimes 7

SpecialPollInterval 1024

EventLogFlags 0

Help:

This policy setting specifies a set of parameters for controlling the Windows NTP Client.

If you enable this policy setting, you can specify the following parameters for the Windows NTP Client.

If you disable or do not configure this policy setting, the Windows NTP Client uses the defaults of each of the following parameters.

NtpServer
The Domain Name System (DNS) name or IP address of an NTP time source. This value is in the form of ""dnsName,flags"" where ""flags"" is a hexadecimal bitmask of the flags for that host. For more information, see the NTP Client Group Policy Settings Associated with Windows Time section of the Windows Time Service Group Policy Settings. The default value is ""time.windows.com,0x09"".

Type
This value controls the authentication that W32time uses. The

OK Cancel Apply

Вернуться в предыдущее окно, выбрать Enforced

Group Policy Management

Forest: int.demo.wsr

Domains

int.demo.wsr

Default Domain Policy

Domain Controllers

Group Policy Objects

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Domain Controllers

Linked Group Policy Objects Group Policy Inheritance Delegation

Link ...	GPO	Enforced	Link Enabled	GPO :
1	Default Domain Controllers Policy	Yes	Yes	Enabl

Edit

✓ Enforced

✓ Link Enabled

Save Report...

Delete

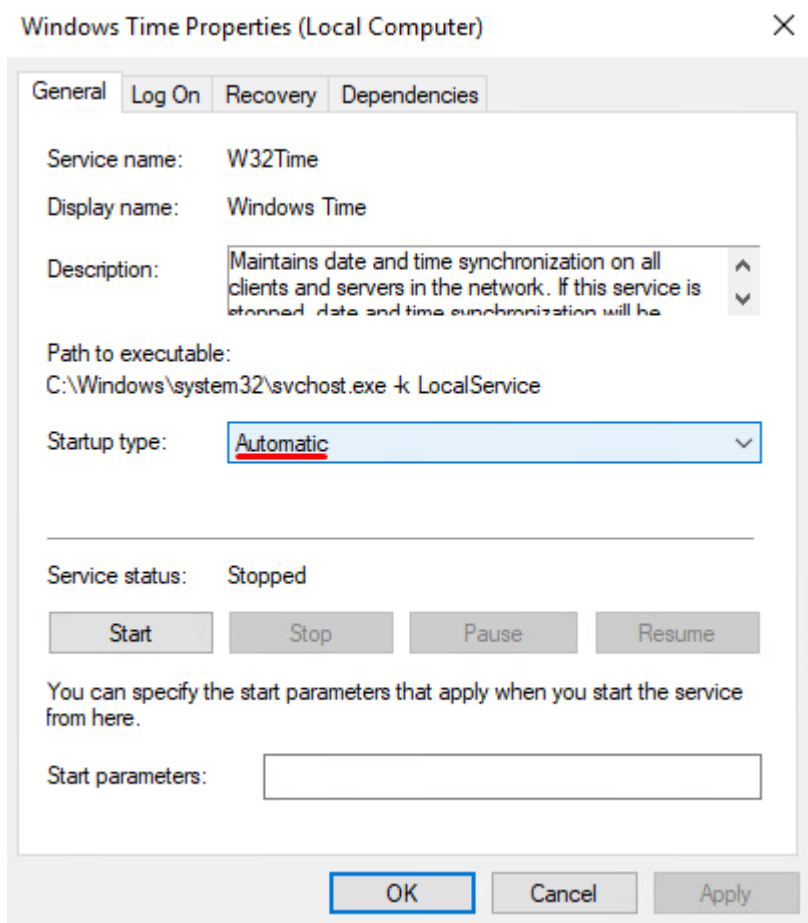
Rename

Refresh

В cmd

- gpupdate /force

Проверить, запущена ли автоматически служба W32Time (Windows Time) и включить ее



После этого можно проверить клиентов на ISP

```
root@isp:~# chronyc clients
Hostname                                NTP    Drop Int IntL Last      Cmd    Drop Int  Last
=====
4.4.4.100                              15     0   7   -   78       0     0   -   -
3.3.3.10                                1     0   -   -  401       0     0   -   -
root@isp:~# _
```

WEB-L, WEB-R, RTR-L, RTR-R

- apt install chrony
- nano /etc/chrony/chrony.conf
- Добавить строчку
 - server srv.int.demo.wsr prefer iburst
- Закомментировать лишние, раскомментировать, поменять 1 на 10, 3 на 30
- Останется только:
 - server srv.int.demo.wsr prefer iburst
 - driftfile
 - log tracking
 - logdir
 - rtcsync
 - makestep 10 30

```

GNU nano 5.4 /etc/chrony/chrony.conf
# Welcome to the chrony configuration file. See chrony.conf(5) for more
# information about usable directives.

# Include configuration files found in /etc/chrony/conf.d.
#confdir /etc/chrony/conf.d

# Use Debian vendor zone.
#pool 2.debian.pool.ntp.org iburst
server srv.int.demo.wsr prefer iburst_

# Use time sources from DHCP.
#sourcedir /run/chrony-dhcp

# Use NTP sources found in /etc/chrony/sources.d.
#sourcedir /etc/chrony/sources.d

# This directive specify the location of the file containing ID/key pairs for
# NTP authentication.
#keyfile /etc/chrony/chrony.keys

# This directive specify the file into which chronyd will store the rate
# information.
driftfile /var/lib/chrony/chrony.drift

# Save NTS keys and cookies.
#ntsdumpdir /var/lib/chrony

# Uncomment the following line to turn logging on.
log tracking measurements statistics

# Log files location.
logdir /var/log/chrony

```

[Wrote 48 lines]

```

GNU nano 5.4 /etc/chrony/chrony.conf
logdir /var/log/chrony

# Stop bad estimates upsetting machine clock.
#maxupdateskew 100.0

# This directive enables kernel synchronisation (every 11 minutes) of the
# real-time clock. Note that it can't be used along with the 'rtcfile' directive.
rtcsync

# Step the system clock instead of slewing it if the adjustment is larger than
# one second, but only in the first three clock updates.
makestep 10 30

# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smeared time.
#leapsectz right/UTC

```

-
- systemctl restart chrony
- systemctl status chrony
- chronyc sources (если *, то время синхронизировалось, если ! – то ошибка)

```

root@web-r:~# chronyc sources
MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
^* SRV.int.demo.wsr         4    6    77    58    -218us[ +858us] +/- 107ms
root@web-r:~#

```

-
- timedatectl set-timezone Asia/Novosibirsk
- date

CIFS

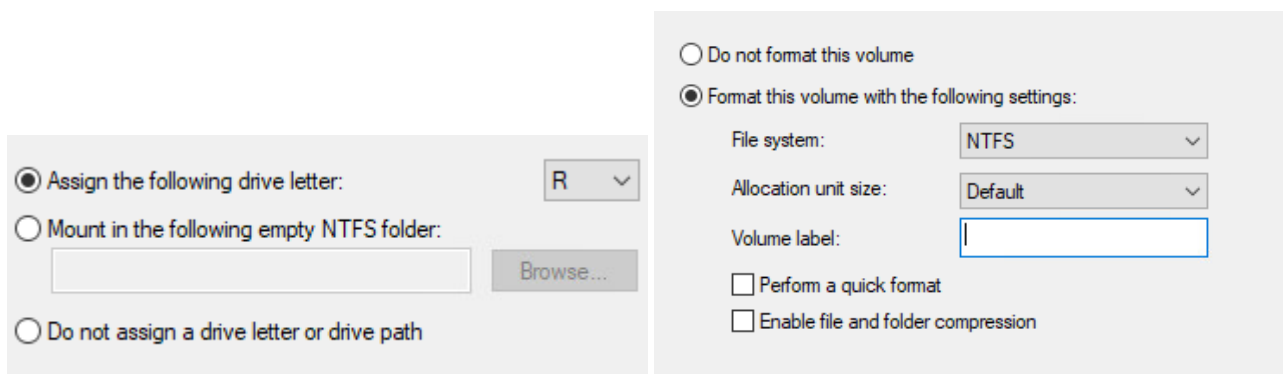
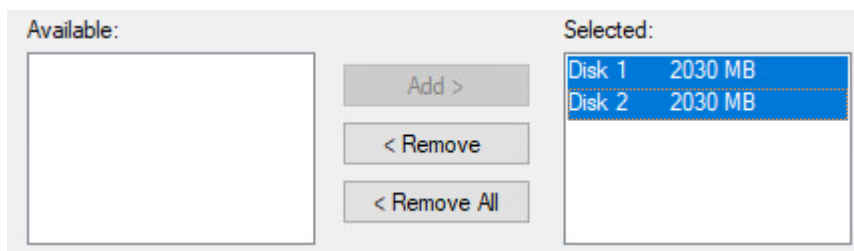
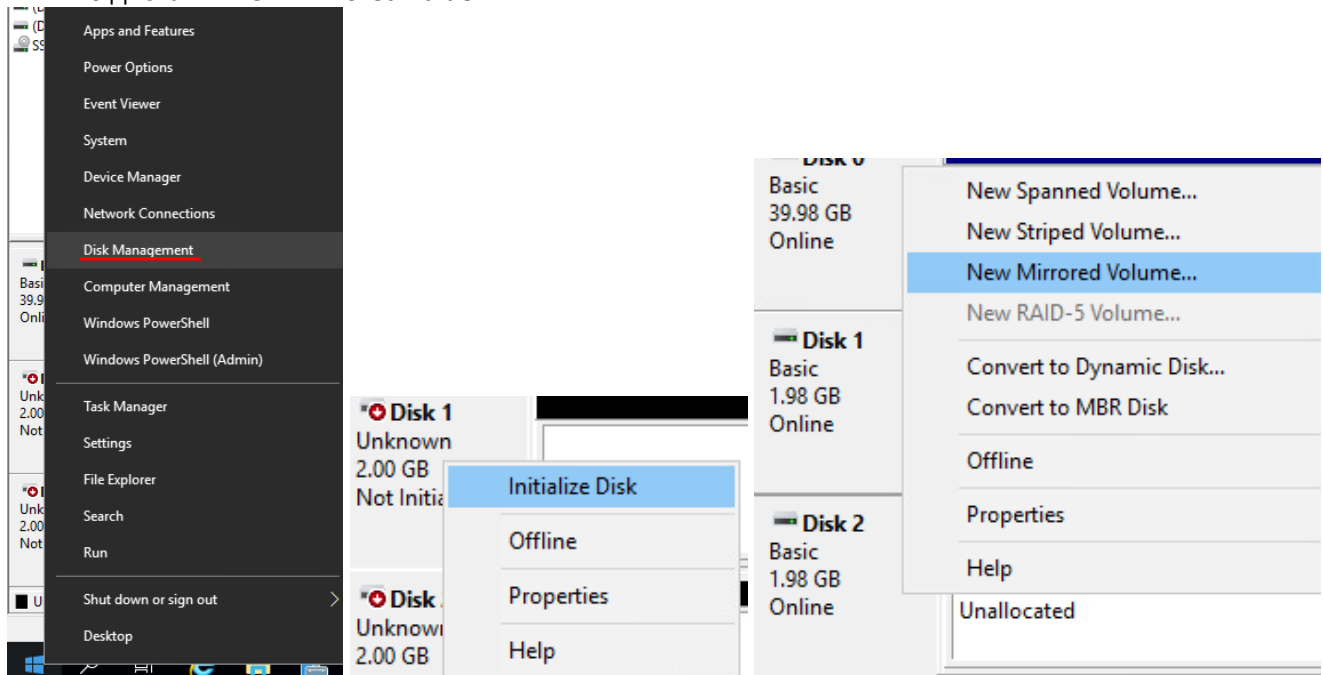
SRV

ПКМ по пуску > Disk management

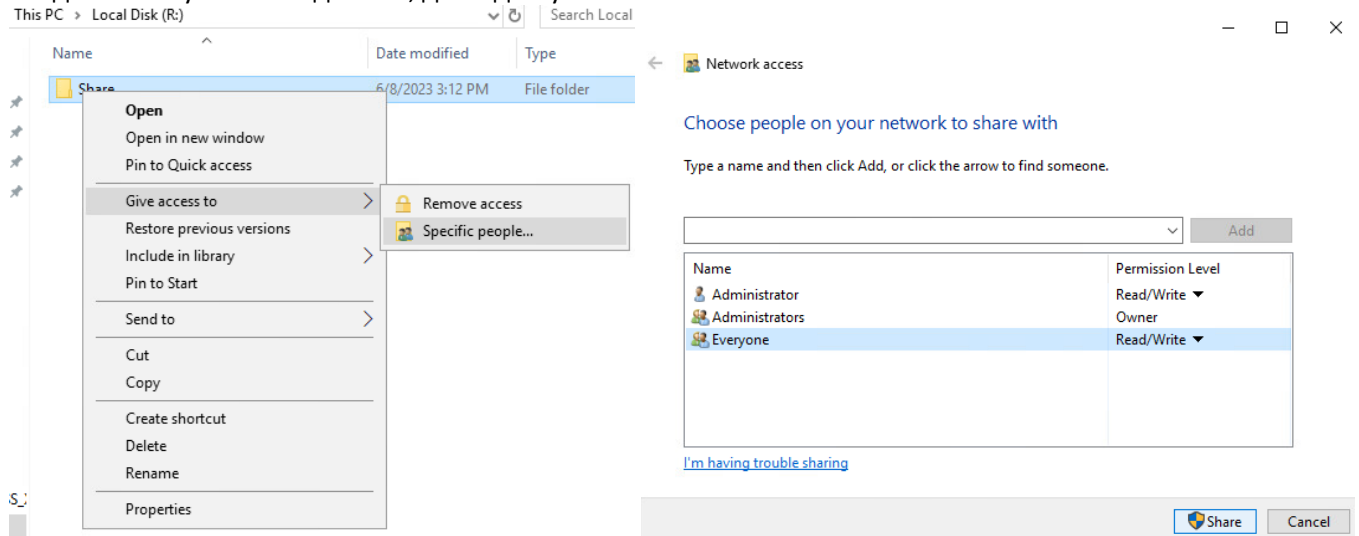
ПКМ по диску > Online

ПКМ по диску > Initialize Disk

ПКМ по диску > New Mirrored Volume



Создаем папку Share на диске R, даем доступ



WEB-L, WEB-R

- apt install cifs-utils
- mkdir /opt/share
- nano /etc/fstab

//srv.int.demo.wsr/share /opt/share cifs rw,username=Administrator,password=P@ssw0rd 0 0

```
GNU nano 5.4 /etc/fstab *
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=f8a4345b-febb-45a2-a32c-9b4b4a091600 / ext4 errors=remount-ro 0 1
# swap was on /dev/sda5 during installation
UUID=a66bf307-90a3-4682-85e0-55ca2864a8ba none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
//srv.int.demo.wsr/share /opt/share cifs rw,username=Administrator,password=P@ssw0rd 0 0
```

- mount -a
- touch /opt/share/test.txt **создать файл для проверки**

Docker

WEB-L, WEB-R

- apt install nginx lynx
- добавить .iso образ докера в виртуальную машину
- mkdir /opt/docker
- mount /dev/cdrom /mnt
- cp /mnt/* /opt/docker/
- cd /opt/docker
- tar -xvf appdockerdemo.tar.gz
- umount /mnt
- dpkg -i containerd*

- `dpkg -i docker-*`
- `docker info`
- `docker version`
- `docker image load -i appdocker0.zip`
- `docker image ls`
- `docker run -d --restart unless-stopped appdocker0` **Добавляет контейнер в автозапуск, если машины перезагрузилась**
- `docker ps` **просмотр имени контейнера**
- `docker container inspect %имя%` **узнать ip и порт контейнера**
-

```

"LinkLocalIPv6PrefixLen": 0,
"Ports": {
  "5000/tcp": null
},
"SandboxKey": "/var/run/docker/netns/3401a675a3ee",
"SecondaryIPAddresses": null,
"SecondaryIPv6Addresses": null,
"EndpointID": "ef09c764509a337032066a740c09cb4439ca815ae38d",
"Gateway": "172.17.0.1",
"GlobalIPv6Address": "",
"GlobalIPv6PrefixLen": 0,
"IPAddress": "172.17.0.2",
"IPPrefixLen": 16,
"IPv6Gateway": "",
"MacAddress": "02:42:ac:11:00:02",
"Networks": {
  "bridge": {
    "IPAMConfig": null,
    "Links": null,
    "Aliases": null,
    "NetworkID": "1cf8ba5fbb44746aff8b7ddb58b169161e7d3",
    "EndpointID": "ef09c764509a337032066a740c09cb4439ca8",
    "Gateway": "172.17.0.1",
    "IPAddress": "172.17.0.2",
    "IPPrefixLen": 16,
    "IPv6Gateway": "",
    "GlobalIPv6Address": "",
    "GlobalIPv6PrefixLen": 0,
    "MacAddress": "02:42:ac:11:00:02",
    "DriverOpts": null
  }
}
}
}
}
root@web-l:/opt/docker# _

```

- `lynx http://[адрес контейнера]:[порт]` **проверка работы docker**

Настройка веб-сервера nginx

- `mv /etc/nginx/sites-enabled/default /etc/nginx/sites-enabled/[имя файла, можно webapp].conf`
- `nano /etc/nginx/sites-enabled/[имя файла, можно webapp].conf`
- Комментируем следующие строки:
 - `listen [::]:80 default_server`

- ```
server {
 listen 80 default_server;

 server_name www.demo.wsr;

 location / {
 # First attempt to serve request as file, then
 # as directory, then fall back to displaying a 404.
 #try_files $uri $uri/ =404;
 proxy_pass http://172.17.0.2:5000;
 }
}
```

- 

МОЖНО И НЕ ЧИТАТЬ

////////////////////////////////////

- `docker image load -i appdocker0.zip.`

Веб-приложение использует порт 5000, доступ к нему происходит через `http://адрес_контейнера:5000`

\_\_\_\_\_  
СООТВЕТСТВЕННО.

- `docker run -d appdocket0:latest.`

Пример команды для запуска контейнера с внешней базой данных:

- `docker run -d appdocker0:latest`

### Список доступных вызовов:

- / или /index.html Возвращает web-страницу с приветствием пользователя

- /health Вызов, возвращающий код 200 и сообщение "Success!" в случае успеха проверки

работоспособности, 503 и сообщение "Database connection is broken!" в случае проблем с подключением к

- БД, а также 503 и "Cannot get home page." в случае проблем с загрузкой страницы "/"

- `/add?message=<Текст>` Команда, добавляющая текстовое сообщение в таблицу сообщений

СУБД, возвращает 'Inserted!' и 200 в случае успеха, "Missing argument!" и 400 в случае отсутствия аргумента

- message.

- `/get` Web-страница со всеми сохраненными сообщениями.

Конец.

////////////////////////////////////

## CA

WEB-L, WEB-R

1. `nano /etc/ssl/openssl.cnf` || Конфигурационный файл запроса сертификата
2. Находим `[req]` и добавляем
  - `req_extensions = v3_req` || имя и расширения файла запроса сертификата

3. Находим [req\_distinguished\_name] и меняем
  - countryName\_Default = RU || Страна запроса
4. Находим [v3\_req] и добавляем
  - subjectAltName = @alt\_names
5. Создаем свой блок доменных имен - [alt\_names]
  - DNS.1 = www.demo.wsr || DNS обращение будет к SRV
6. cd /opt/share || Сразу переходим в каталог сетевой папки, чтобы запрос создавался сразу там
7. openssl req -nodes -newkey rsa -out csr.req || Создаем запрос
  - Country Name: RU
  - Organization Name: DEMO.WSR
  - Common Name: www.demo.wsr
  - Все остальное пустое

```

root@web-1:/opt/share# openssl req -nodes -newkey rsa -out csr.req
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privkey.pem'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [RU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]: DEMO.WSR
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []: www.demo.wsr
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@web-1:/opt/share#
root@web-1:/opt/share#

```

## SRV DEBIAN

- Apt install network-manager chrony bind9 dnsutils bind9utils

## Раздача IP адресов

1. apt-cdrom add
  - apt-update
  - apt install network-manager
  - DNS внешний RTR-L
  - Шлюз внутренний RTR-R

## DNS bind9

1. Nano /etc/bind/named.conf.options  
forwarders { \*isp cli\* };  
...  
listen-on { any; };  
recursion yes;  
allow-query { any; };  
dnssec-validation no;  
listen-on-v6 { no; };  
allow-recursion { 10.0.0.0/30; \*сетка web-l\*/24; \*сетка web-r\*/24; };  
};
2. Nano /etc/bind/named.conf.local  
zone "int.demo.wsr" {  
type master;  
allow-transfer { any; };  
file "/opt/dns/int,demo.wsr.zone";  
};  
zone "200.168.192.in-addr.arpa" {  
type master;  
allow-transfer { any; };  
file "/opt/dns/backleft";  
};  
zone "100.16.172.in-addr.arpa" {  
type master;  
allow-transfer { any; };  
file "/opt/dns/backright";  
};
3. Mkdir /opt/dns  
cd /opt/dns  
cp /etc/bind/db.local /opt/dns/int.demo.wsr.zone  
chmod 665 /opt/dns/int.demo.wsr.zone
4. nano /etc/apparmor.d/usr.sbin.named  
добавить /opt/dns/\*\* rw  
service apparmor restart
- nano /opt/dns/int.demo.wsr.zone  
@ IN SOA int.demo.wsr. root.int.demo.wsr. (  
...  
@ IN NS srv.inr.demo.wsr.  
srv IN A \*srv\*  
web-l A \*web-l\*  
web-r A \*web-r\*  
rtr-l A \*rtr-l внутренний\*  
rtr-r A \*rtr-r внутренний\*  
ntp CNAME srv.int.demo.wsr  
dns CNAME srv.int.demo.wsr  
  
cp /etc/bind/db.local /opt/dns/backleft  
cp /etc/bind/db.local /opt/dns/backright  
  
nano /opt/dns/backleft  
  
@ IN SOA int.demo.wsr. root.int.demo.wsr. (  
...

```
@ IN NS srv.int.demo.wsr.
100 IN PTR web-l.int.demo.wsr.
200 IN PTR srv.int.demo.wsr.
254 IN PTR rtr-l.int.demo.wsr.
```

- 
- nano /opt/dns/backright

```
@ IN SOA int.demo.wsr. root.int.demo.wsr. (
...
```

- @ IN NS srv.int.demo.wsr.
- 100 IN PTR web-r.int.demo.wsr.
- 254 IN PTR rtr-r.int.demo.wsr.

```
named-checkconf -z
systemctl restart named
```

## Время Chrony

1. apt-cdrom add  
apt update  
apt install chrony
2. nano /etc/chrony/crony.conf  
закомментировать:
  1. pool  
sourcedir  
sourcedir  
keyfile  
ntsdump  
leapsectz
 раскомментировать
  2. log tracking  
makestep 10 30
3. Прописать  
server srv.int.demo.wsr prefer iburst  
local stratum 4  
allow 192.168.200.200/24  
allow 192.168.200.100/24  
allow 192.168.200.254/24  
allow 172.16.100.254/24  
allow 172.16.100.100/24  
allow 10.0.0.1/30  
allow 10.0.0.2/30
4. Systemctl restart chrony  
systemctl status chrony  
timedatectl set-timezone Asia/Novosibirsk  
chronyc sources  
может потребоваться ребут

## Share Samba

1. Apt-cdrom add  
apt update  
apt install mdadm samba
2. Fdisk -l  
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdb /dev/sdc  
Mkfs -t ext4 /dev/md0

```

mkdir /mnt/storage
fdisk -l
reboot
3. Nano /etc/fstab
/dev/md127 /mnt/storage ext4 defaults 0 0
mount /dev/md127 /mnt/storage
lsblk
chmod -R 777 /mnt/storage
ls -l /mnt/
4. Nano /etc/samba/smb.conf
[smb.demo.wsr]
comment = SMB server on SRV
path = /mnt/storage
guest ok = yes
browseable = yes
create mask = 0777
directory mask = 0777
writable = yes
read only = no
hosts allow = 192.168.200.200 172.16.100.100 10.0.0.1 10.0.0.2

systemctl restart smbd

```

## Web-I | web-r

```

echo username=root >> /root/.smbclient
echo password=toor >> /root/.smbclient

1. /etc/fstab
//192.168.200.200/smb.demo.wsr /opt/share cifs
user,rw,_netdev,file_mode=0777,dir_mode=0777,credentials=/root/.smbclient 0 0
2. Mkdir /opt/share
mount -a
3. Если не робит
umount /opt/share
mount -a

```