DEMO2022 https://github.com/storm39mad/DEMO2022

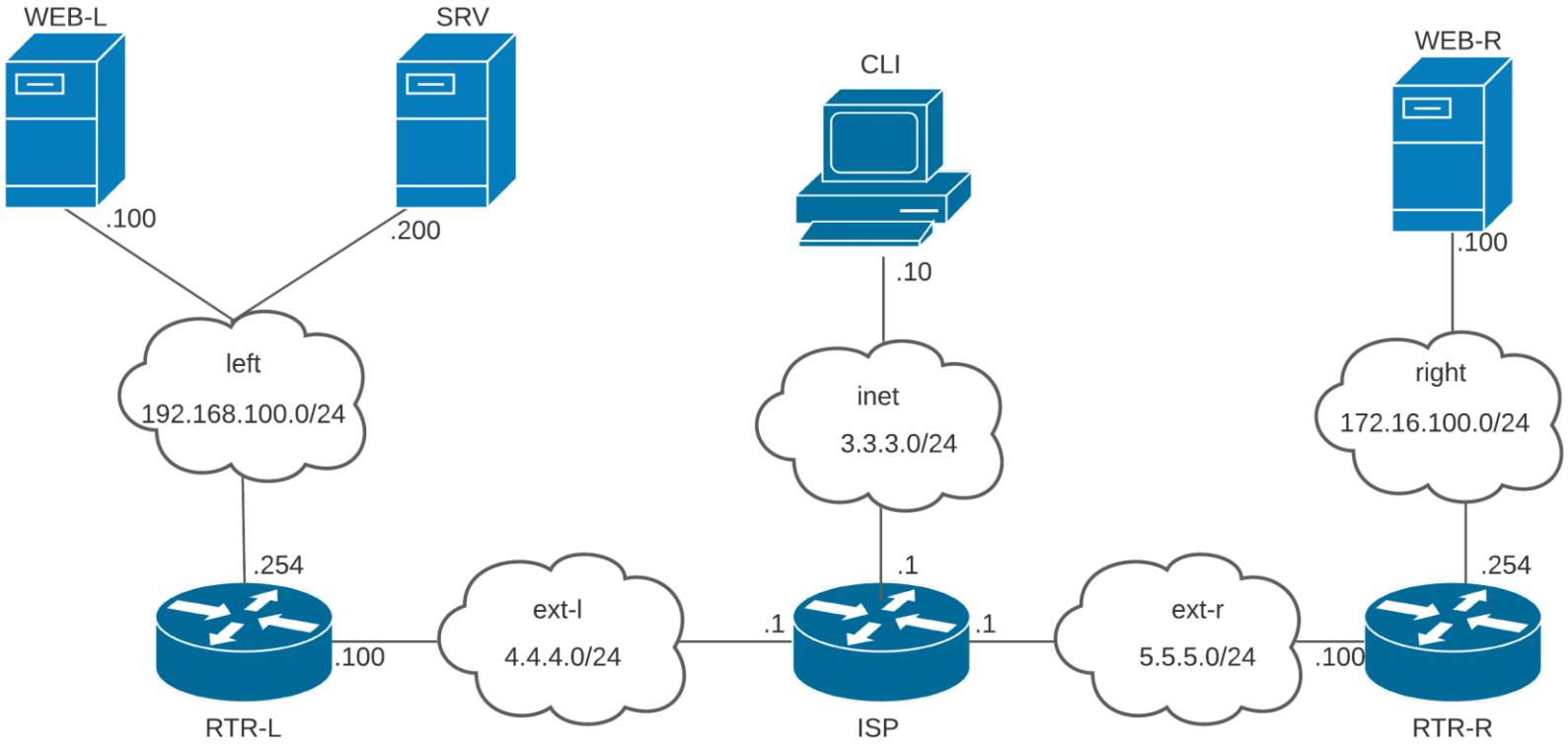
Образец задания

Образец задания для демонстрационного экзамена по комплекту оценочной документации.

Описание задания

Модуль 1

Вариант 1-0 (публичный)



Виртуальные машины и коммутация.

Необходимо выполнить создание и базовую конфигурацию виртуальных машин.

1. На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.
    - Характеристики ВМ установите в соответствии с Таблицей 1;
    - Коммутацию (если таковая не выполнена) выполните в соответствии со схемой сети.
2. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.
3. Адресация должна быть выполнена в соответствии с Таблицей 1;
4. Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с Таблицей 1;

Таблица 1. Характеристики ВМ

Name VM	OC	RAM	CPU	IP	Additionally
RTR-L	Debian 11/CSR	2 GB	2/4	4.4.4.100/24	
				192.168.100.254/24	
RTR-R	Debian 11/CSR	2 GB	2/4	5.5.5.100/24	
				172.16.100.254 /24	
SRV	Debian 11/Win 2019	2 GB /4 GB	2/4	192.168.100.200/24	Доп диски 2 шт по 5 GB
WEB-L	Debian 11	2 GB	2	192.168.100.100/24	
WEB-R	Debian 11	2 GB	2	172.16.100.100/24	
ISP	Debian 11	2 GB	2	4.4.4.1/24	
				5.5.5.1/24	
				3.3.3.1/24	
CLI	Win 10	4 GB	4	3.3.3.10/24	

1. На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.

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

RTR-L

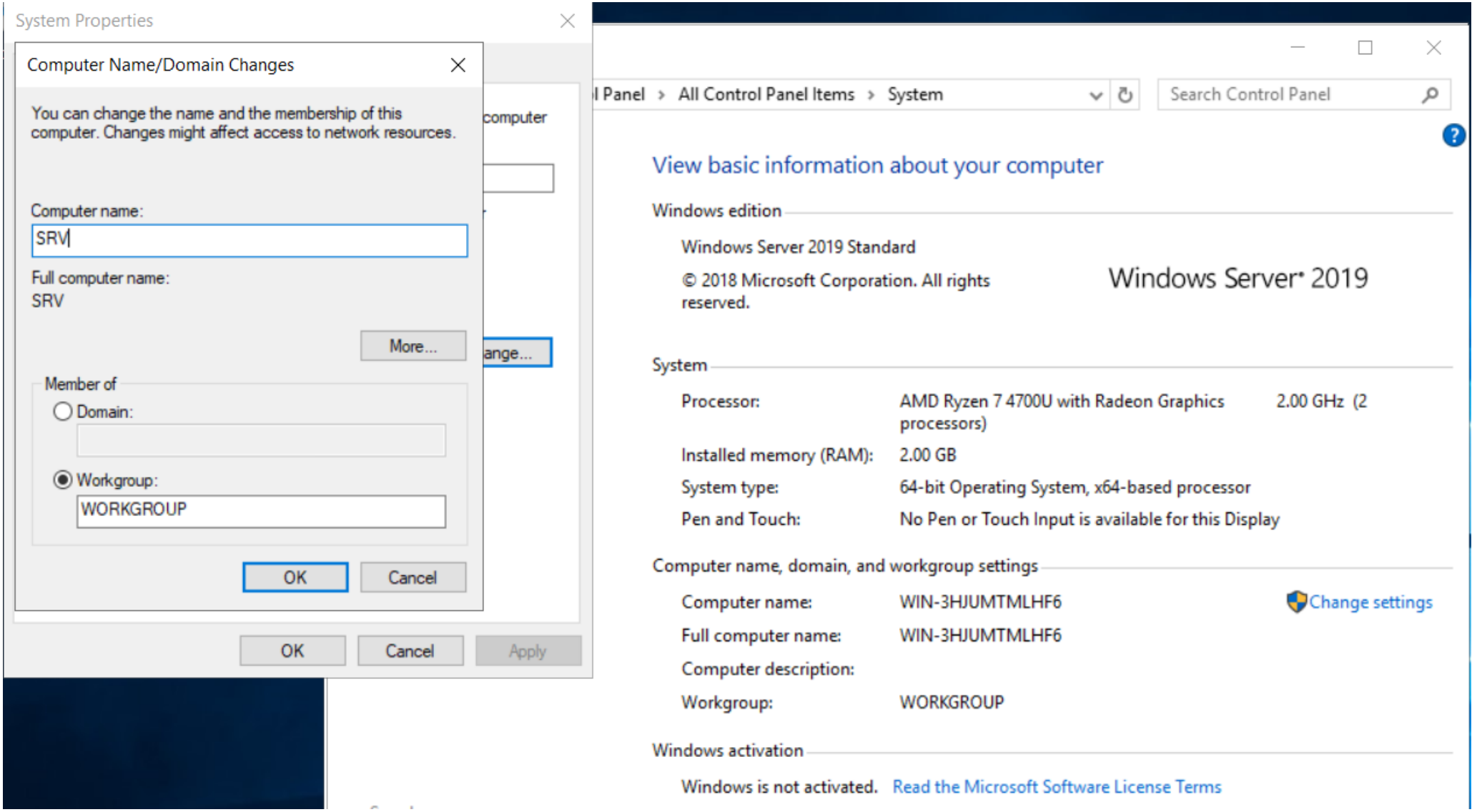
en
conf t
hostname RTR-L
do wr

RTR-R

en
conf t
hostname RTR-R
do wr

SRV

Открыть проводник. Правой клавишей на “This PC” => Properties => Advanced system setting => Computer Name => Change



Или команда в PowerShell:

Rename-Computer -NewName SRV

Перезагрузка ПК

WEB-L

hostnamectl set-hostname WEB-L
reboot

WEB-R

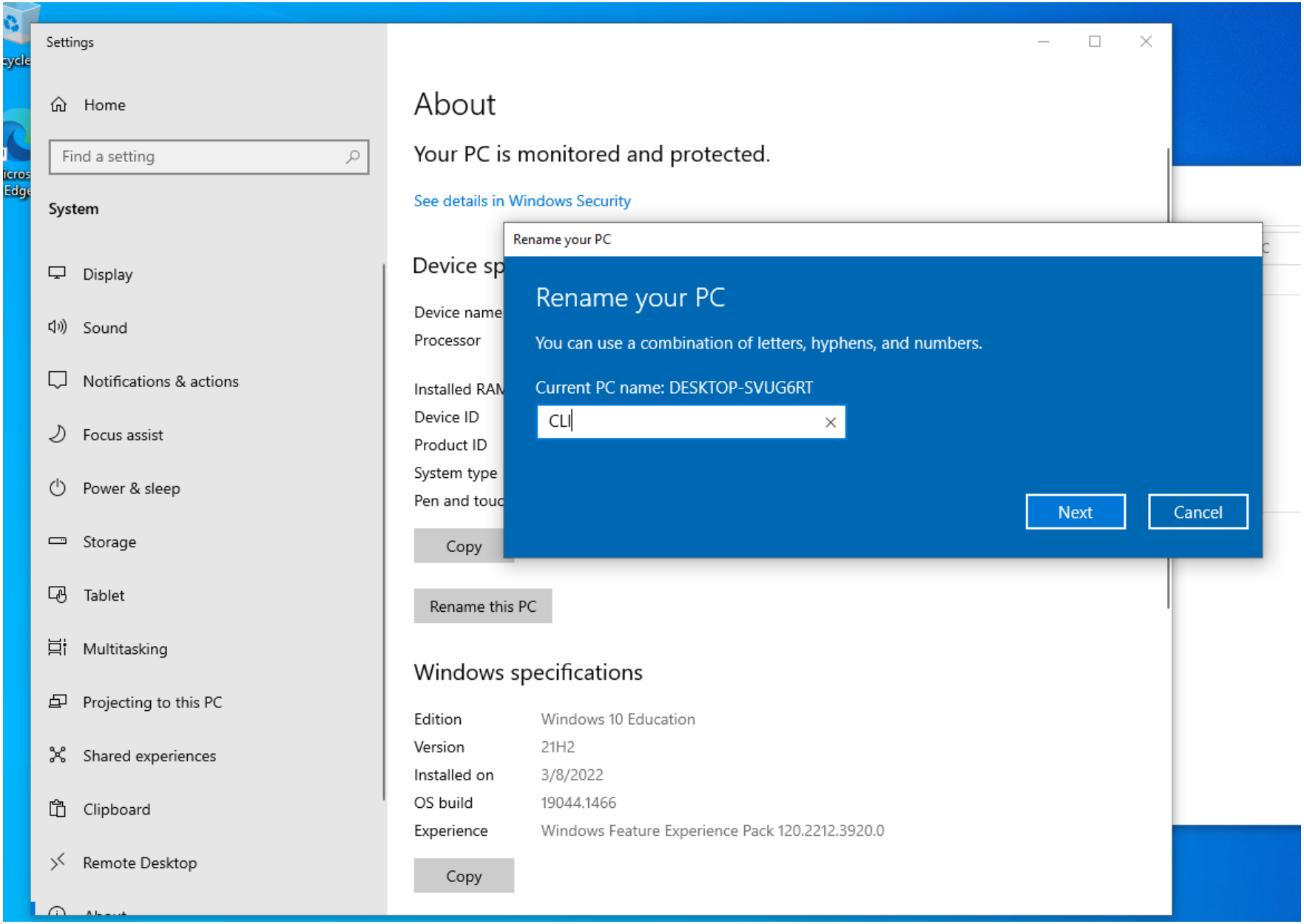
hostnamectl set-hostname WEB-R
reboot

ISP

hostnamectl set-hostname ISP
reboot

CLI

Открыть проводник. Правой клавишей на “This PC” => Properties => Advanced system setting => Rename this PS


Settings
Home
Find a setting
System
Display
Sound
Notifications & actions
Focus assist
Power & sleep
Storage
Tablet
Multitasking
Projecting to this PC
Shared experiences
Clipboard
Remote Desktop
About
About
Your PC is monitored and protected.
See details in Windows Security
Device sp
Device name
Processor
Installed RAM
Device ID
Product ID
System type
Pen and touc
Copy
Rename this PC
Windows specifications
Edition Windows 10 Education
Version 21H2
Installed on 3/8/2022
OS build 19044.1466
Experience Windows Feature Experience Pack 120.2212.3920.0
Copy
Rename your PC
Rename your PC
You can use a combination of letters, hyphens, and numbers.
Current PC name: DESKTOP-SVUG6RT
CLI
Next
Cancel

Или команда в PowerShell:

Rename-Computer -NewName CLI

Перезагрузка ПК

3. Адресация должна быть выполнена в соответствии с Таблицей 1;

RTR-L

С помощью команды sh intr смотрим какие MAC адреса на каком интерфейсе. Через настройки виртуальной машины проверяем в каком направлении они работают. После чего настраиваем IP адреса.

```
en
conf t
int gi 1
ip address 4.4.4.100 255.255.255.0
no sh
exit
int gi 2
ip address 192.168.100.254 255.255.255.0
no sh
end
wr
```

Для проверки:

sh ip interface brief

RTR-R

en
conf t
int gi 1
ip address 5.5.5.100 255.255.255.0
no sh
exit
int gi 2
ip address 172.16.100.254 255.255.255.0
no sh
end
wr

Для проверки:
sh ip interface brief

SRV

Правой клавишей на значке сети
Выбрать “Open Network & Internet setting”
Далее выбрать “Change adapter options”
Выбрать сетевой адаптер => Правой клавишей => Properties => Internet Protocol Version 4 => Properties
Настроить IPv4

Settings

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

Proxy

Status

Network status

Ethernet0
Public network

No Internet access

Your device is connected, but you might not be able to access anything on the network. If you have a limited data plan, you can make this network a metered connection or change other properties.

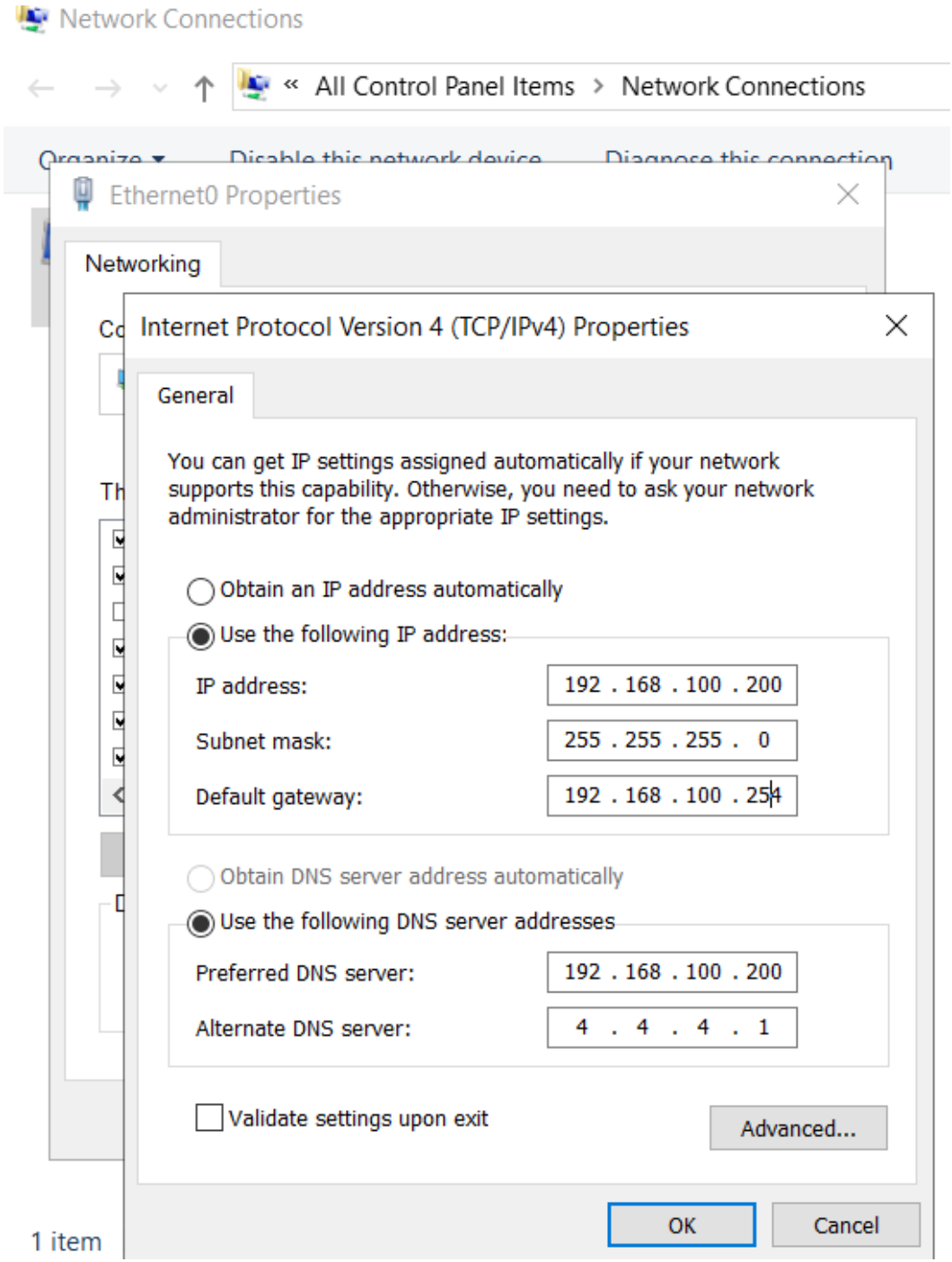
Troubleshoot

Change connection properties

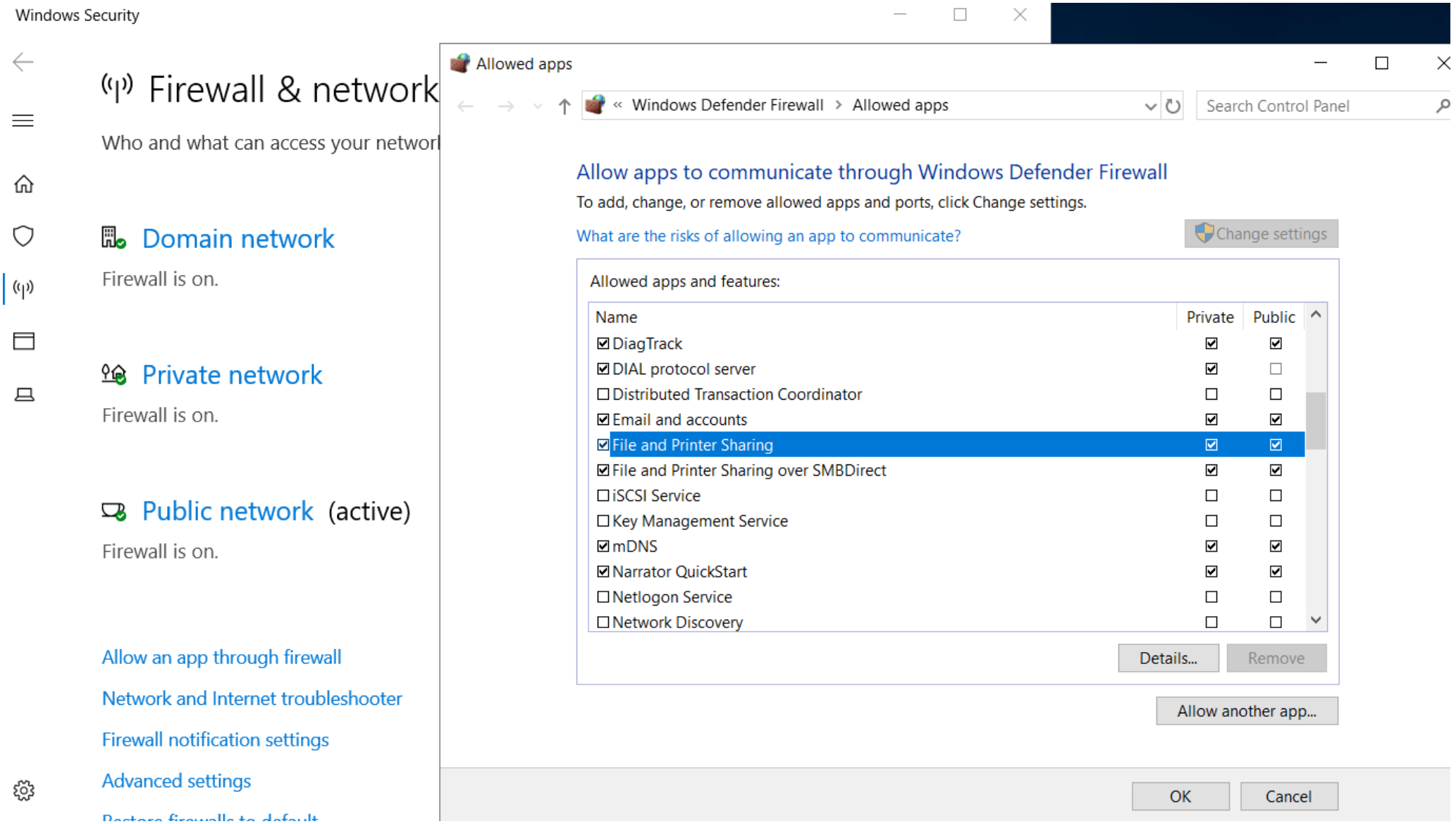
Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.


Network Connections
« All Control Panel Items › Network Connections
Organize
Disable this network device
Diagnose this connection
Ethernet0 Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 100 . 200
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 100 . 254
Obtain DNS server address automatically
Use the following DNS server addresses
Preferred DNS server: 192 . 168 . 100 . 200
Alternate DNS server: 4 . 4 . 4 . 1
Validate settings upon exit
Advanced...
OK
Cancel
1 item

Выбрать “Windows Firewall” => Allow an app through firewall
Отметить “"File And Printer Sharing” и “"File And Printer Sharing over SMBDirect”



Или можно ввести команды в PowerShell

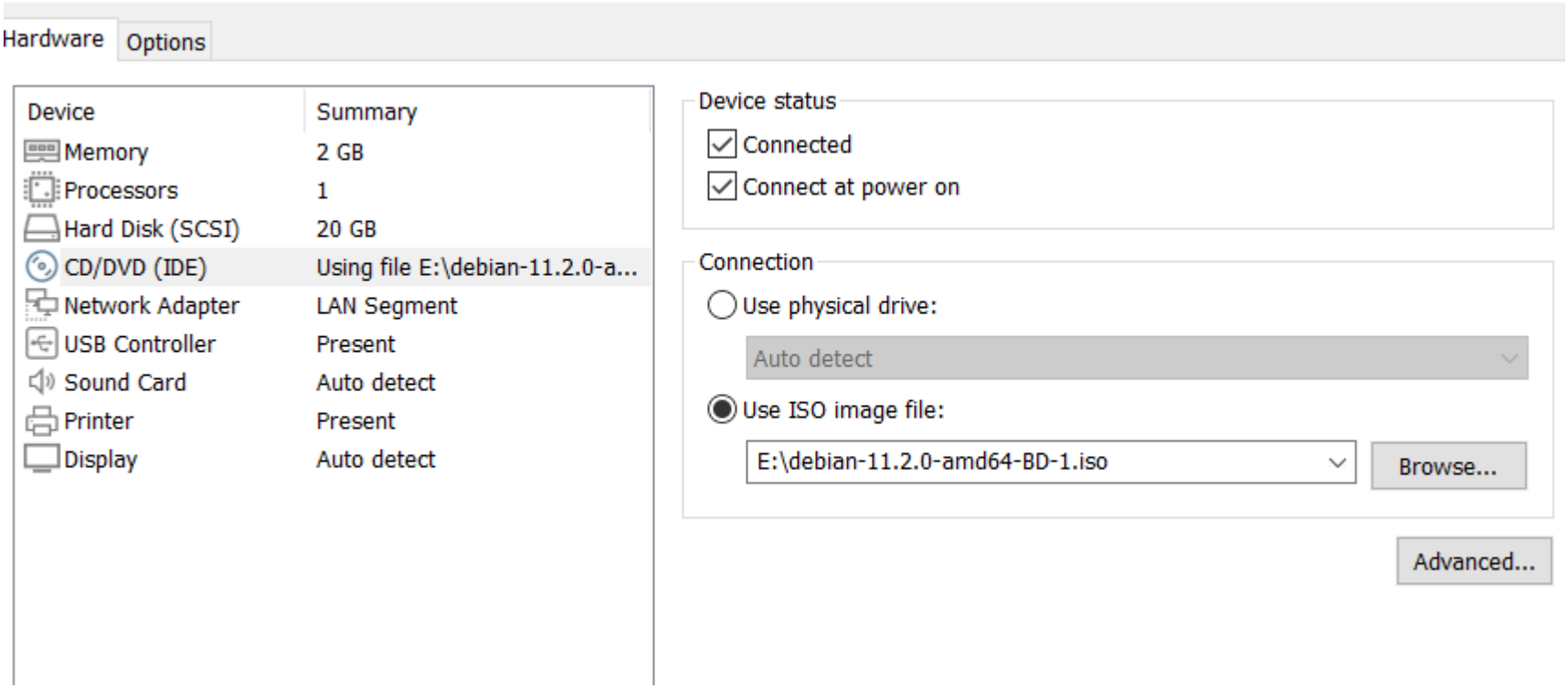
```
$GetIndex = Get-NetAdapter
New-NetIPAddress -InterfaceIndex $GetIndex.ifIndex -IPAddress 192.168.100.200 -PrefixLength 24 -DefaultGateway 192.168.100.254
Set-DnsClientServerAddress -InterfaceIndex $GetIndex.ifIndex -ServerAddresses
```

```
("192.168.100.200","4.4.4.1")
```

```
Set-NetFirewallRule -DisplayGroup "File And Printer Sharing" -Enabled True -Profile Any
```

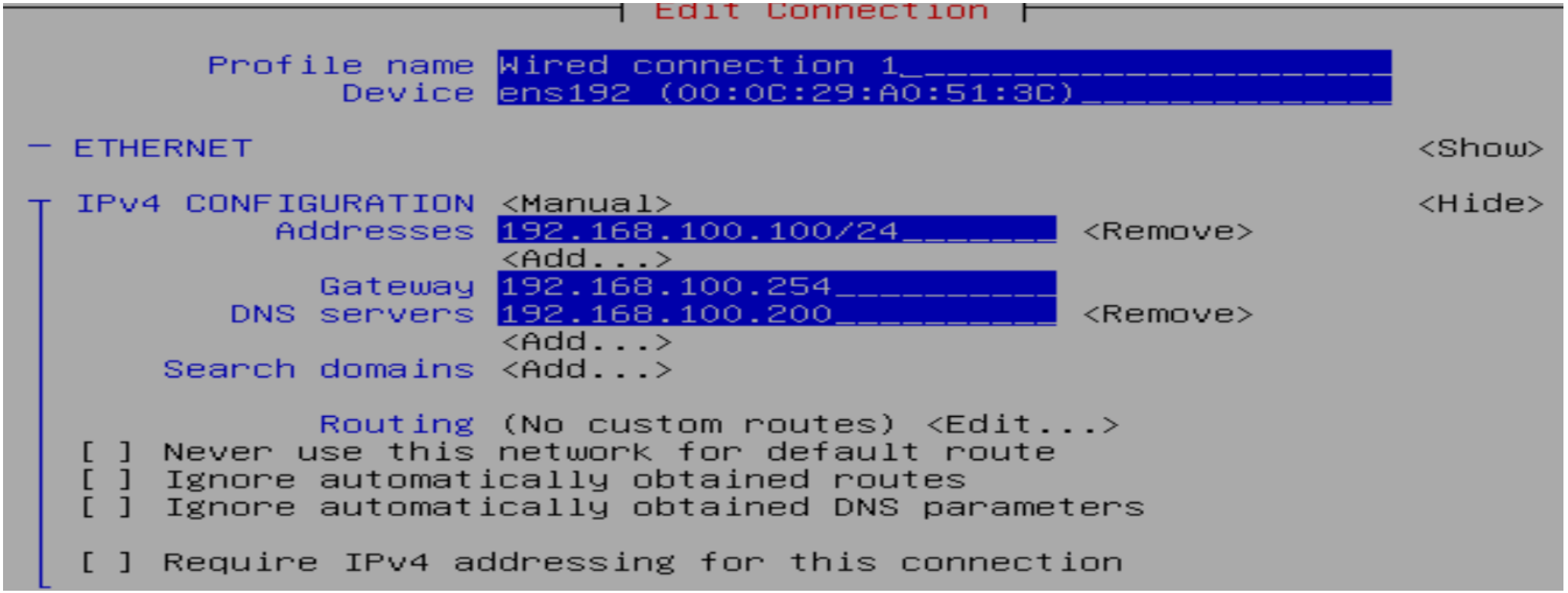
WEB-L

Подключить диск BD-1 в настройка виртуальной машины



apt-cdrom add
apt install -y network-manager

nmtui



Перезапустить NetworkManager

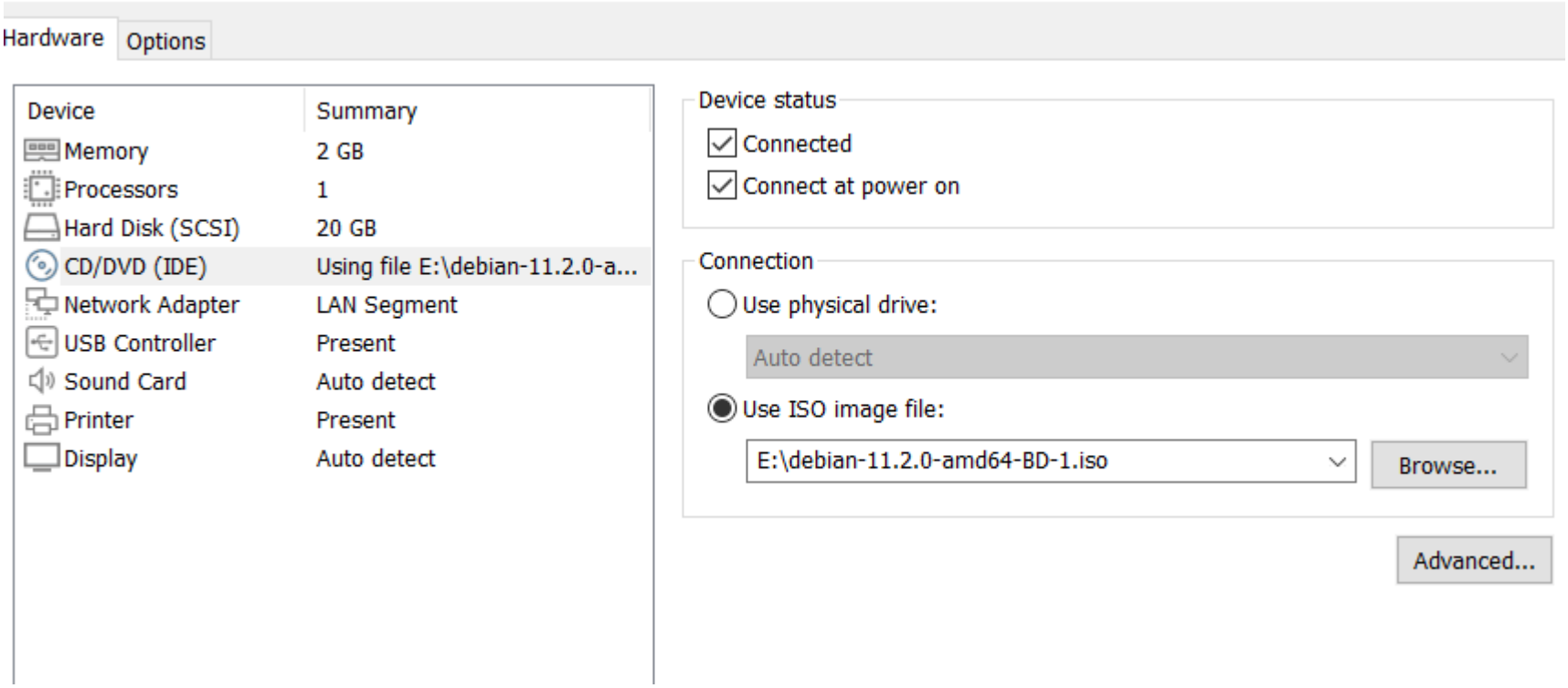
systemctl restart NetworkManager

То же самое, через терминал:

nmcli connection show
nmcli connection modify Wired\ connection\ 1 conn.autoconnect yes conn.interface-name ens192 ipv4.method manual ipv4.addresses '192.168.100.100/24' ipv4.dns 192.168.100.200 ipv4.gateway 192.168.100.254

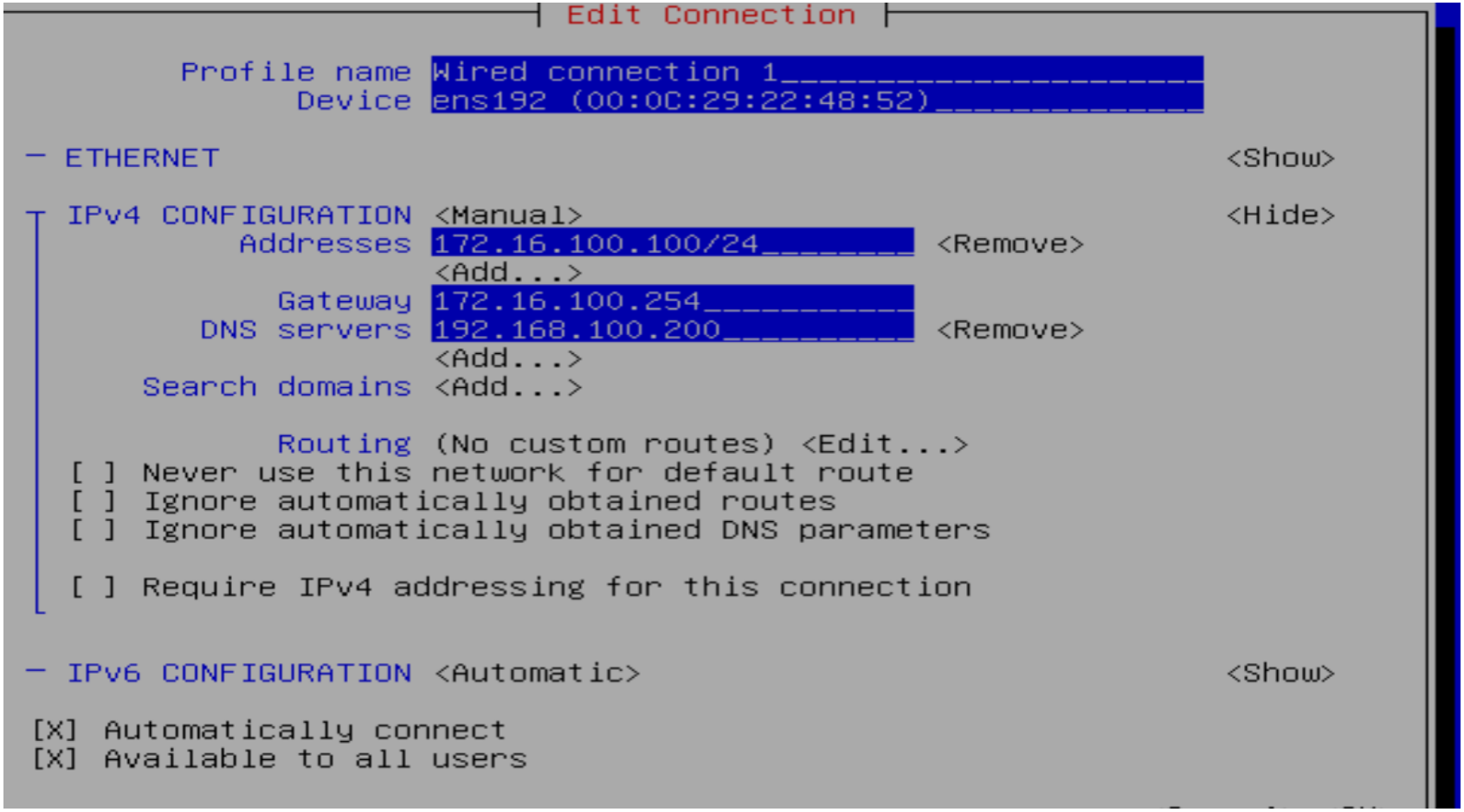
WEB-R

Подключить диск BD-1 в настройка виртуальной машины



apt-cdrom add
apt install -y network-manager

nmtui



Перезапустить NetworkManager

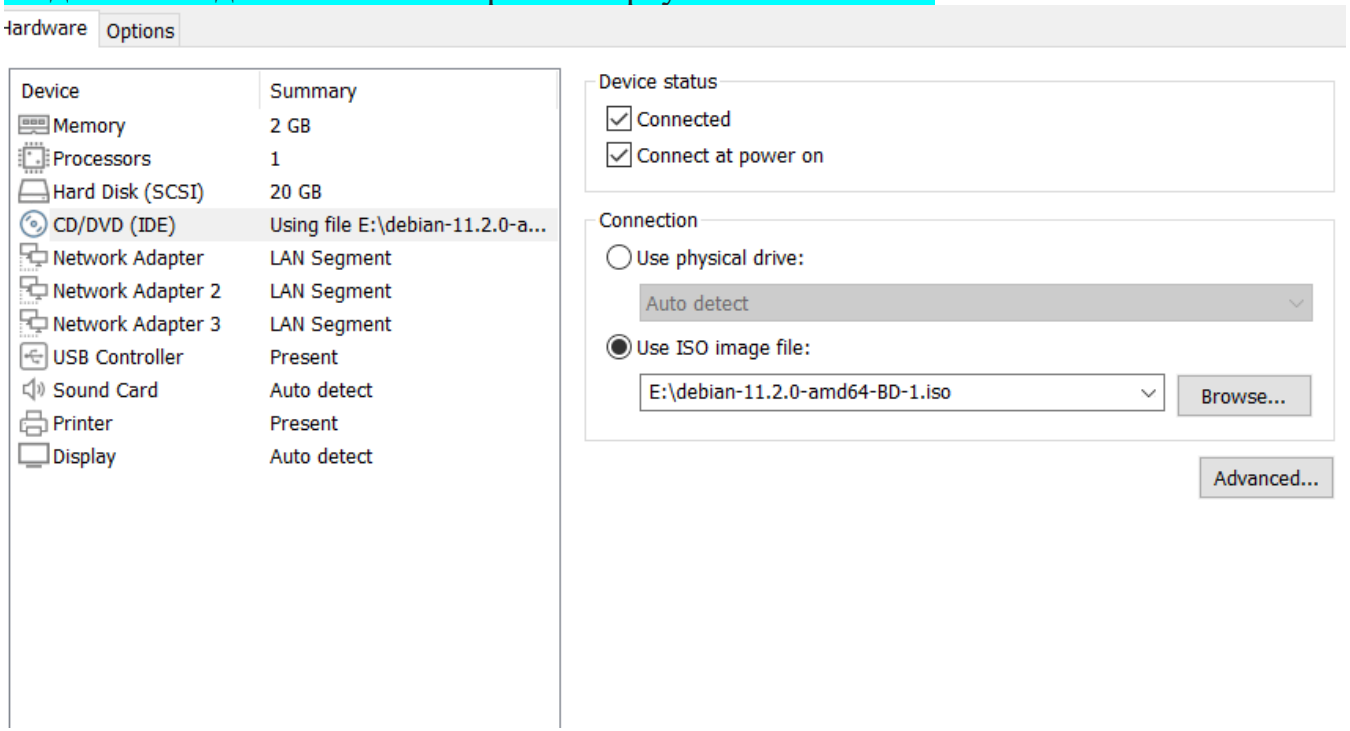
systemctl restart NetworkManager

То же самое, через терминал:

nmcli connection show
nmcli connection modify Wired\ connection\ 1 conn.autoconnect yes conn.interface-name ens192 ipv4.method manual ipv4.addresses '172.16.100.100/24' ipv4.dns 192.168.100.200 ipv4.gateway 172.16.100.254

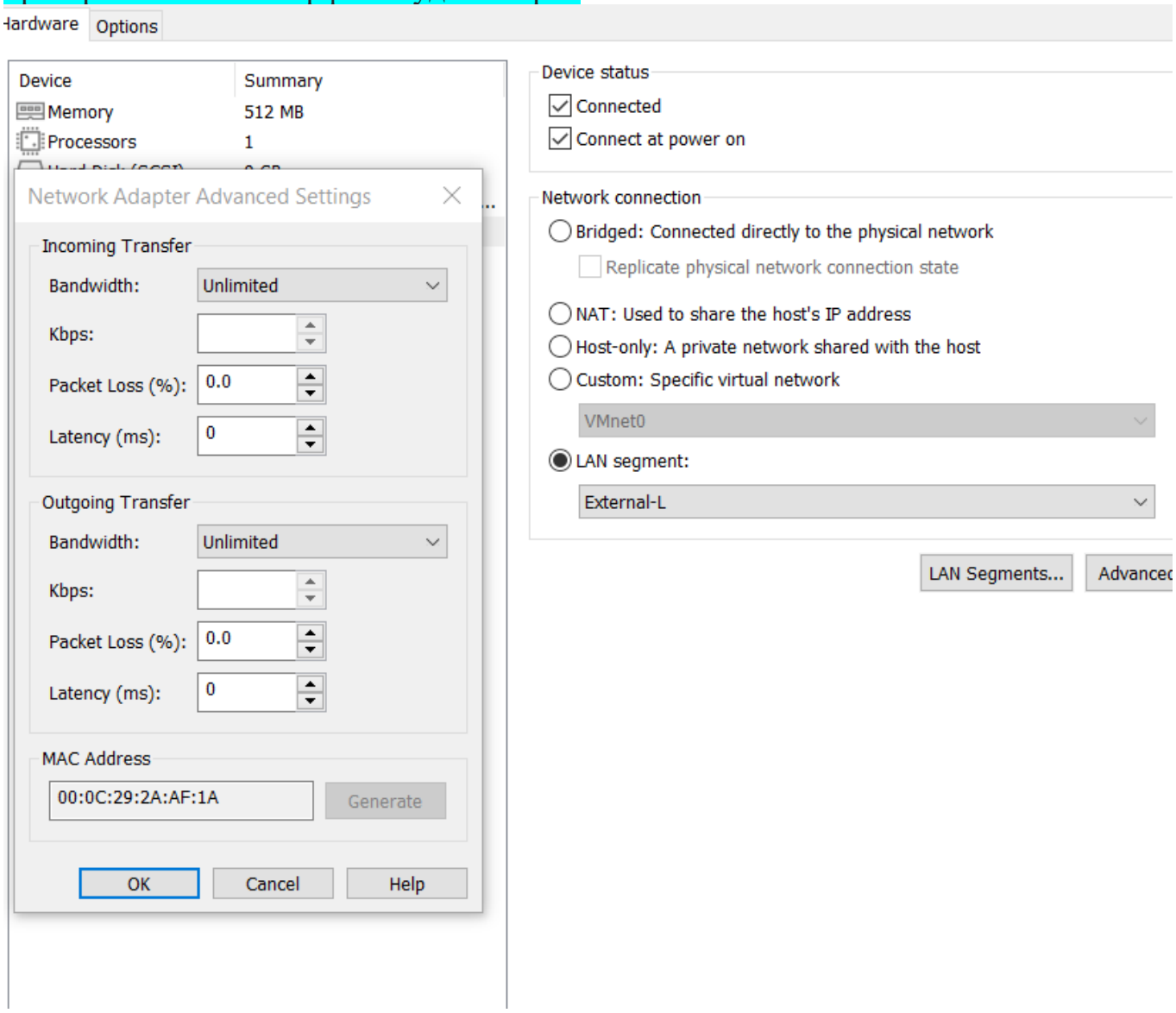
ISP

Подключить диск BD-1 в настройка виртуальной машины

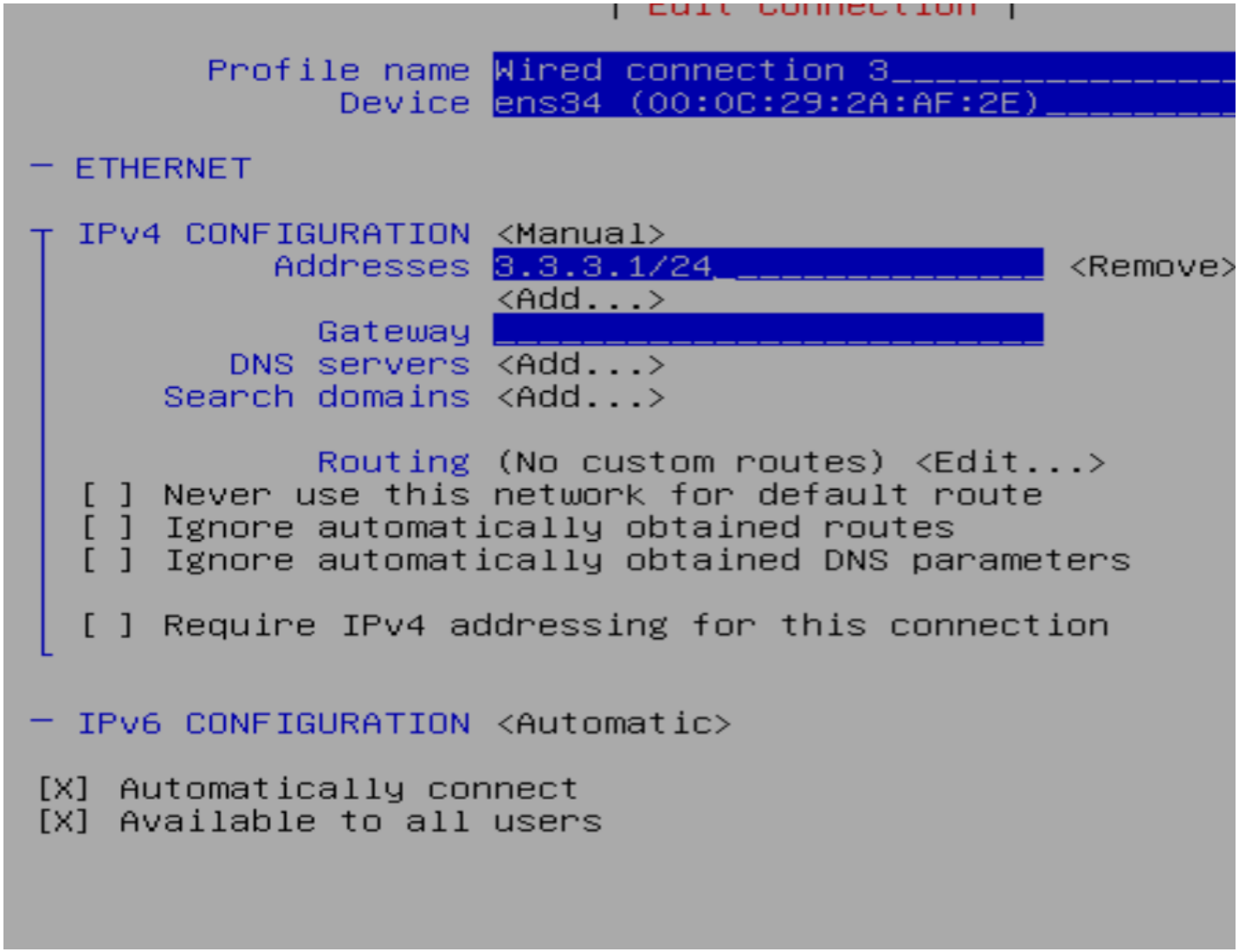


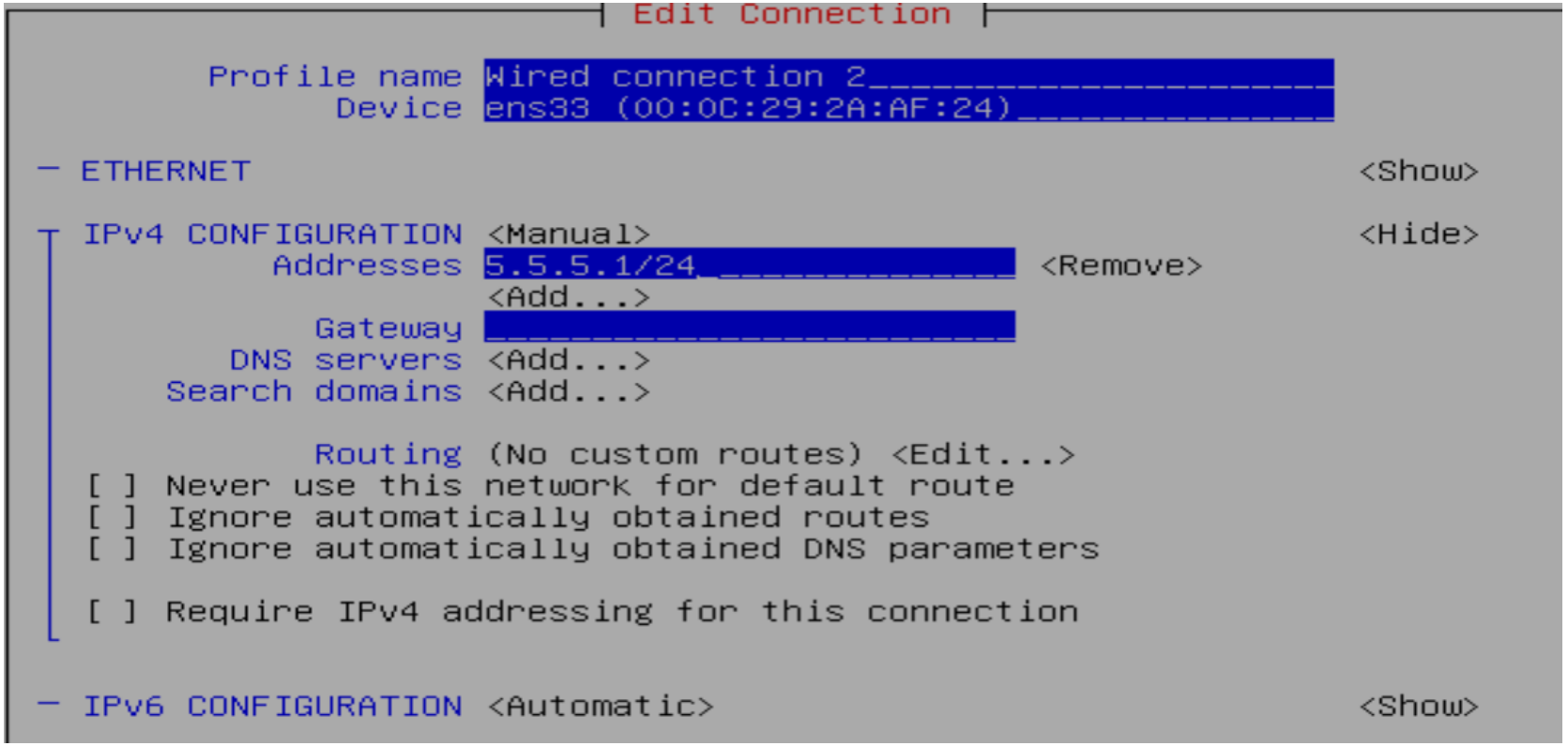
apt-cdrom add
apt install -y network-manager bind9 chrony

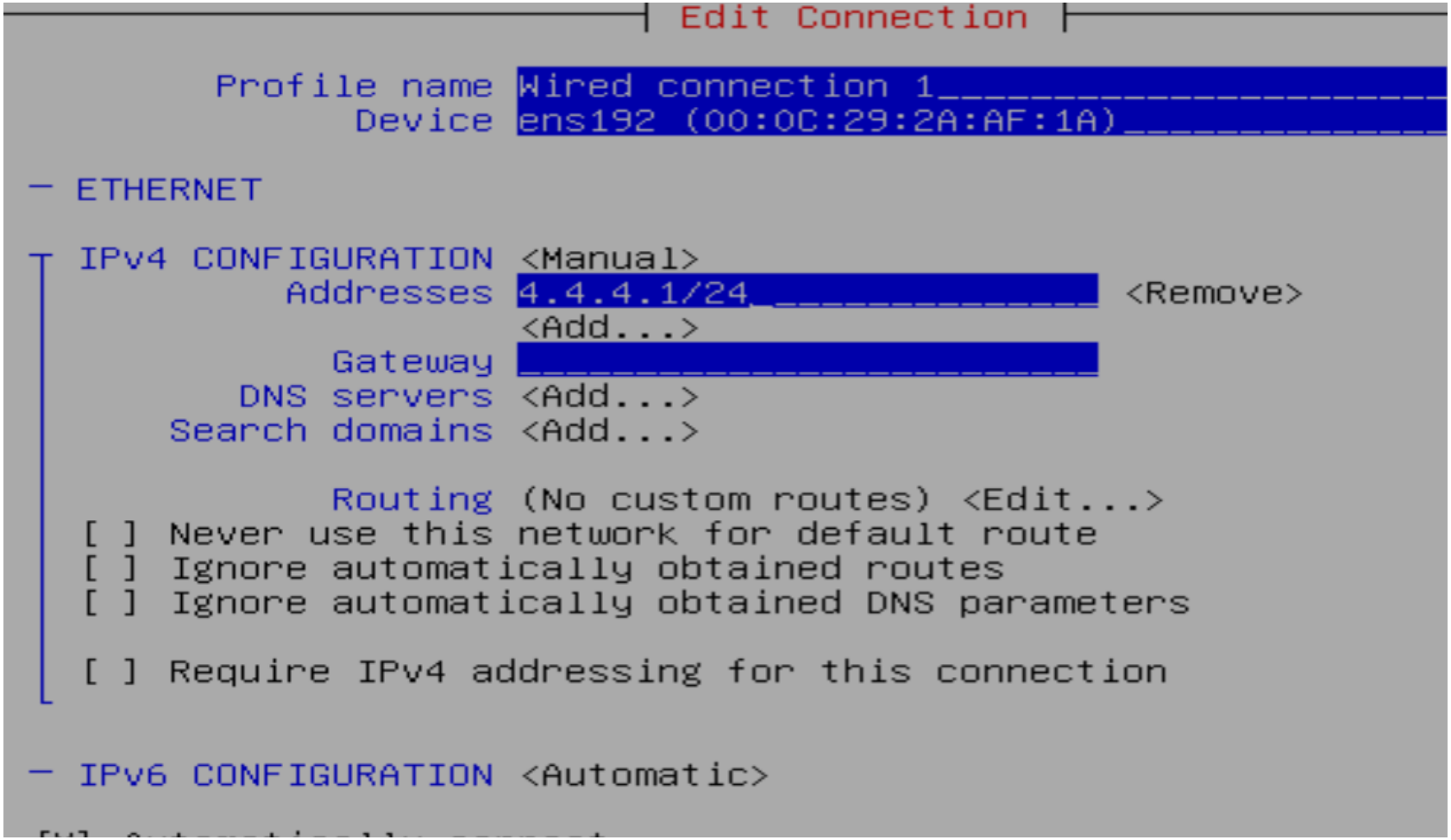
проверяем какой интерфейс куда смотрит

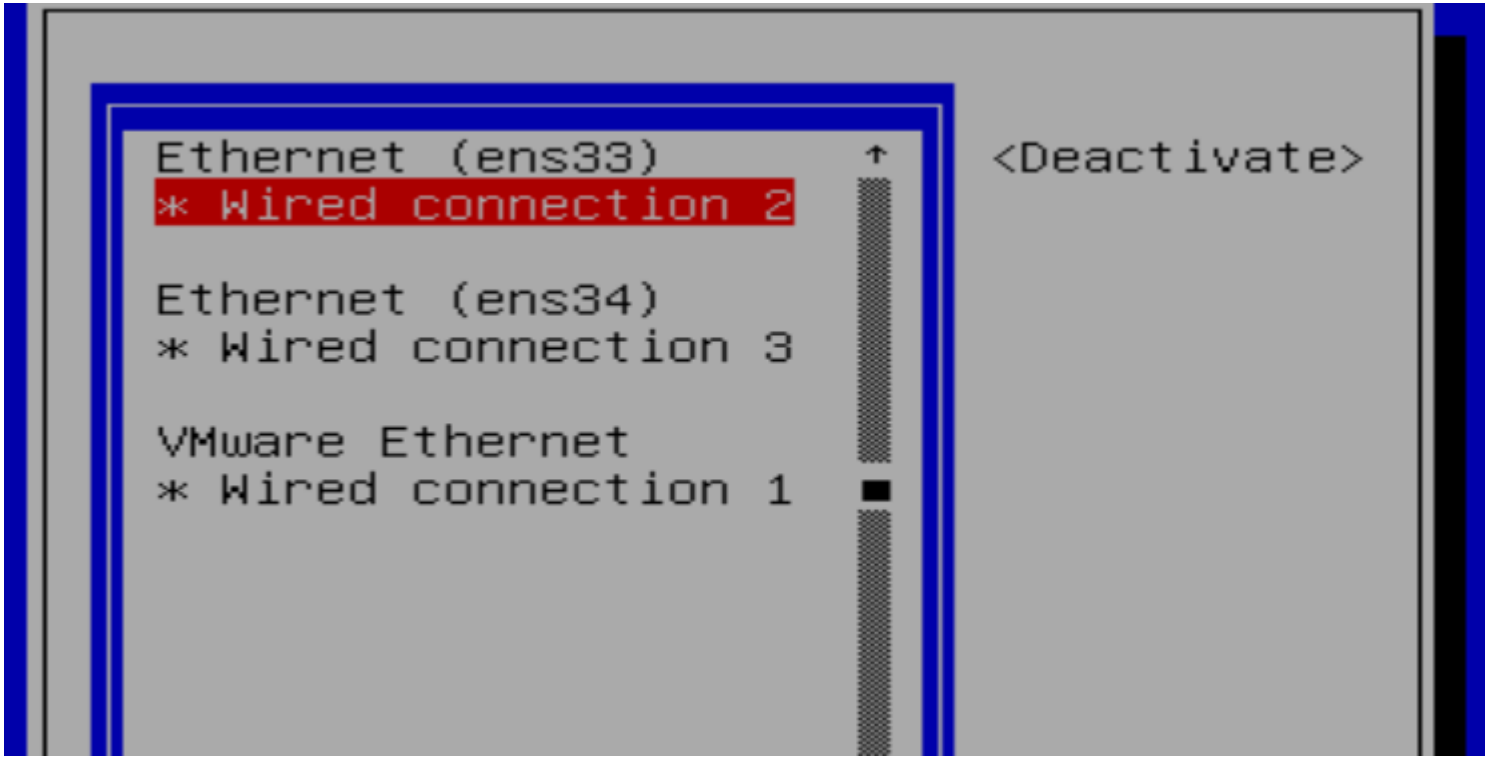


nmtui


Edit connection
Profile name Wired connection 3
Device ens34 (00:0C:29:2A:AF:2E)
ETHERNET
IPv4 CONFIGURATION <Manual>
Addresses 3.3.3.1/24 <Remove>
<Add...>
Gateway
DNS servers <Add...>
Search domains <Add...>
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 CONFIGURATION <Automatic>
[X] Automatically connect
[X] Available to all users


Edit Connection
Profile name Wired connection 2
Device ens33 (00:0C:29:2A:AF:24)
ETHERNET <Show>
IPv4 CONFIGURATION <Manual> <Hide>
Addresses 5.5.5.1/24 <Remove>
<Add...>
Gateway
DNS servers <Add...>
Search domains <Add...>
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 CONFIGURATION <Automatic> <Show>


Edit Connection
Profile name Wired connection 1
Device ens192 (00:0C:29:2A:AF:1A)
ETHERNET
IPv4 CONFIGURATION <Manual>
Addresses 4.4.4.1/24 <Remove>
<Add...>
Gateway
DNS servers <Add...>
Search domains <Add...>
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 CONFIGURATION <Automatic>



Перезапустить NetworkManager

systemctl restart NetworkManager

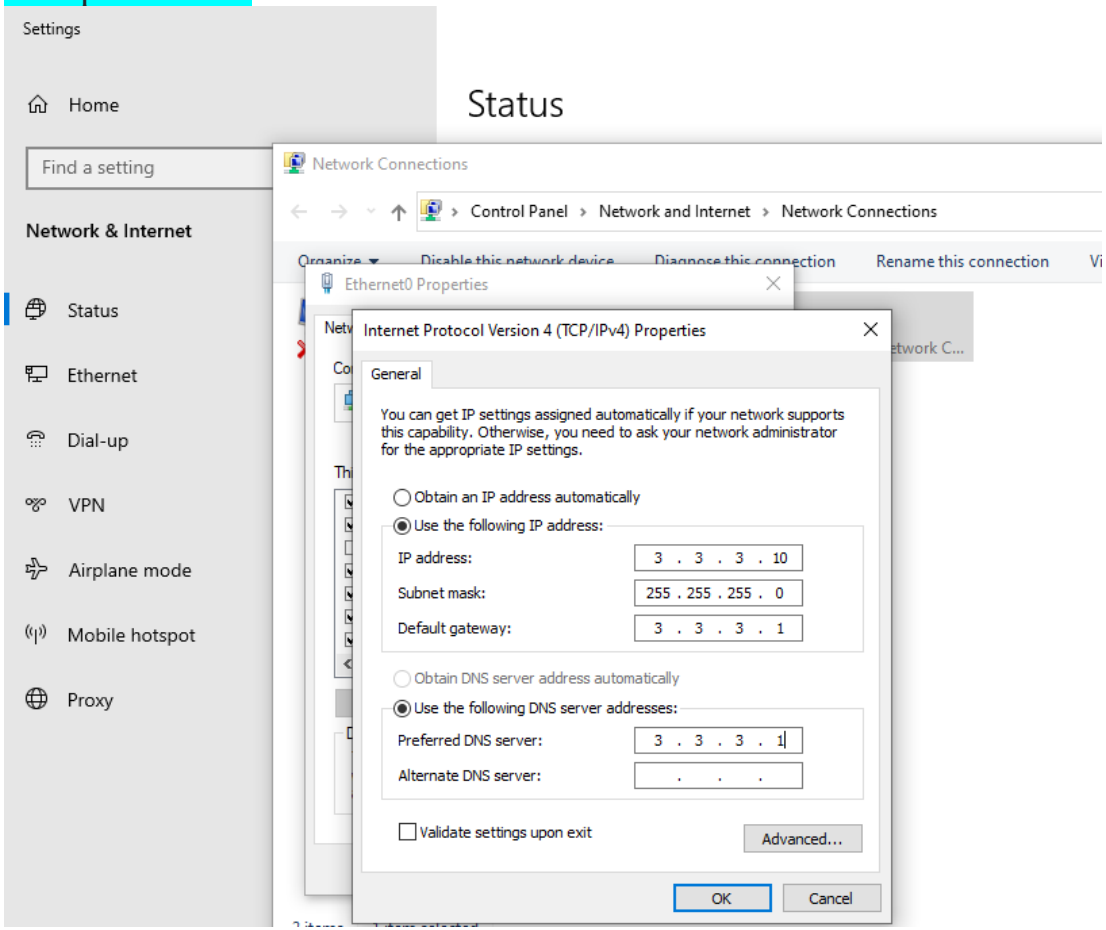
То же самое, через терминал:

nmcli connection show
nmcli connection modify Wired\ connection\ 1 conn.autoconnect yes conn.interface-name ens192 ipv4.method manual ipv4.addresses '3.3.3.1/24'
nmcli connection modify Wired\ connection\ 2 conn.autoconnect yes conn.interface-name ens224 ipv4.method manual ipv4.addresses '4.4.4.1/24'

nmcli connection modify Wired\ connection\ 3 conn.autoconnect yes conn.interface-name ens256 ipv4.method manual ipv4.addresses '5.5.5.1/24'

CLI

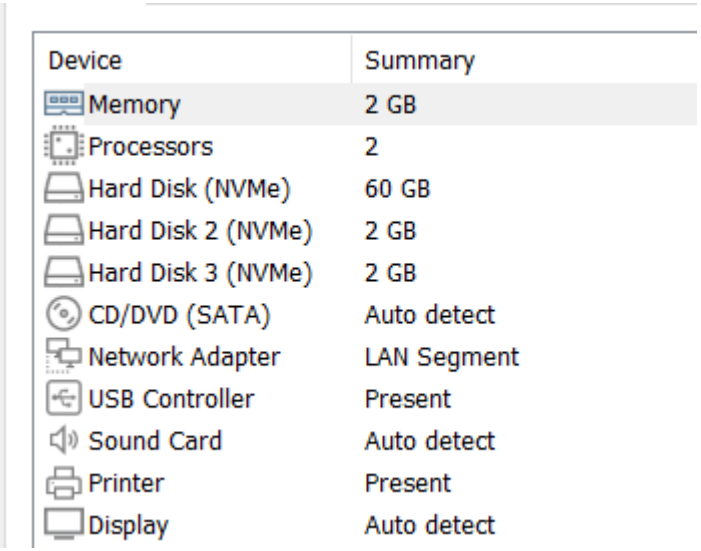
Правой клавишей на значке сети
Выбрать “Open Network & Internet setting” => Change adapter options
Выбрать сетевой адаптер => Правой клавишей => Properties => Internet Protocol Version 4 => Properties
Настроить IPv4



Команды через PowerShell:

```
$GetIndex = Get-NetAdapter
New-NetIPAddress -InterfaceIndex $GetIndex.ifIndex -IPAddress 3.3.3.10 -PrefixLength 24 -DefaultGateway 3.3.3.1
Set-DnsClientServerAddress -InterfaceIndex $GetIndex.ifIndex -ServerAddresses ("3.3.3.1")
```

4. Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с Таблицей 1;



Сетевая связность.

В рамках данного модуля требуется обеспечить сетевую связность между регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть “Интернет”

1. Сети, подключенные к ISP, считаются внешними:
    - Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;
2. Платформы контроля трафика, установленные на границах регионов, должны выполнять трансляцию трафика, идущего из соответствующих внутренних сетей во внешние сети стенда и в сеть Интернет.
    - Трансляция исходящих адресов производится в адрес платформы,расположенный во внешней сети.
3. Между платформами 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 платформами 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.
4. Платформа управления трафиком RTR-L выполняет контроль входящего трафика согласно следующим правилам:
    - Разрешаются подключения к портам DNS, HTTP и HTTPS для всех клиентов;
        - Порты необходимо для работы настраиваемых служб
    - Разрешается работа выбранного протокола организации защищенной связи;
        - Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”
    - Разрешается работа протоколов ICMP;
    - Разрешается работа протокола SSH;
    - Прочие подключения запрещены;
    - Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;
5. Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:
    - Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;

        - Порты необходимо для работы настраиваемых служб
    - Разрешается работа выбранного протокола организации защищенной связи;
        - Разрешение портов должно быть выполнено по принципу необходимо и достаточно”
    - Разрешается работа протоколов ICMP;
    - Разрешается работа протокола SSH;
    - Прочие подключения запрещены;
    - Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;
6. Обеспечьте настройку служб SSH региона Left и Right:
    - Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на BM Web-L;
    - Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-R на порт 2244 должны быть перенаправлены на BM Web-R;

1. Сети, подключенные к ISP, считаются внешними:

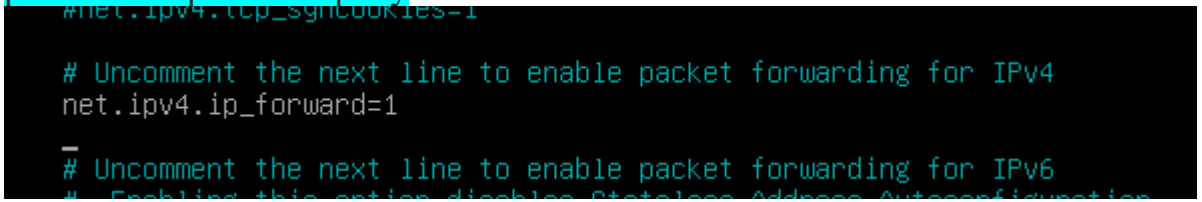
ISP forward

nano /etc/sysctl.conf

net.ipv4.ip_forward=1

sysctl -p

разкоментировать строку



reboot

RTR-L Gitw

ip route 0.0.0.0 0.0.0.0 4.4.4.1

RTR-R Gitw

ip route 0.0.0.0 0.0.0.0 5.5.5.1

2. Платформы контроля трафика, установленные на границах регионов, должны выполнять трансляцию трафика, идущего из соответствующих внутренних сетей во внешние сети стенда и в сеть Интернет.

RTR-L NAT

посмотреть, где какой интерфейс командой show ip int brief

на внутр. интерфейсе - ip nat inside

на внешн. интерфейсе - ip nat outside

int gi 1
ip nat outside
exit
int gi 2
ip nat inside
exit

access-list 1 permit 192.168.100.0 0.0.0.255
ip nat inside source list 1 interface Gi1 overload

RTR-R NAT

посмотреть, где какой интерфейс командой show ip int brief

на внутр. интерфейсе - ip nat inside

на внешн. интерфейсе - ip nat outside

int gi 1
ip nat outside
exit
int gi 2
ip nat inside
exit

access-list 1 permit 172.16.100.0 0.0.0.255
ip nat inside source list 1 interface Gi1 overload

show ip nat translations – проверяет правильность работы NAT. (только если был трафик из под NAT адреса иначе покажет 0)

3. Между платформами должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.

RTR-L GRE

interface Tunnel 1
ip address 172.16.1.1 255.255.255.0
tunnel mode gre ip
tunnel source 4.4.4.100
tunnel destination 5.5.5.100

exit
router eigrp 6500
network 192.168.100.0 0.0.0.255
network 172.16.1.0 0.0.0.255
exit

RTR-R

interface Tunnel 1
ip address 172.16.1.2 255.255.255.0
tunnel mode gre ip
tunnel source 5.5.5.100
tunnel destination 4.4.4.100
exit
router eigrp 6500
network 172.16.100.0 0.0.0.255
network 172.16.1.0 0.0.0.255
exit

Проверка соседей show ip eigrp neighbors

RTR-L

crypto isakmp policy 1
encr aes
authentication pre-share
hash sha256
group 14
exit

crypto isakmp key TheSecretMustBeAtLeast13bytes address 5.5.5.100

```
crypto isakmp nat keepalive 5

crypto ipsec transform-set TSET  esp-aes 256 esp-sha256-hmac
mode tunnel
exit

crypto ipsec profile VTI
set transform-set TSET
exit

interface Tunnel1
tunnel mode ipsec ipv4
tunnel protection ipsec profile VTI
exit
```

RTR-R

```
conf t

crypto isakmp policy 1
encr aes
authentication pre-share
hash sha256
group 14
exit

crypto isakmp key TheSecretMustBeAtLeast13bytes address 4.4.4.100
crypto isakmp nat keepalive 5

crypto ipsec transform-set TSET  esp-aes 256 esp-sha256-hmac
mode tunnel
```

crypto ipsec profile VTI
set transform-set TSET
exit

interface Tunnel1
tunnel mode ipsec ipv4
tunnel protection ipsec profile VTI
exit

Проверка работы
show crypto isakmp sa – Эта команда отображает сопоставление безопасности (SA) протокола ISAKMP, созданное между двумя одноранговыми узлами

```
RTR-L(config)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
5.5.5.100       4.4.4.100       QM_IDLE           1001 ACTIVE
4.4.4.100       5.5.5.100       QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA
```

show crypto ipsec sa – проверяет состояние готовности туннеля IPsec

4. Платформа управления трафиком RTR-L выполняет контроль входящего трафика согласно следующим правилам:

RTR-L ACL

ip access-list extended Lnew
permit tcp any any established
permit udp host 4.4.4.100 eq 53 any
permit udp host 5.5.5.1 eq 123 any
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 2222
permit udp host 5.5.5.100 host 4.4.4.100 eq 500
permit esp any any
permit icmp any any
exit

применить на внешний интерфейс

int gi 1
ip access-group Lnew in

do wr

5. Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:

RTR-R ACL

ip access-list extended Rnew
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 4.4.4.100 host 5.5.5.100 eq 500
permit esp any any
permit icmp any any
exit

применить на внешний интерфейс

int gi 1
ip access-group Rnew in

do wr

6. Обеспечьте настройку служб SSH региона Left:

RTR-L SSH

ip nat inside source static tcp 192.168.100.100 22 4.4.4.100 2222

do wr

RTR-R SSH

ip nat inside source static tcp 172.16.100.100 22 5.5.5.100 2244

do wr

SSH WEB-L

apt-cdrom add
apt install -y openssh-server ssh
systemctl start sshd
systemctl enable ssh

SSH WEB-R

apt-cdrom add
apt install -y openssh-server ssh
systemctl start sshd
systemctl enable ssh

Инфраструктурные службы

В рамках данного модуля необходимо настроить основные инфраструктурные службы и настроить представленные ВМ на применение этих служб для всех основных функций.

1. Выполните настройку первого уровня DNS-системы стенда:
    - Используется ВМ ISP;
    - Обслуживается зона demo.wsr
        - Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;
    - Сервер делегирует зону int.demo.wsr на SRV;
        - Поскольку SRV находится во внутренней сети западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона.
        - Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV
    - Внешний клиент CLI должен использовать DNS-службу, развернутую на ISP, по умолчанию;
2. Выполните настройку второго уровня DNS-системы стенда;
    - Используется ВМ SRV;
    - Обслуживается зона int.demo.wsr;
        - Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;
    - Обслуживаются обратные зоны для внутренних адресов регионов

        - Имена для разрешения обратных записей следует брать из Таблицы 2;
    - Сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;
        - Обслуживание клиентов(внешних и внутренних), обращающихся к к зоне int.demo.wsr, должно производится без каких либо ограничений по адресу источника;
    - Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен;
3. Выполните настройку первого уровня системы синхронизации времени:
    - Используется сервер ISP.
    - Сервер считает собственный источник времени верным, stratum=4;
    - Сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком;
        - Подразумевается обращение SRV для синхронизации времени;
    - Клиент CLI должен использовать службу времени ISP;
4. Выполните конфигурацию службы второго уровня времени на SRV
    - Сервер синхронизирует время с хостом ISP;
        - Синхронизация с другими источникам запрещена;
    - Сервер должен допускать обращения внутренних хостов регионов, в том числе и платформ управления трафиком, для синхронизации времени;
    - Все внутренние хосты(в том числе и платформы управления трафиком) должны синхронизировать свое время с SRV;
5. Реализуйте файловый SMB-сервер на базе SRV
    - Сервер должен предоставлять доступ для обмена файлами серверам WEB-L и WEB-R;
    - Сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:
        - /mnt/storage для система на базе Linux;
        - Диск R:\ для систем на базе Windows;
    - Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа “Зеркало”;
6. Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:
    - Служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux
        - Разделяемый каталог должен быть смонтирован по адресу /opt/share;

- Каталог должен позволять удалять и создавать файлы в нем для всех пользователей;

7. Выполните настройку центра сертификации на базе SRV:
   - В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca
   - Выдаваемые сертификаты должны иметь срок жизни не менее 500 дней;
   - Параметры выдаваемых сертификатов:
     - Страна RU;
     - Организация DEMO.WSR;
     - Прочие поля (за исключением CN) должны быть пусты;

Таблица 2. DNS-записи зон

Zone	Type	Key	Meaning
demo.wsr	A	isp	3.3.3.1
	A	srv	4.4.4.100
	A	www	4.4.4.100
	A	www	5.5.5.100
	CNAME	internet	isp
	NS	int	rtr-l.demo.wsr
	NS	int.demo.wsr	srv.demo.wsr
	A	rtr-l	4.4.4.100

1. Выполните настройку первого уровня DNS-системы стенда:

ISP

apt-cdrom add
apt install -y bind9

Создать каталог

mkdir /opt/dns

Скопировать файлы

cp /etc/bind/db.local /opt/dns/demo.db

chown -R bind:bind /opt/dns

Открыть файл
nano /etc/apparmor.d/usr.sbin.named

Добавить строку (смотри скрин)
/opt/dns/** rw,

```
# /etc/bind should be read-only for bind
# /var/lib/bind is for dynamically updated zone (and journal) files.
# /var/cache/bind is for slave/stub data, since we're not the origin of it.
# See /usr/share/doc/bind9/README.Debian.gz
/etc/bind/** r,
/var/lib/bind/** rw,
/var/lib/bind/ rw,
/var/cache/bind/** lrw,
/var/cache/bind/ rw,
/opt/dns/** rw,
# Database file used by allow-new-zones
/var/cache/bind/_default.nzd-lock rwk,
```

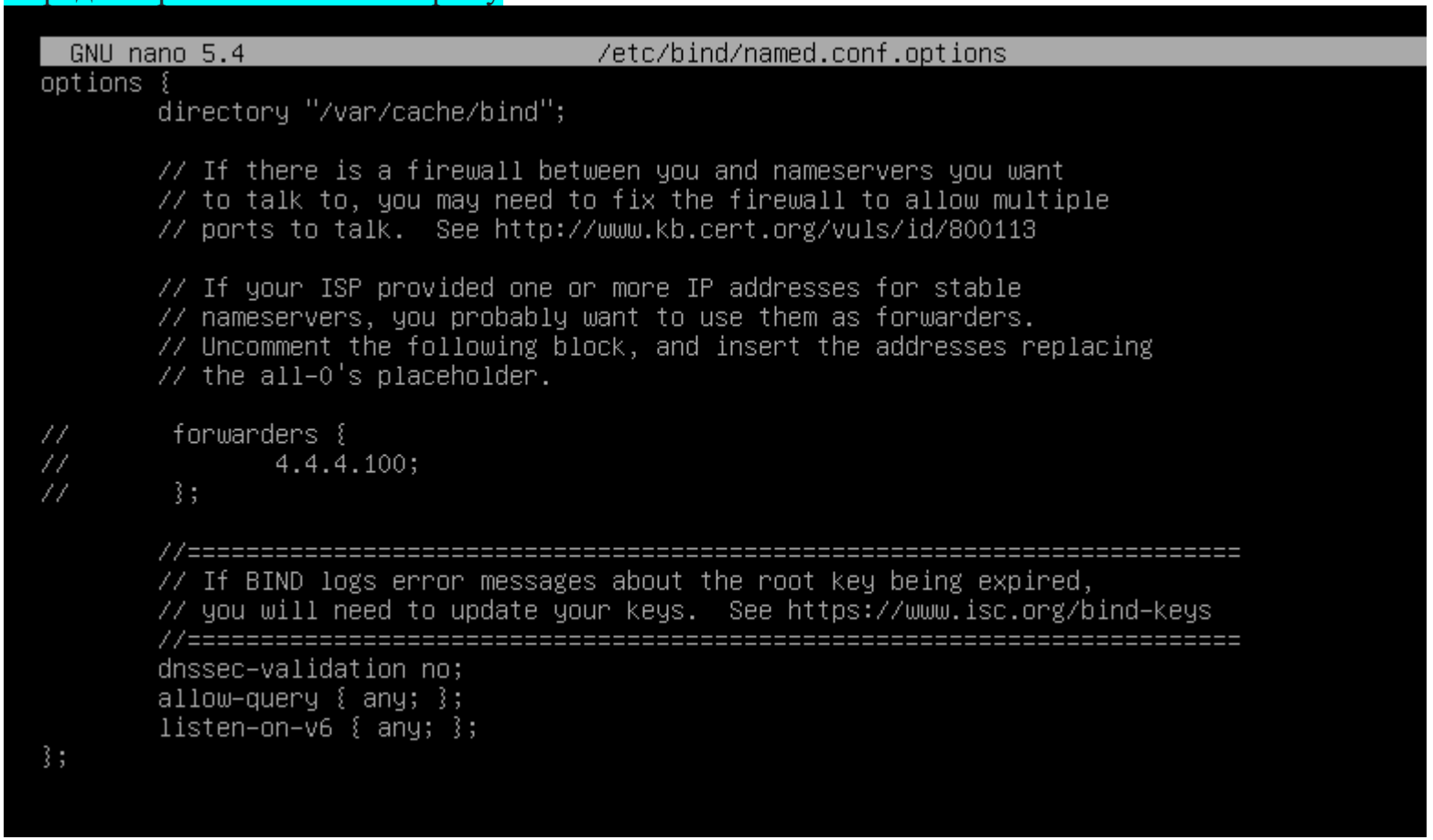
Перезапустить сервис

systemctl restart apparmor.service

Открыть файл

nano /etc/bind/named.conf.options

Отредактировать согласно скрину



Открыть файл

nano /etc/bind/named.conf.default-zones

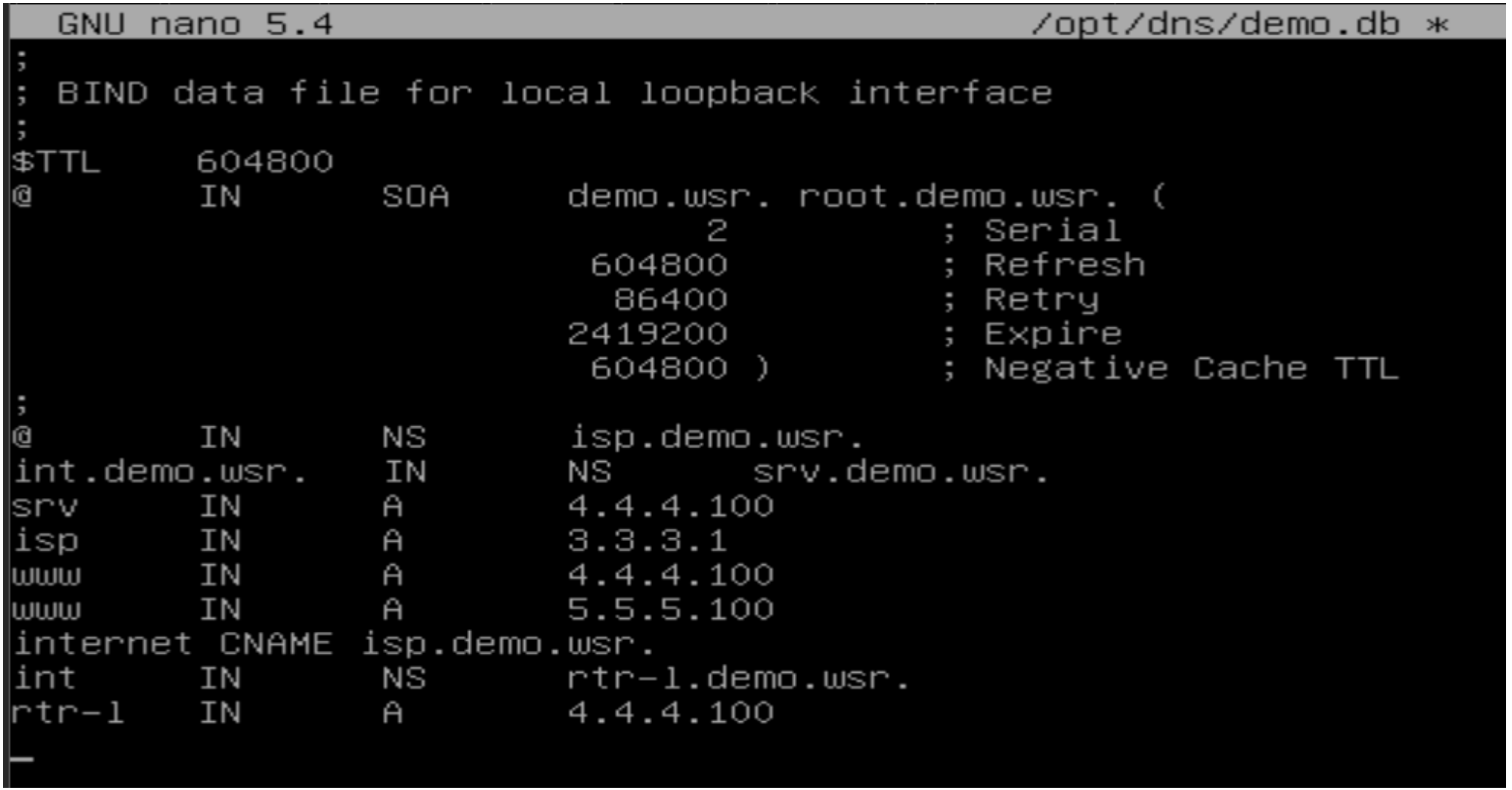
и отредактировать (смотри скрин)

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

```
// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

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

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

Открыть файл и отредактировать

nano /opt/dns/demo.db



systemctl restart bind9

RTR-L

b. Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV.

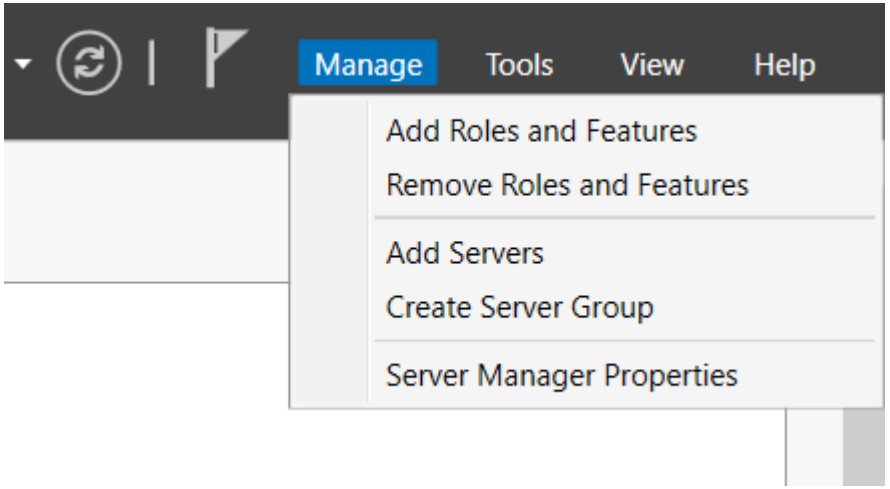
ip nat inside source static tcp 192.168.100.200 53 4.4.4.100 53

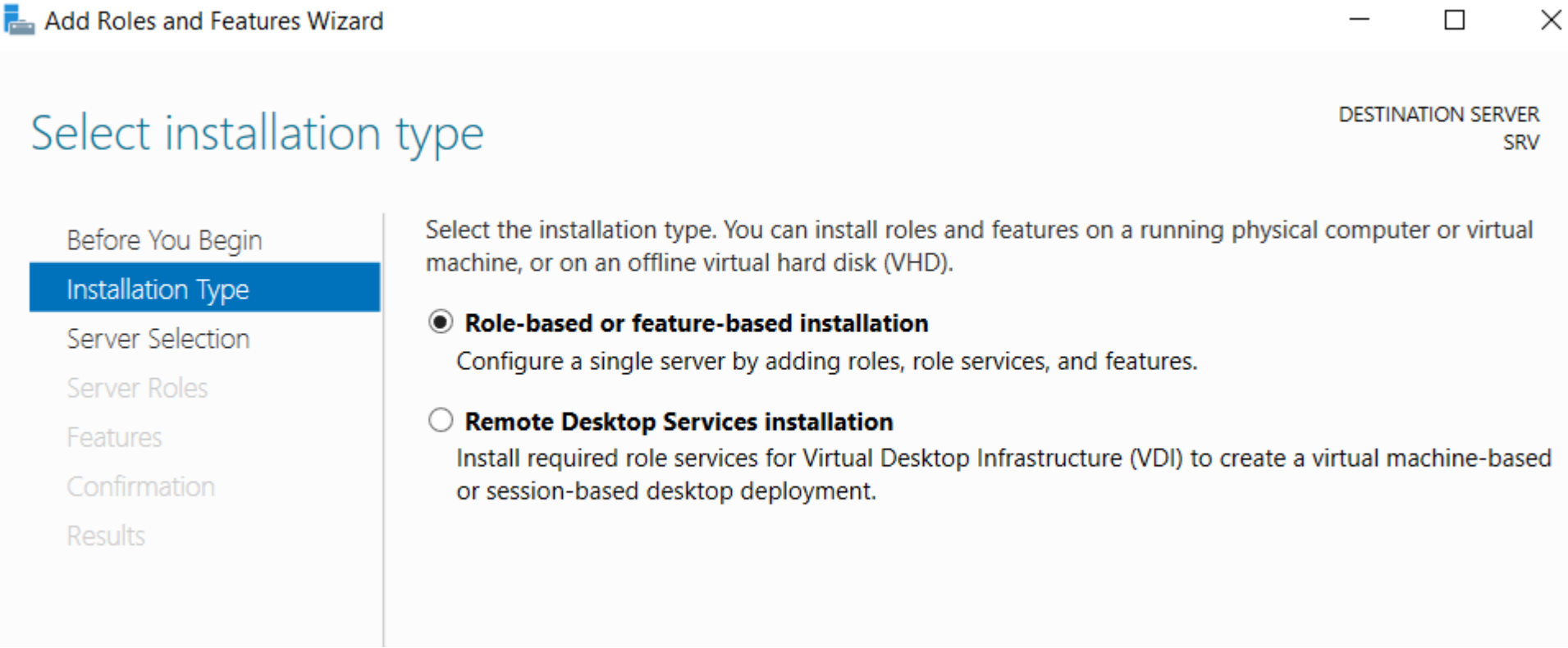
ip nat inside source static udp 192.168.100.200 53 4.4.4.100 53

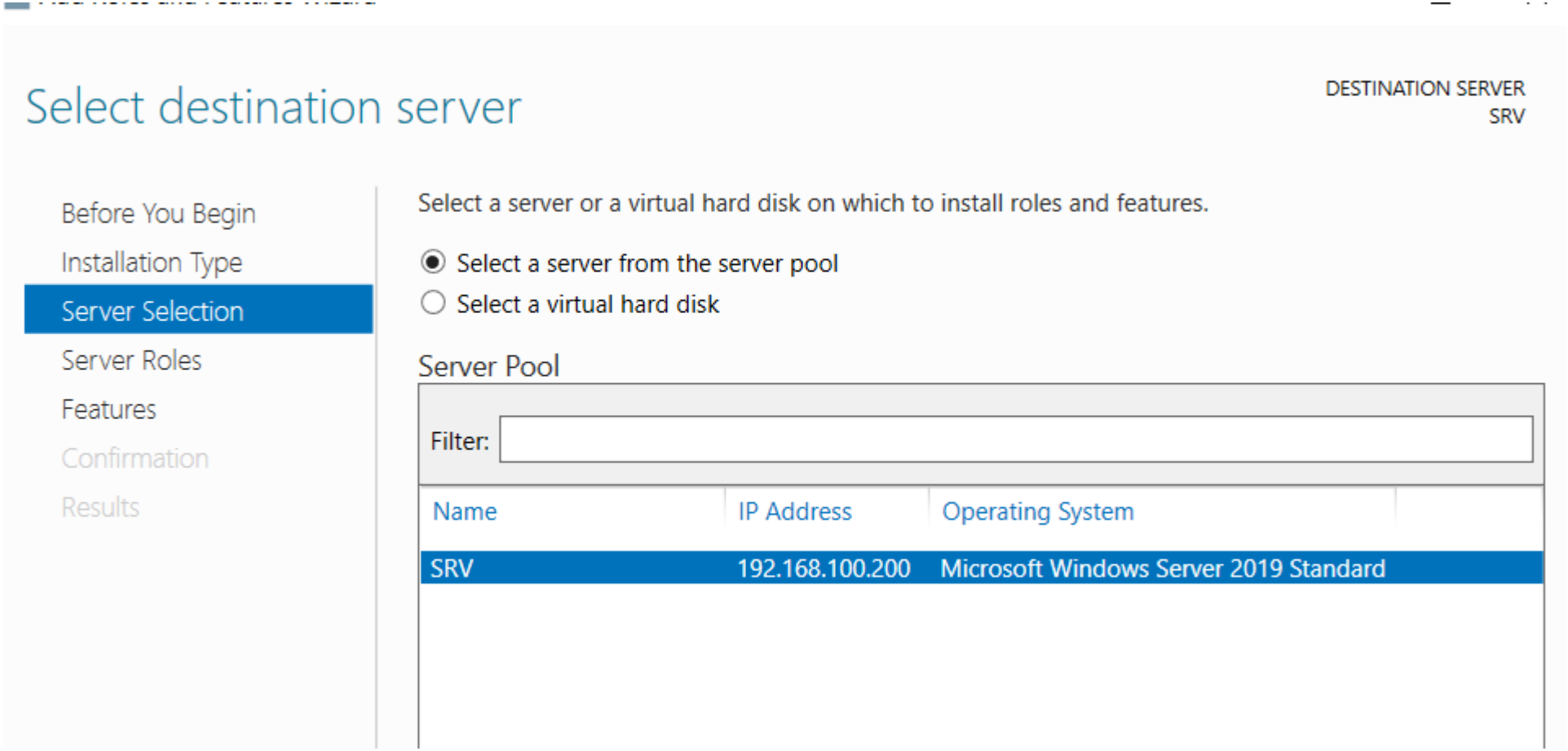
do wr

2. Выполните настройку второго уровня DNS-системы стенда;

SRV

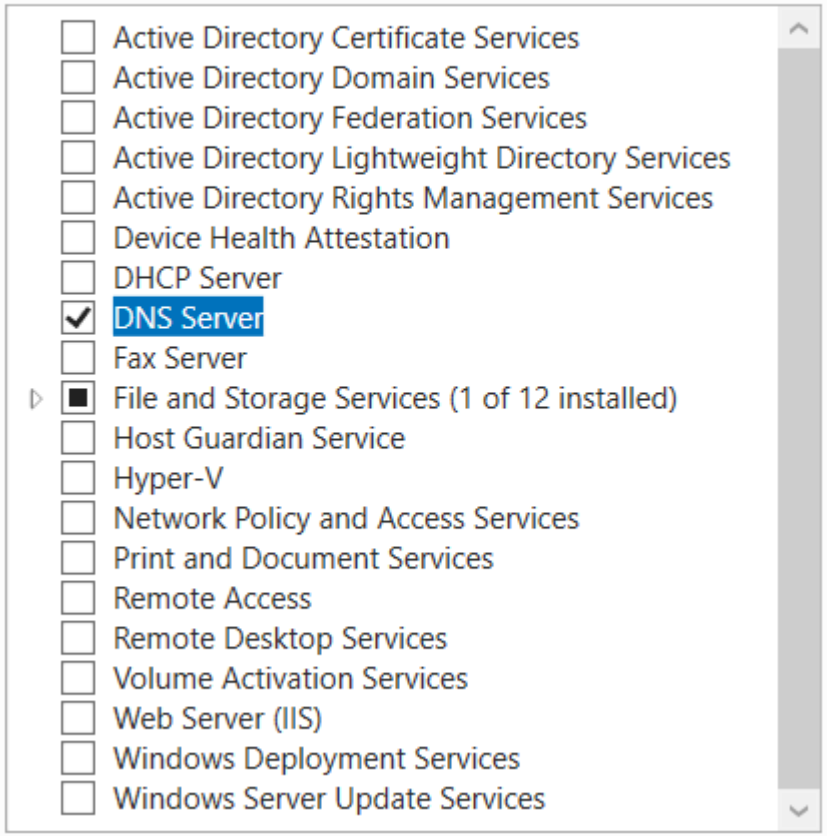


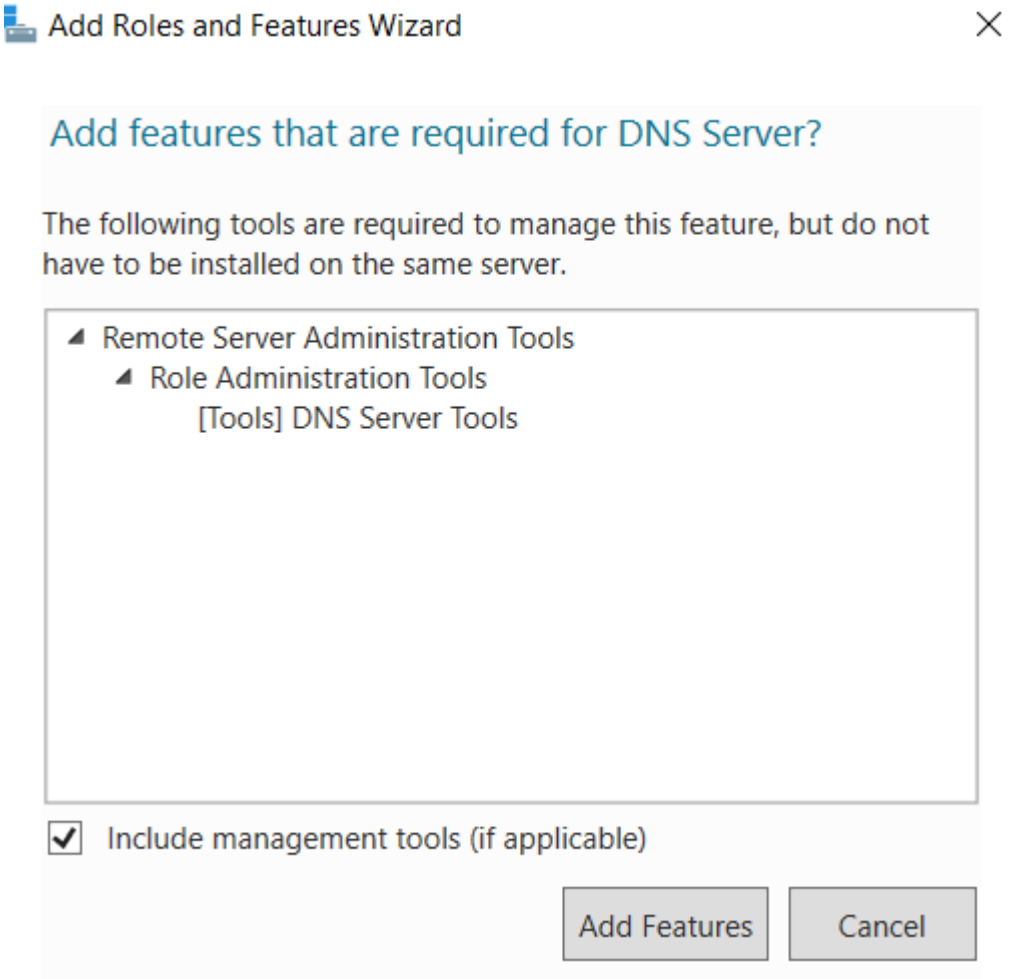

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.


Select destination server
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
SRV
192.168.100.200
Microsoft Windows Server 2019 Standard

Select one or more roles to install on the selected server.

Roles




Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
SRV

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- DNS Server
- Confirmation
- Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

DNS Server

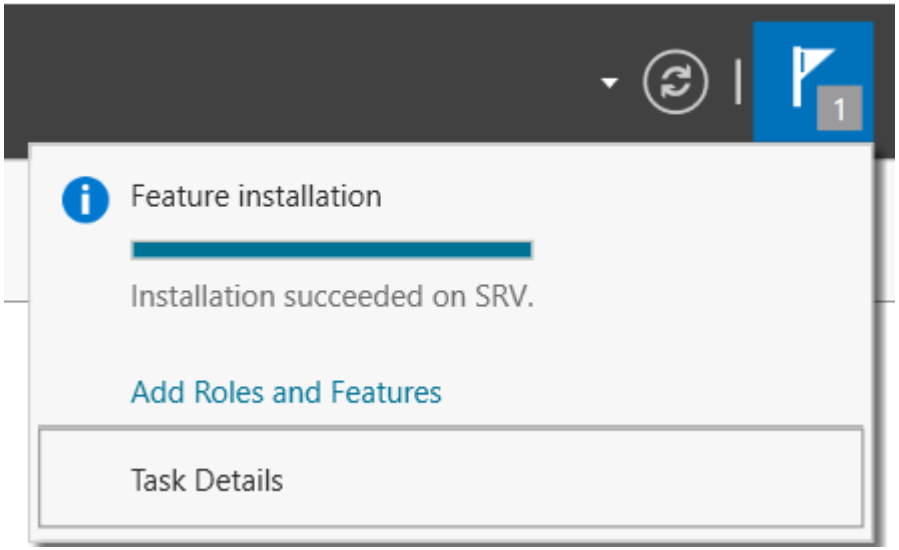
Remote Server Administration Tools

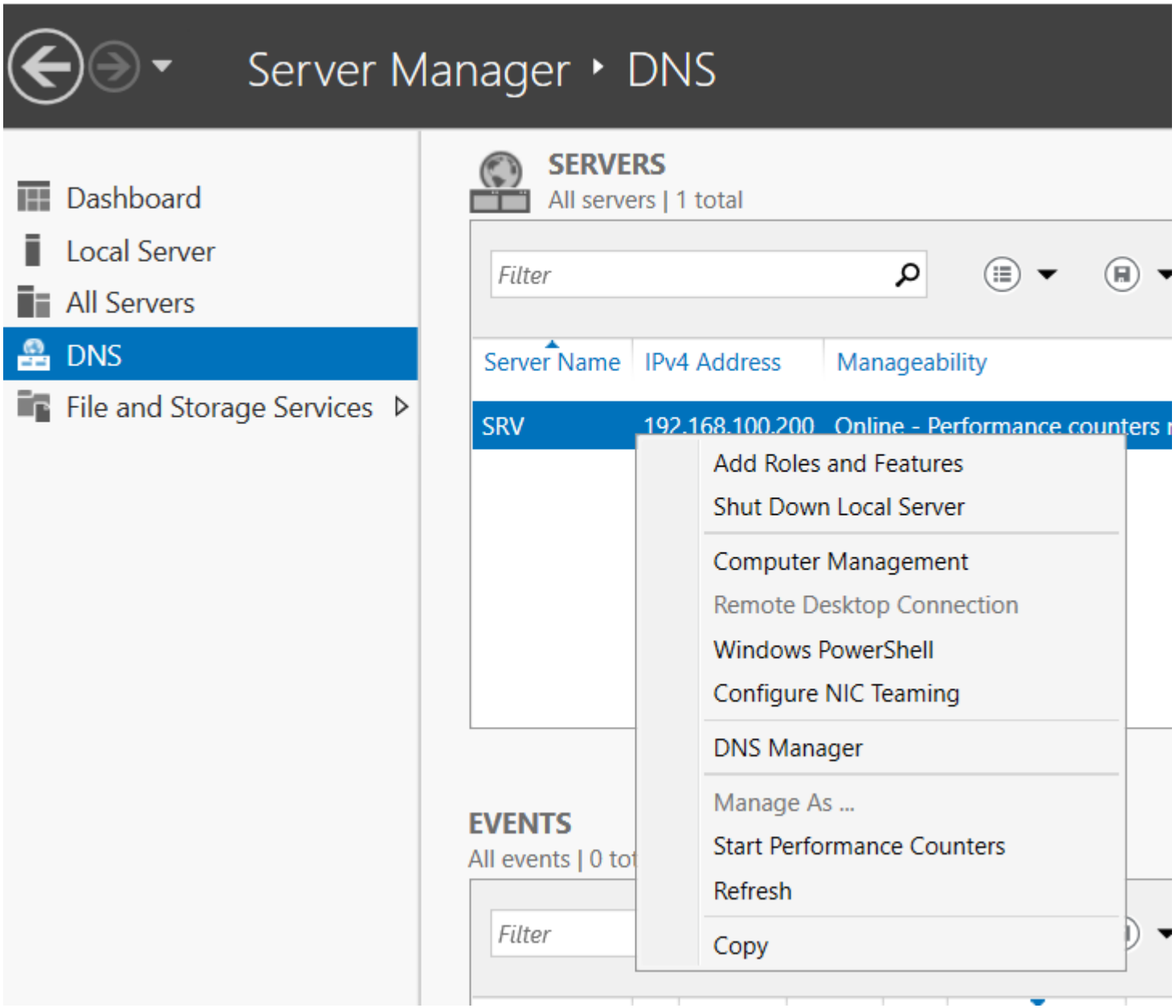
Role Administration Tools

DNS Server Tools

Export configuration settings
Specify an alternate source path

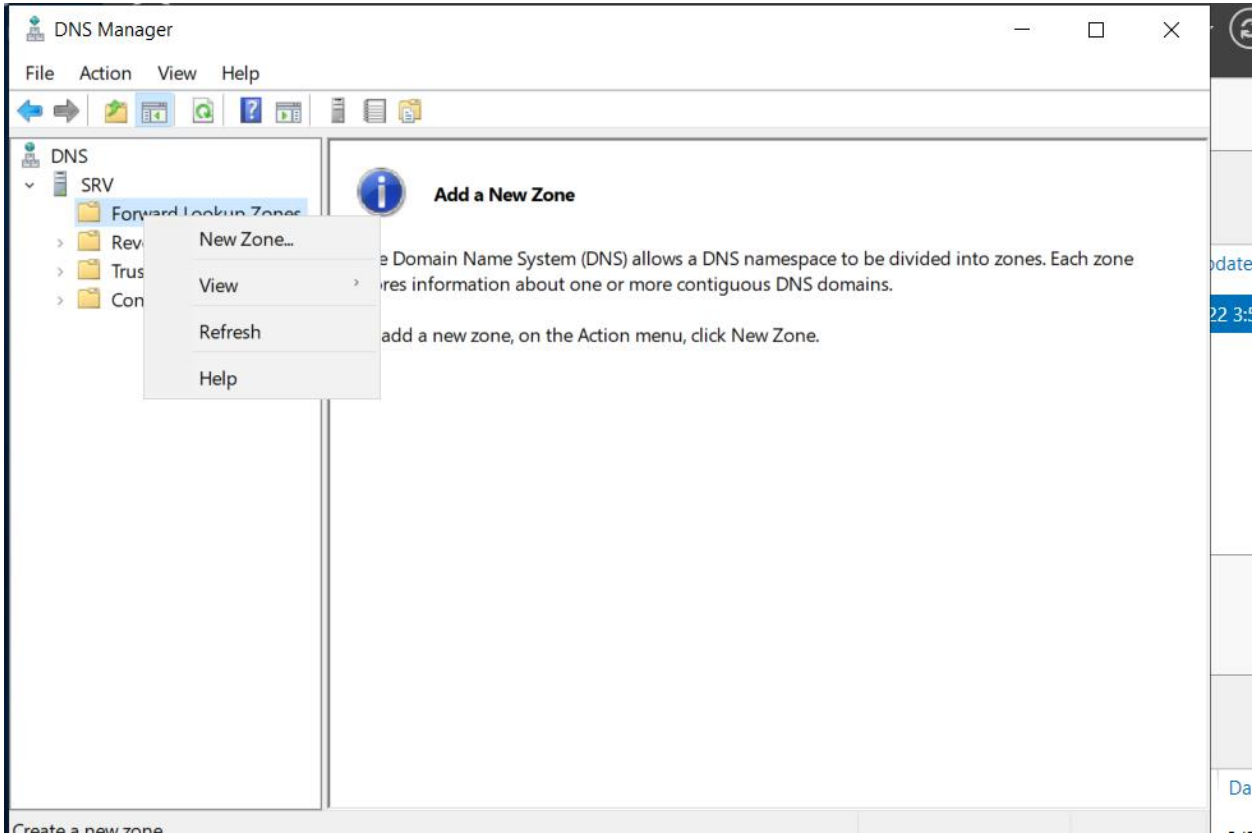
< Previous | Next > | Install | Cancel

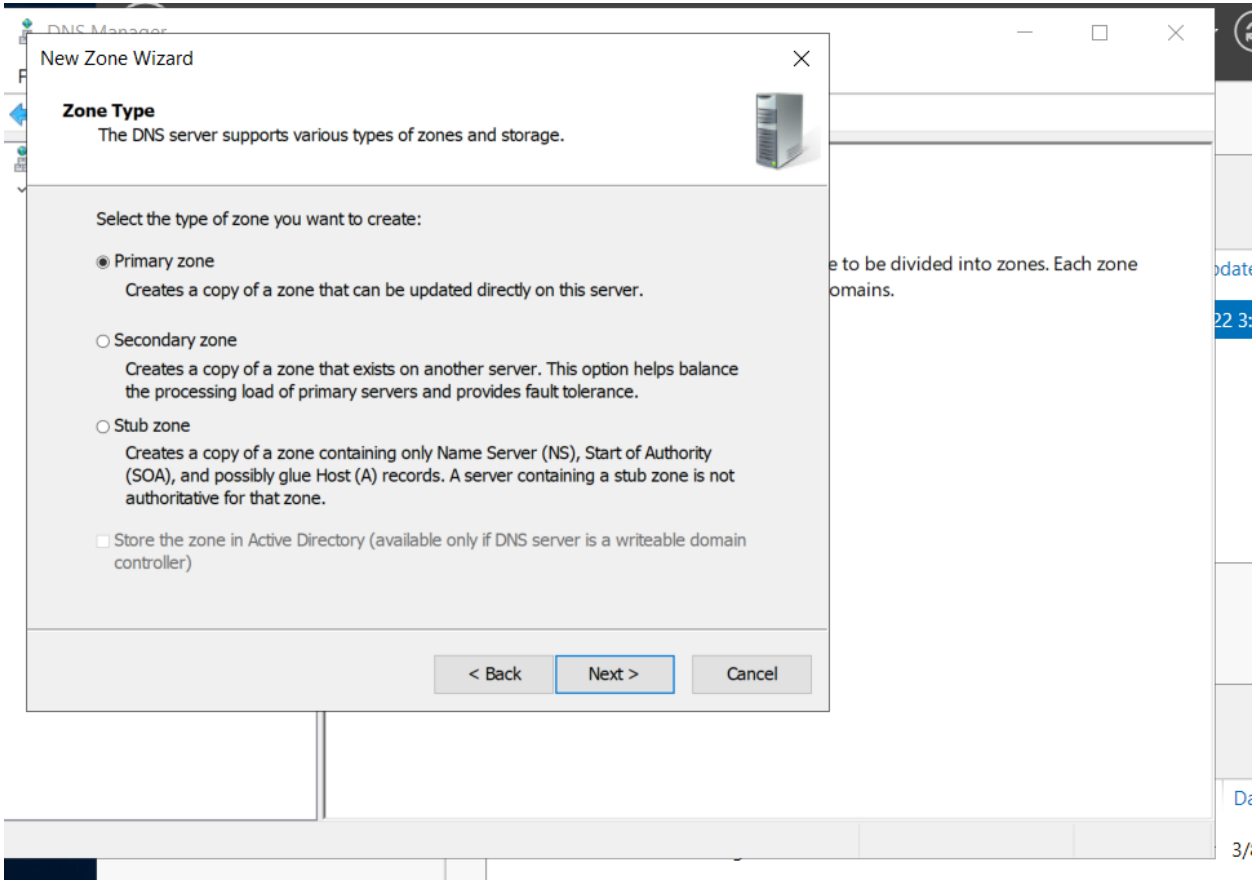

1
Feature installation
Installation succeeded on SRV.
Add Roles and Features
Task Details

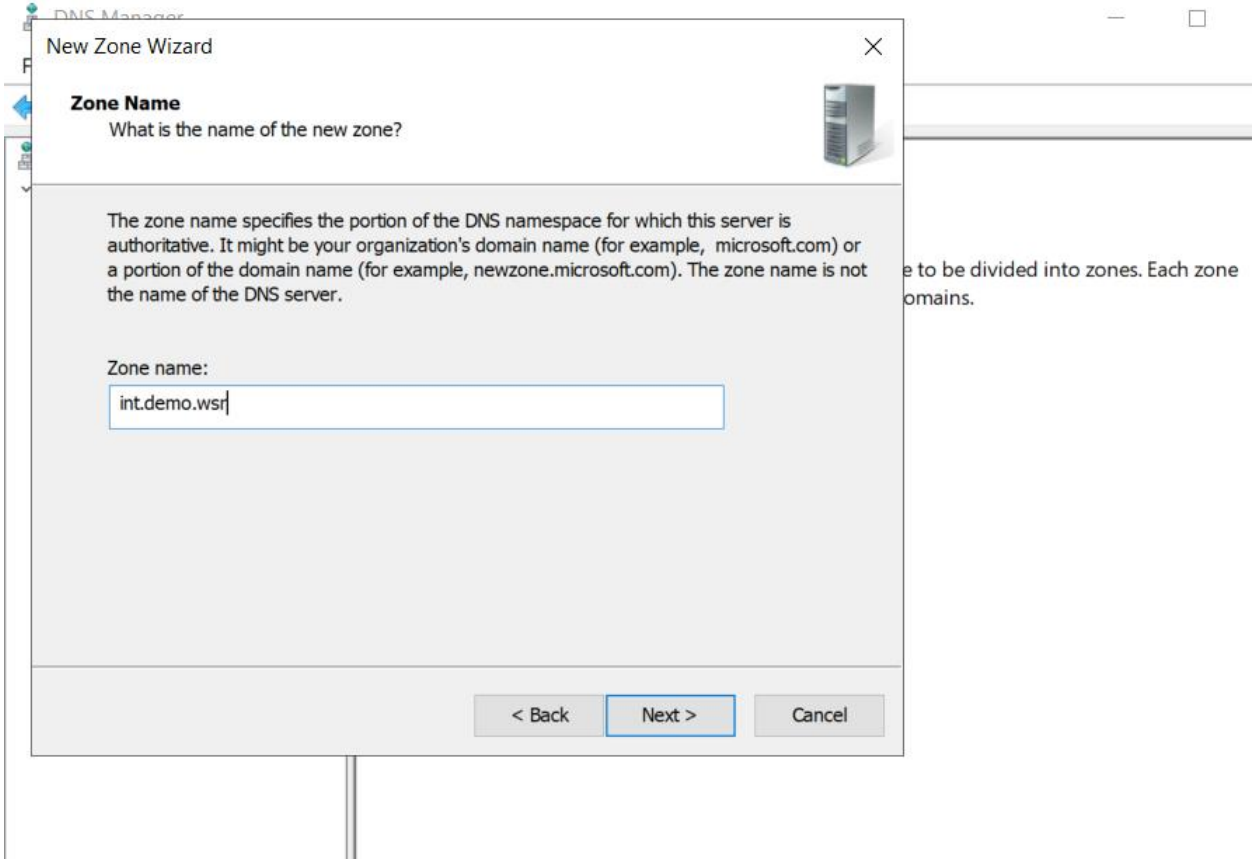


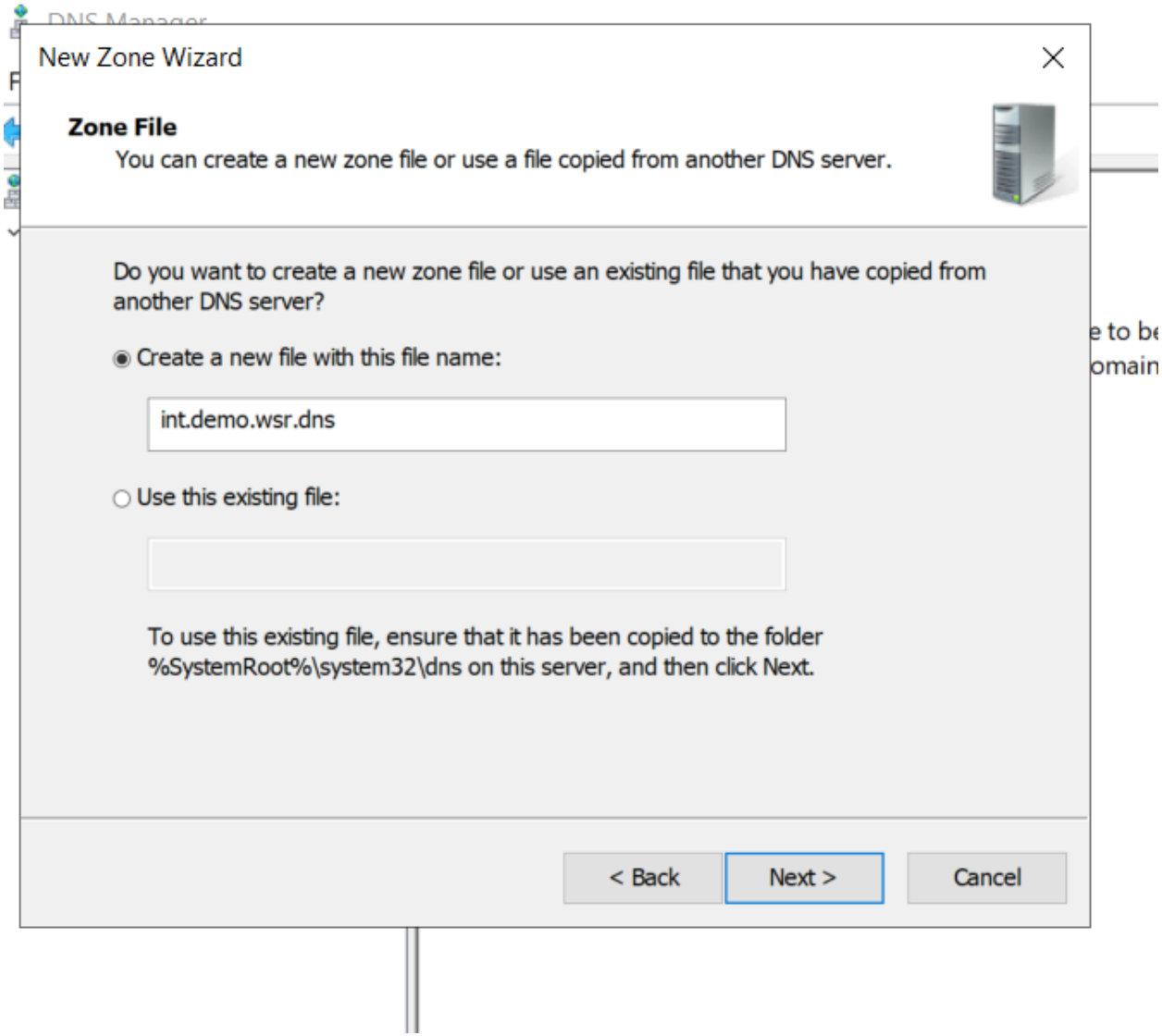
Выбрать “DNS Manager”

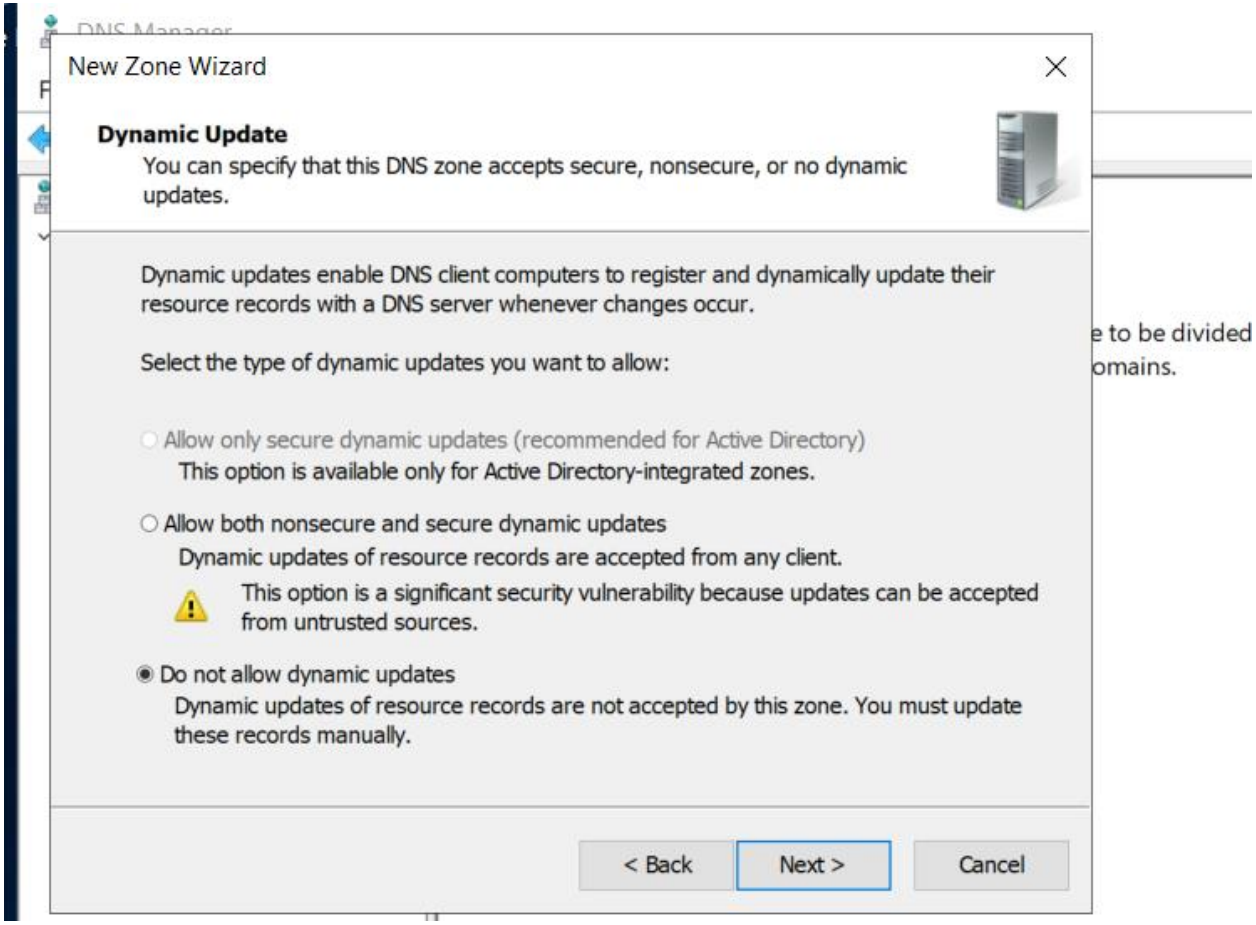
Правой клавишей на Forward Lookup Zones = > New Zone

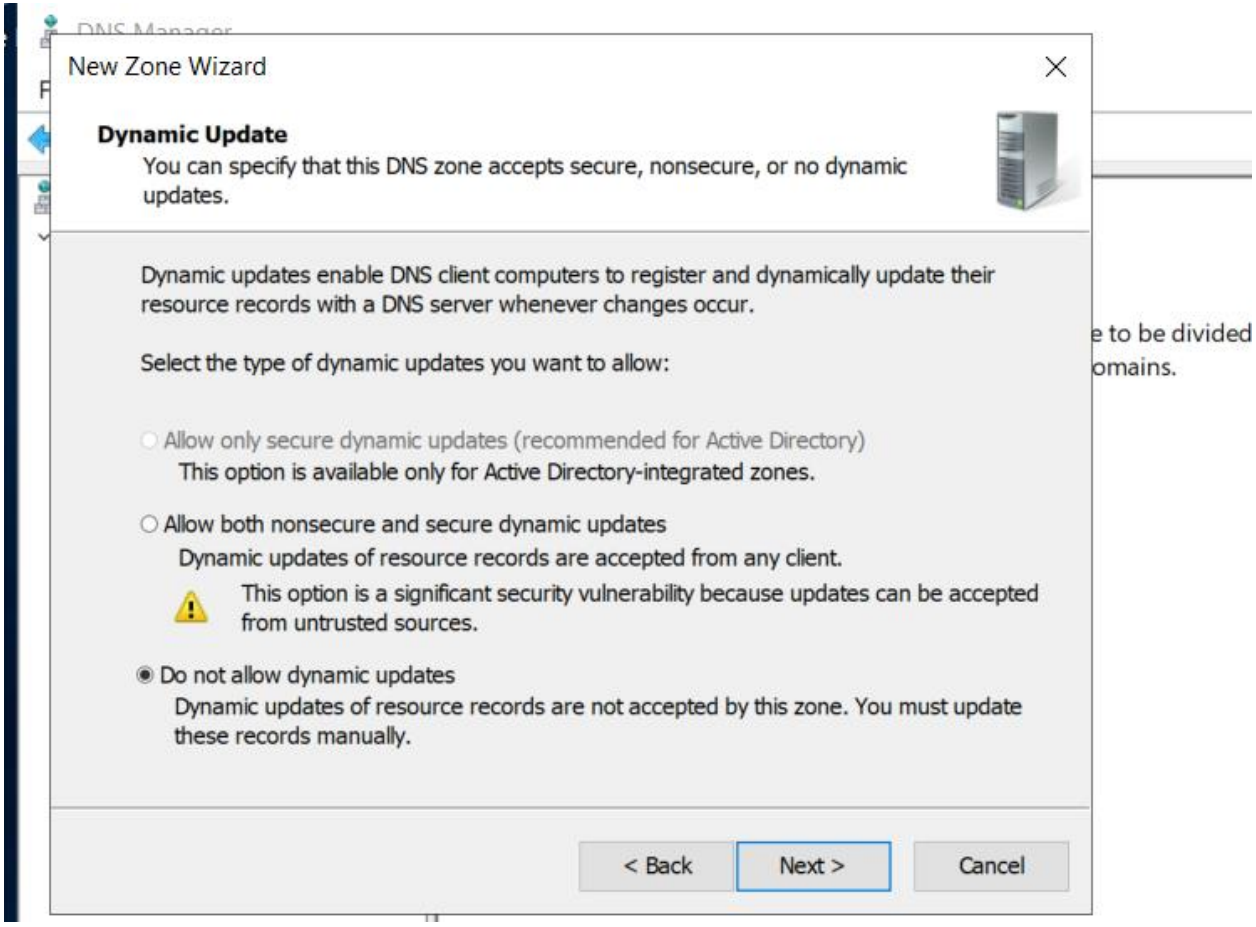



DNS Manager
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
e to be divided into zones. Each zone
omains.


New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
int.demo.wsr
< Back
Next >
Cancel

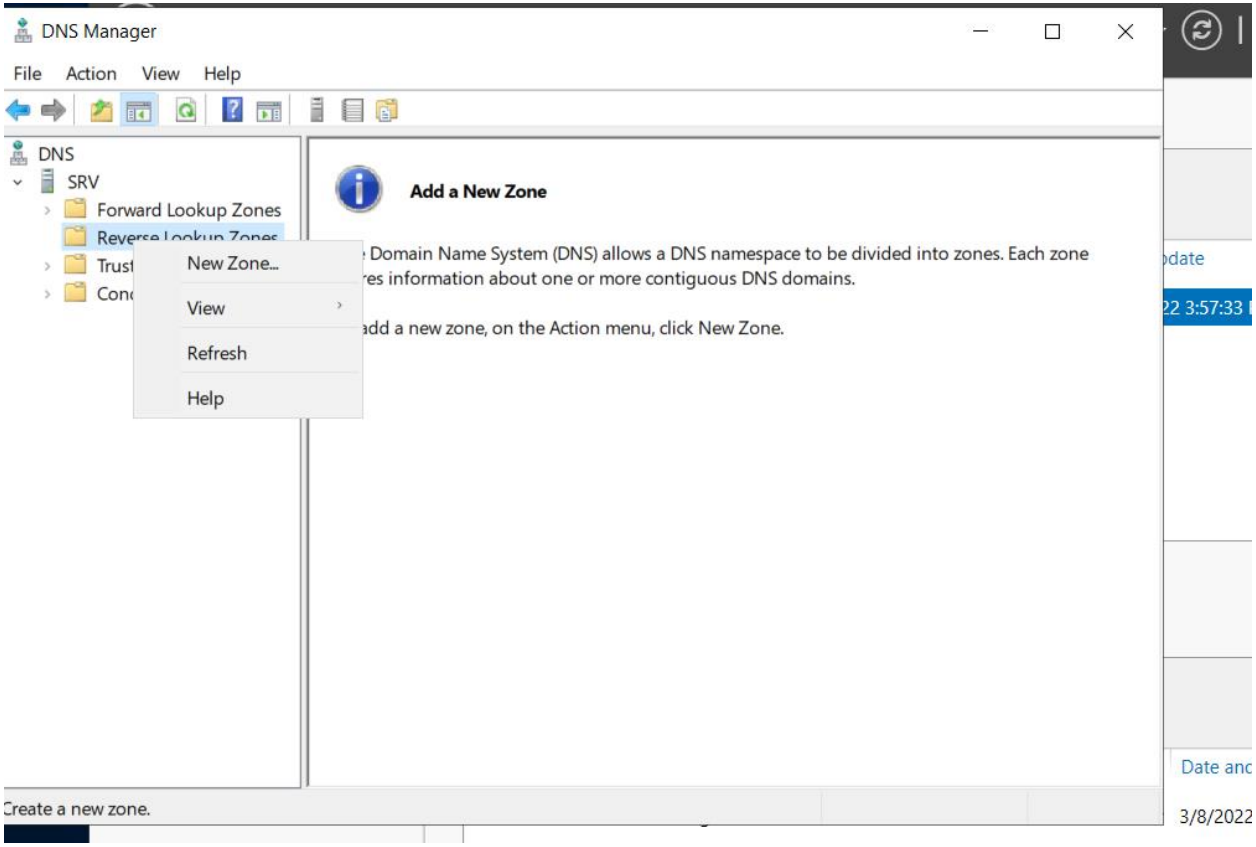

DNS Manager
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
int.demo.wsr.dns
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel

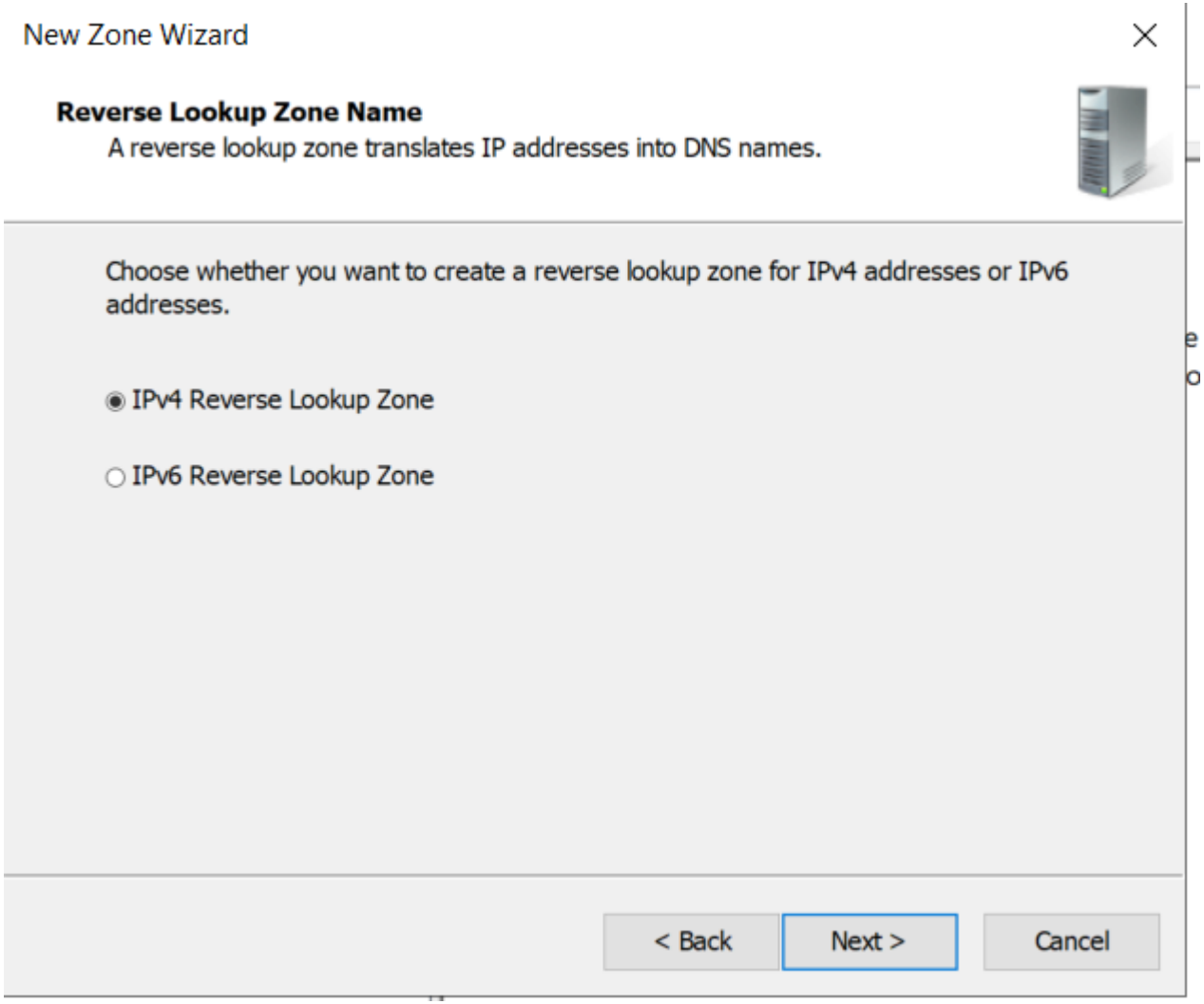

DNS Manager
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
e to be divided
omains.

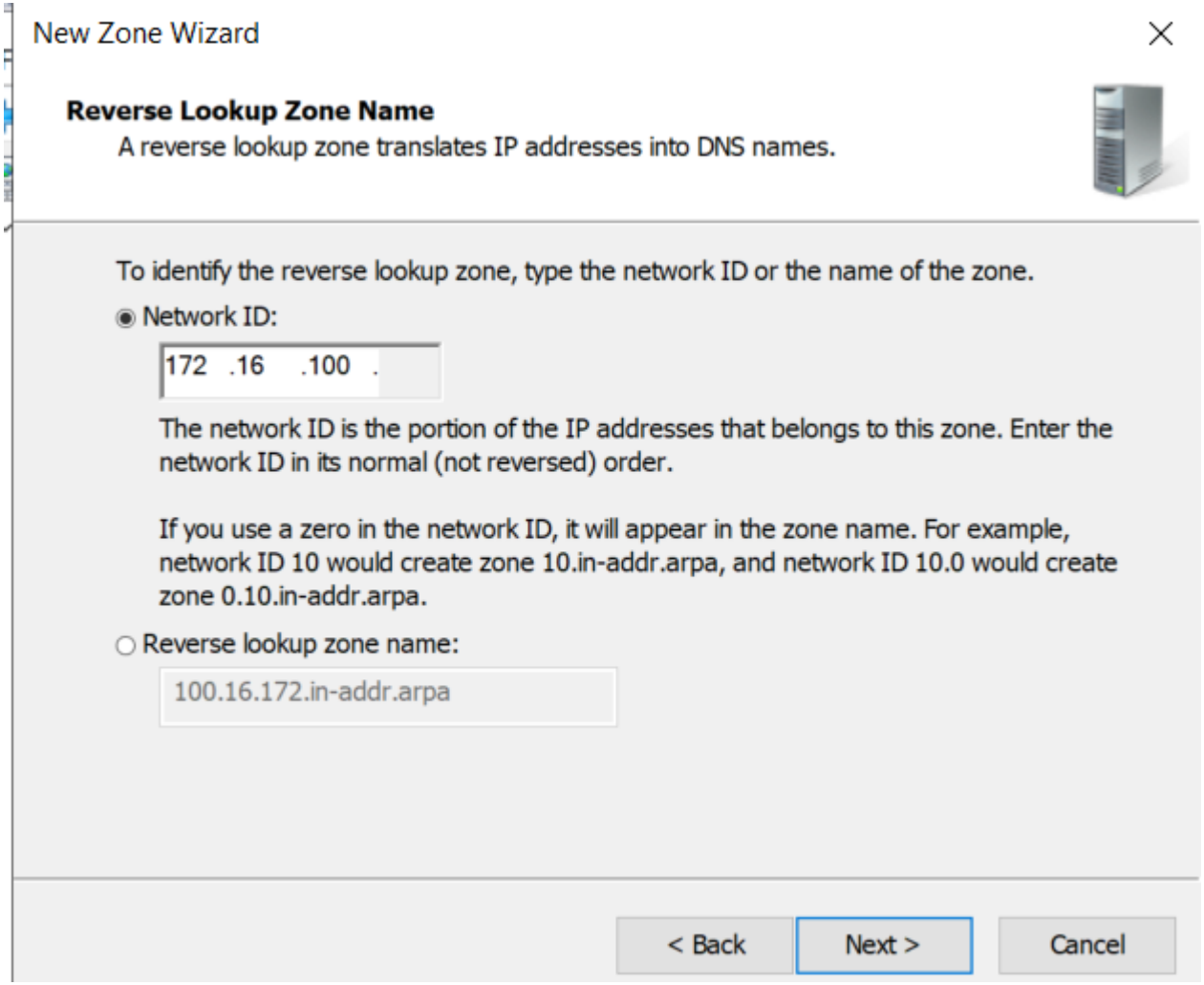

DNS Manager
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
e to be divided
omains.

Создать две зоны обратного просмотра

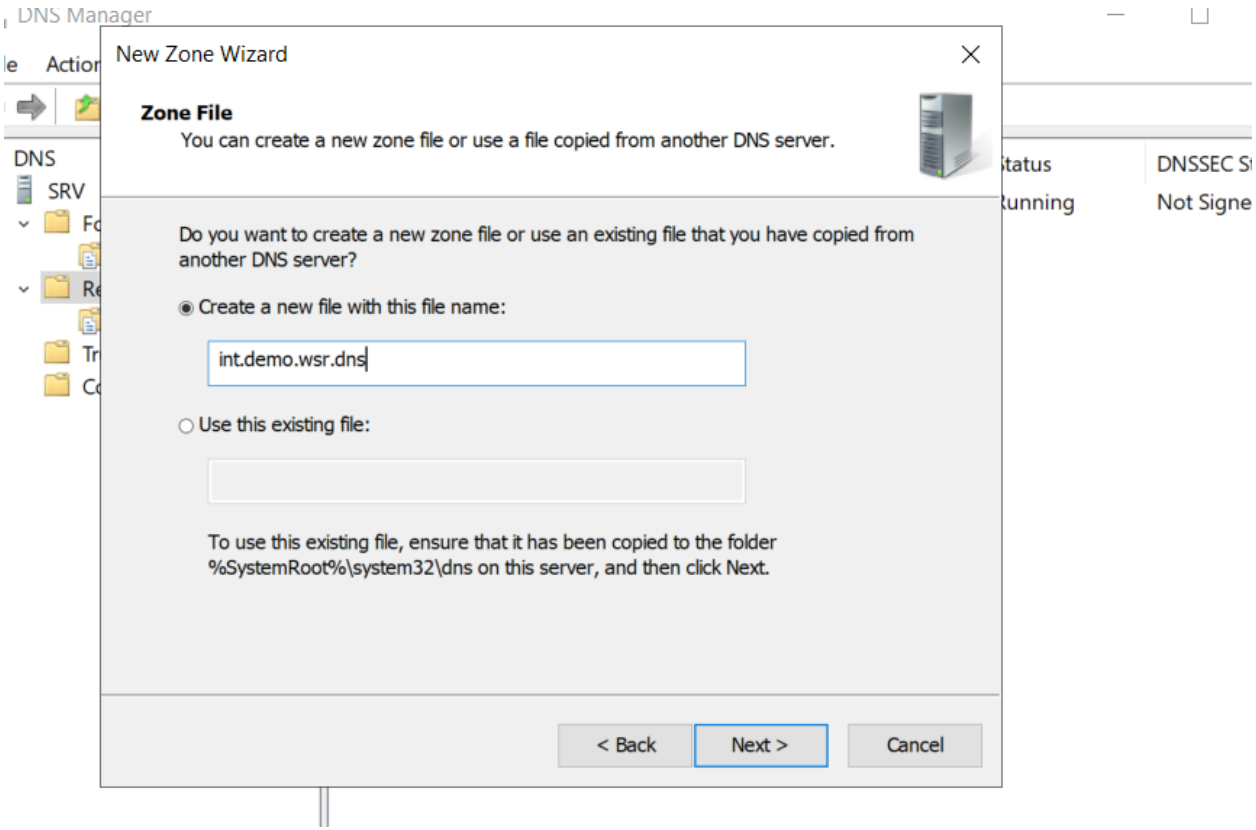
Правой клавишей на “Reverse Lookup Zones” => New Zone

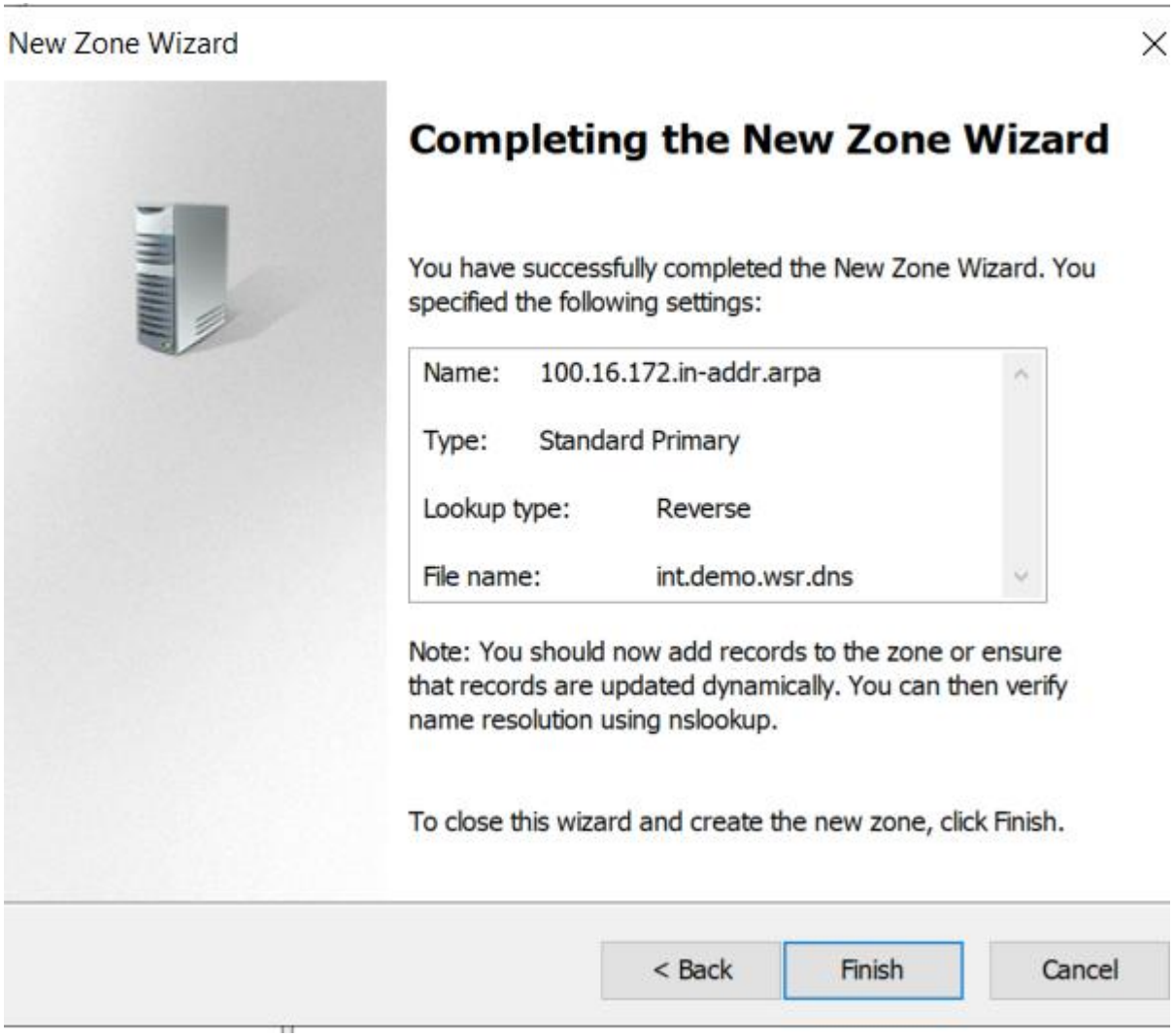



New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.
IPv4 Reverse Lookup Zone
IPv6 Reverse Lookup Zone
< Back
Next >
Cancel

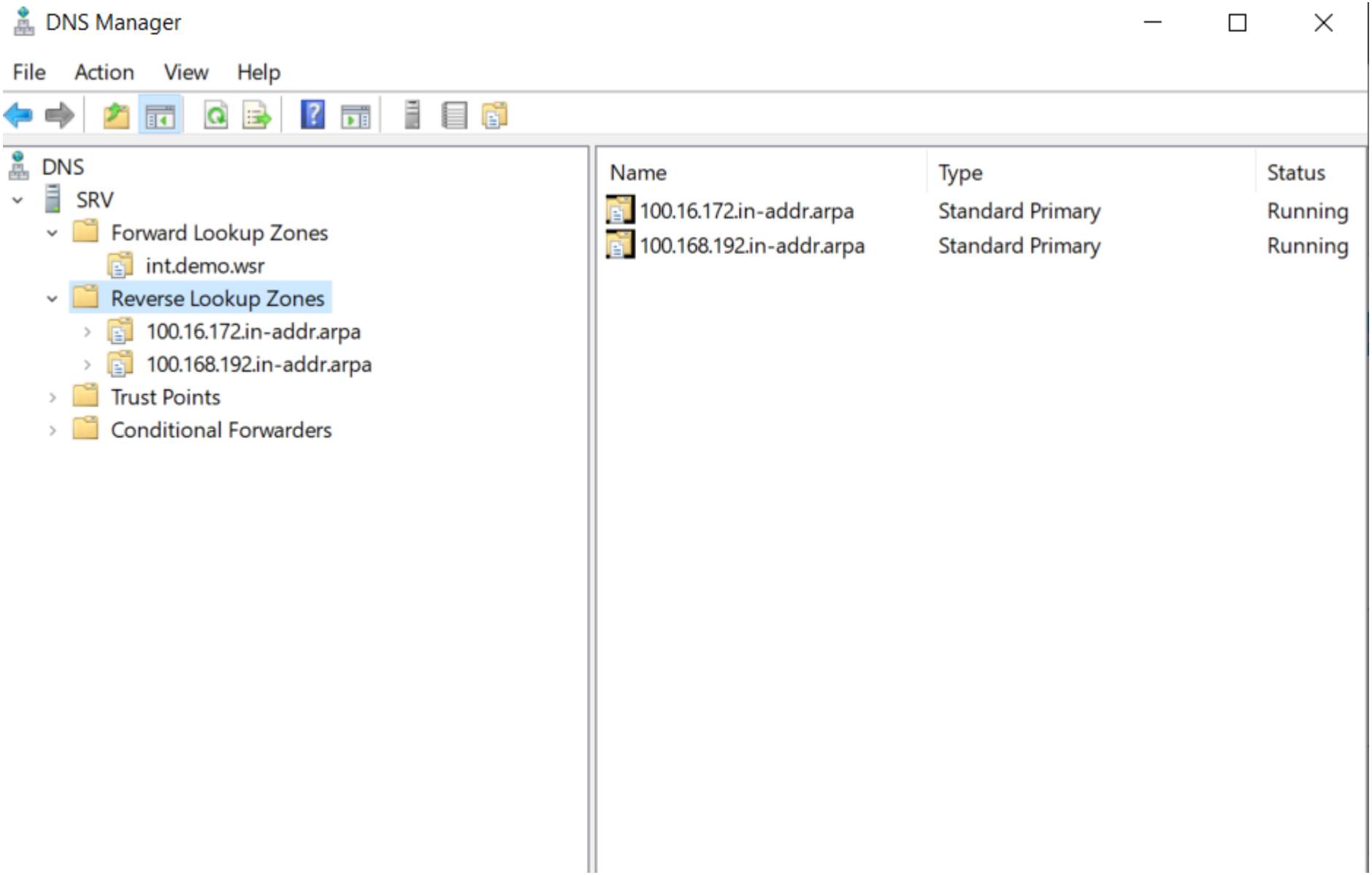


Изменить название файла


DNS Manager
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
int.demo.wsr.dns
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
DNS
SRV
Status
DNSSEC
Running
Not Signe



Аналогично для 192.168.100.0/24

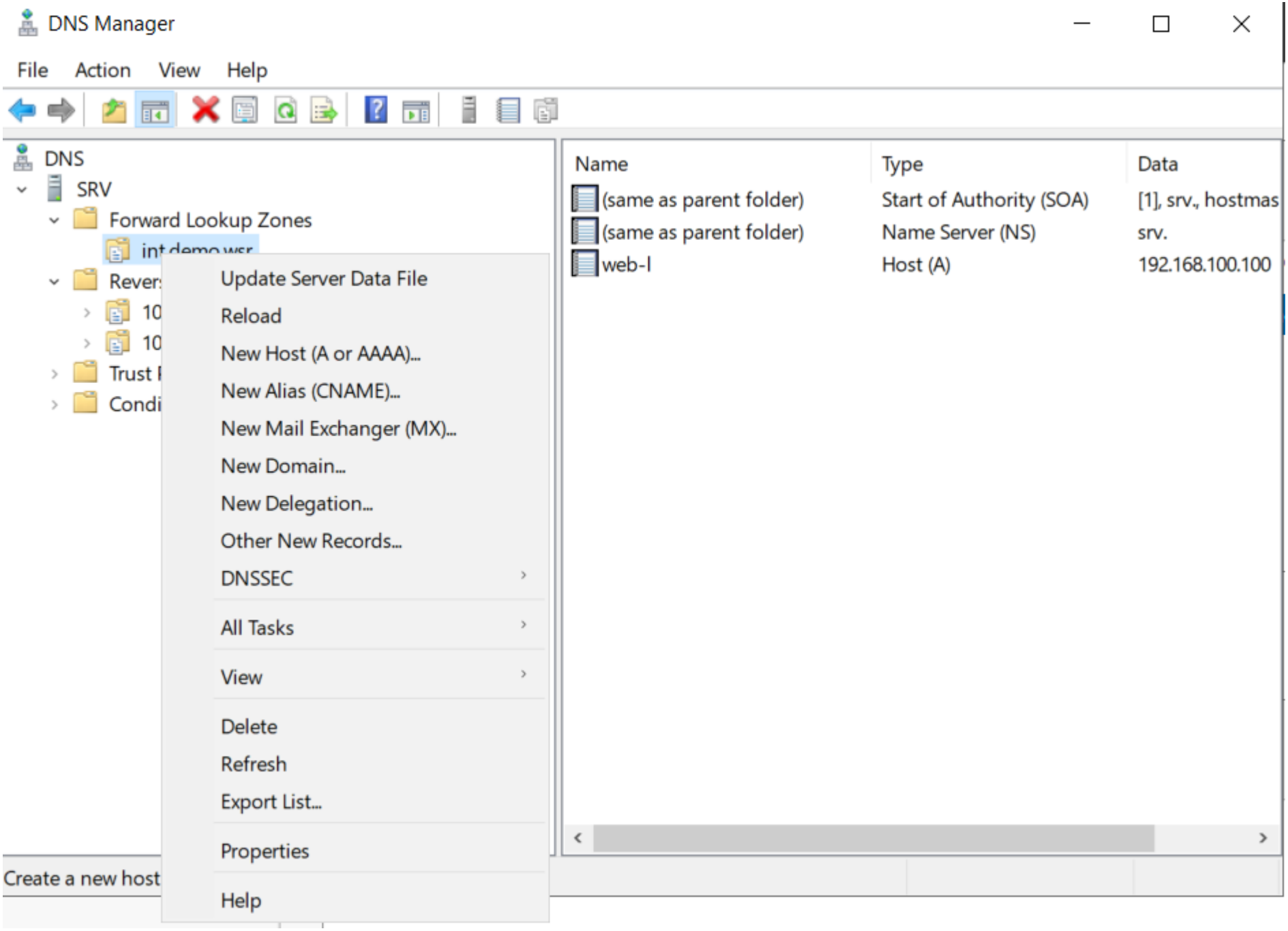

DNS Manager
File
Action
View
Help
DNS
SRV
Forward Lookup Zones
int.demo.wsr
Reverse Lookup Zones
100.16.172.in-addr.arpa
100.168.192.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
Status
100.16.172.in-addr.arpa
Standard Primary
Running
100.168.192.in-addr.arpa
Standard Primary
Running

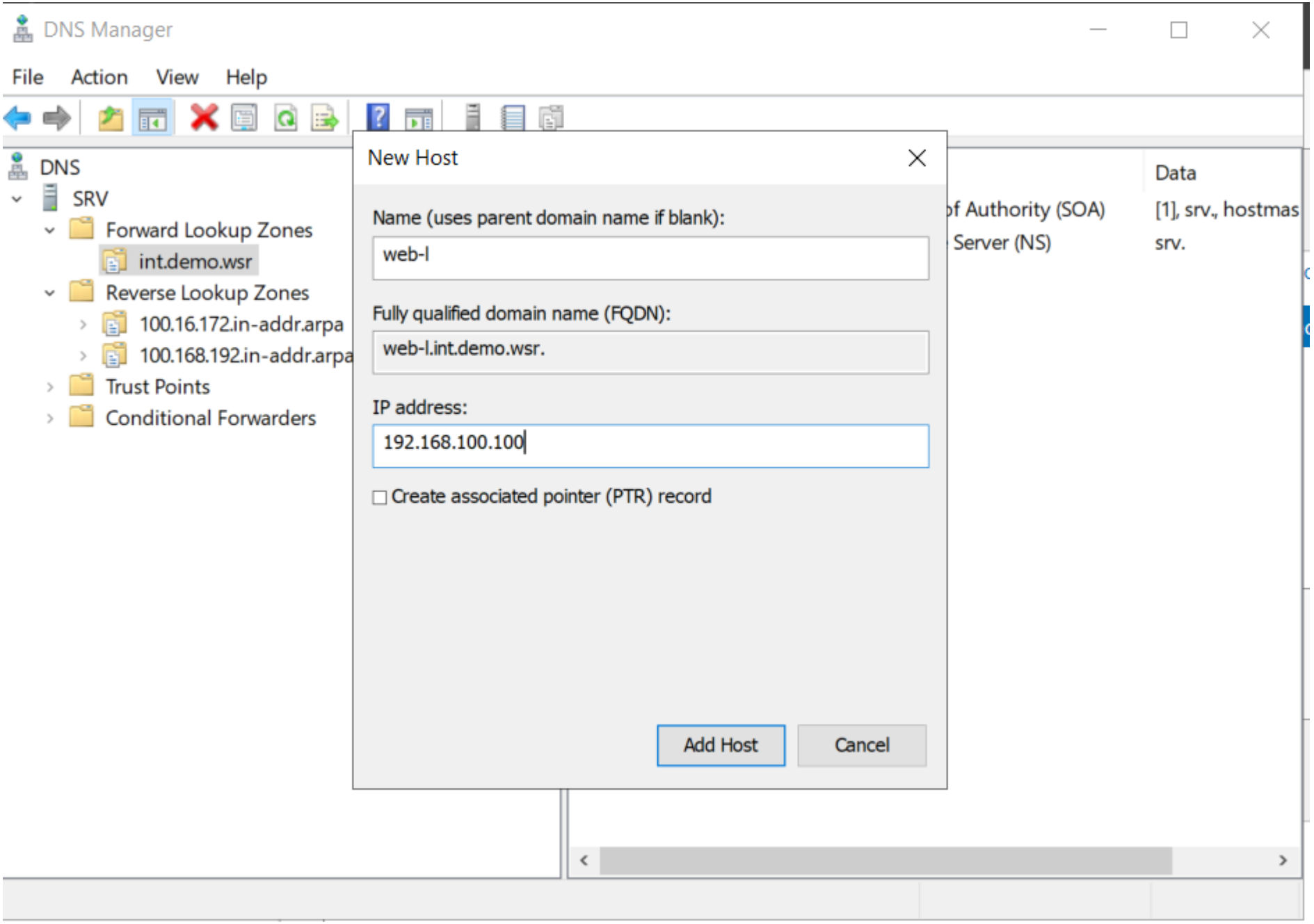
Тоже, но используя PowerShell

```
Install-WindowsFeature -Name DNS -IncludeManagementTools
Add-DnsServerPrimaryZone -Name "int.demo.wsr" -ZoneFile "int.demo.wsr.dns"
Add-DnsServerPrimaryZone -NetworkId 192.168.100.0/24 -ZoneFile "int.demo.wsr.dns"
Add-DnsServerPrimaryZone -NetworkId 172.16.100.0/24 -ZoneFile "int.demo.wsr.dns"
```

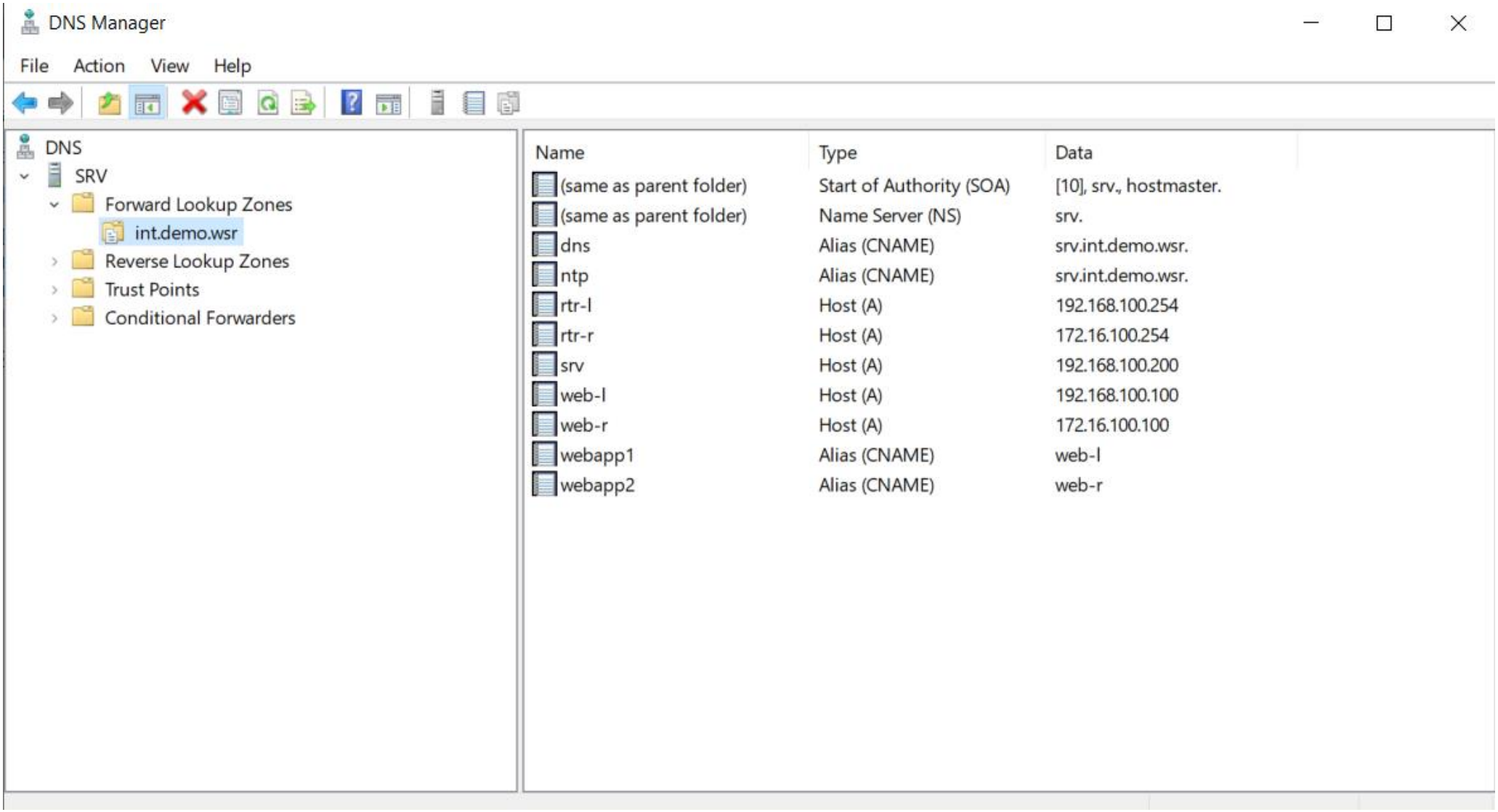
Zone	Type	Key	Meaning
int.demo.wsr	A	web-l	192.168.100.100
	A	web-r	172.16.100.100
	A	srv	192.168.100.200
	A	rtr-l	192.168.100.254
	A	rtr-r	172.16.100.254
	CNAME	webapp1	web-l
	CNAME	webapp2	web-r
	CNAME	ntp	srv
	CNAME	dns	srv

Добавляем записи в соответствии с таблицей

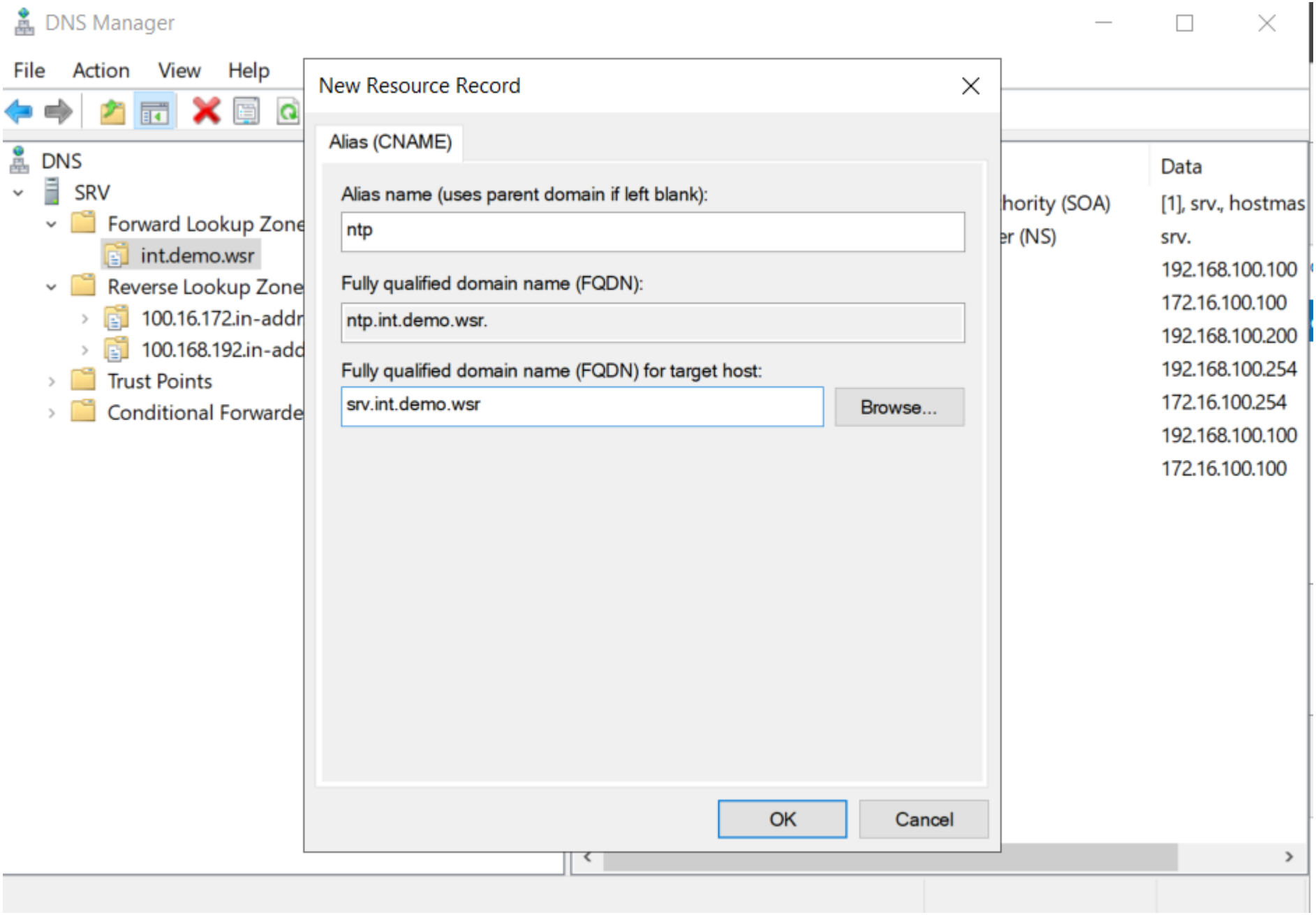

DNS Manager
File
Action
View
Help
DNS
SRV
Forward Lookup Zones
Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...
New Delegation...
Other New Records...
DNSSEC
All Tasks
View
Delete
Refresh
Export List...
Properties
Help
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[1], srv., hostmas
(same as parent folder)
Name Server (NS)
srv.
web-I
Host (A)
192.168.100.100
Create a new host


DNS Manager
File
Action
View
Help
DNS
SRV
Forward Lookup Zones
int.demo.wsr
Reverse Lookup Zones
100.16.172.in-addr.arpa
100.168.192.in-addr.arpa
Trust Points
Conditional Forwarders
Data
of Authority (SOA)
[1], srv., hostmas
Server (NS)
srv.
New Host
Name (uses parent domain name if blank):
web-l
Fully qualified domain name (FQDN):
web-l.int.demo.wsr.
IP address:
192.168.100.100
Create associated pointer (PTR) record
Add Host
Cancel

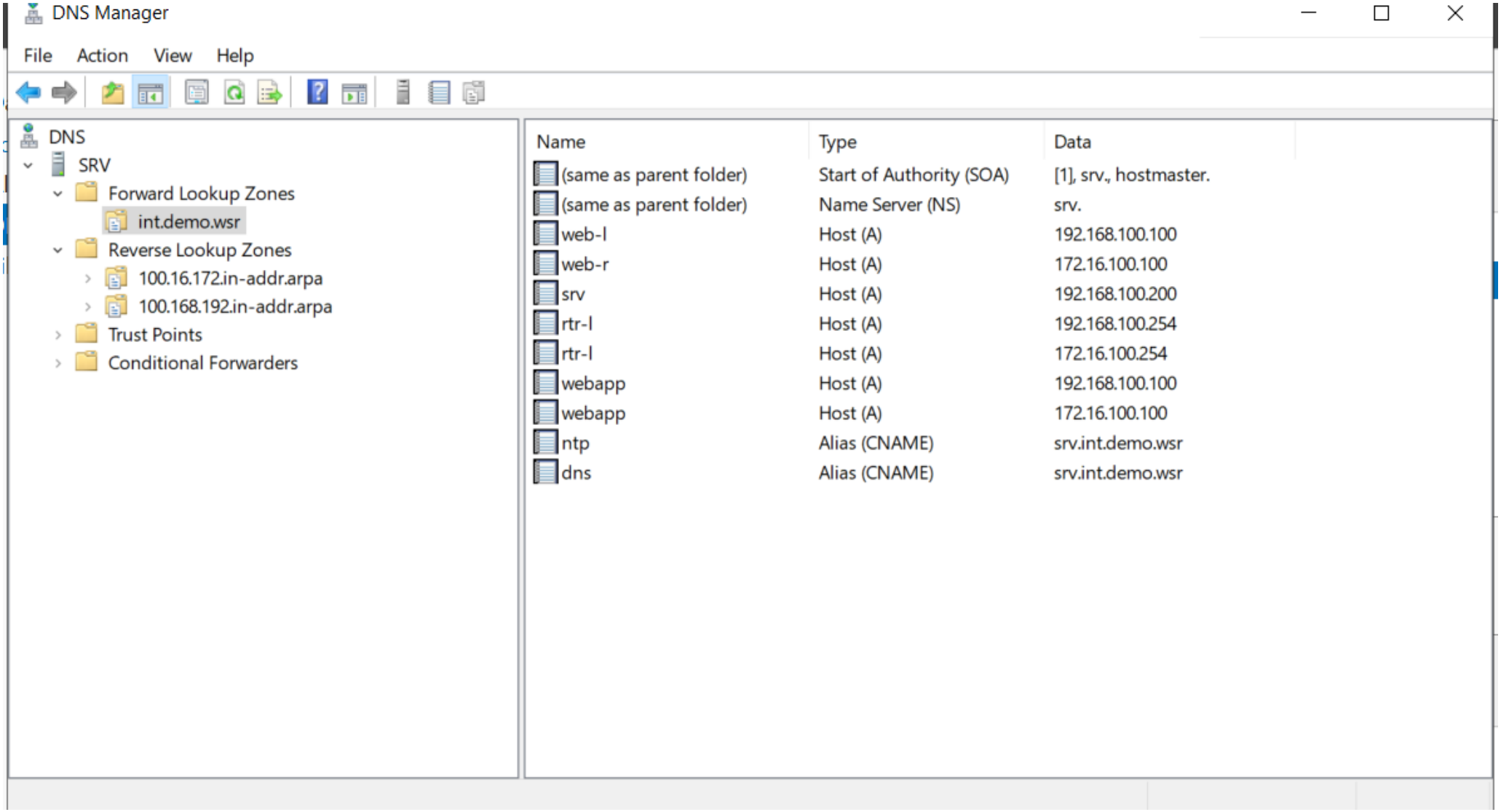
Аналогично добавить все записи A



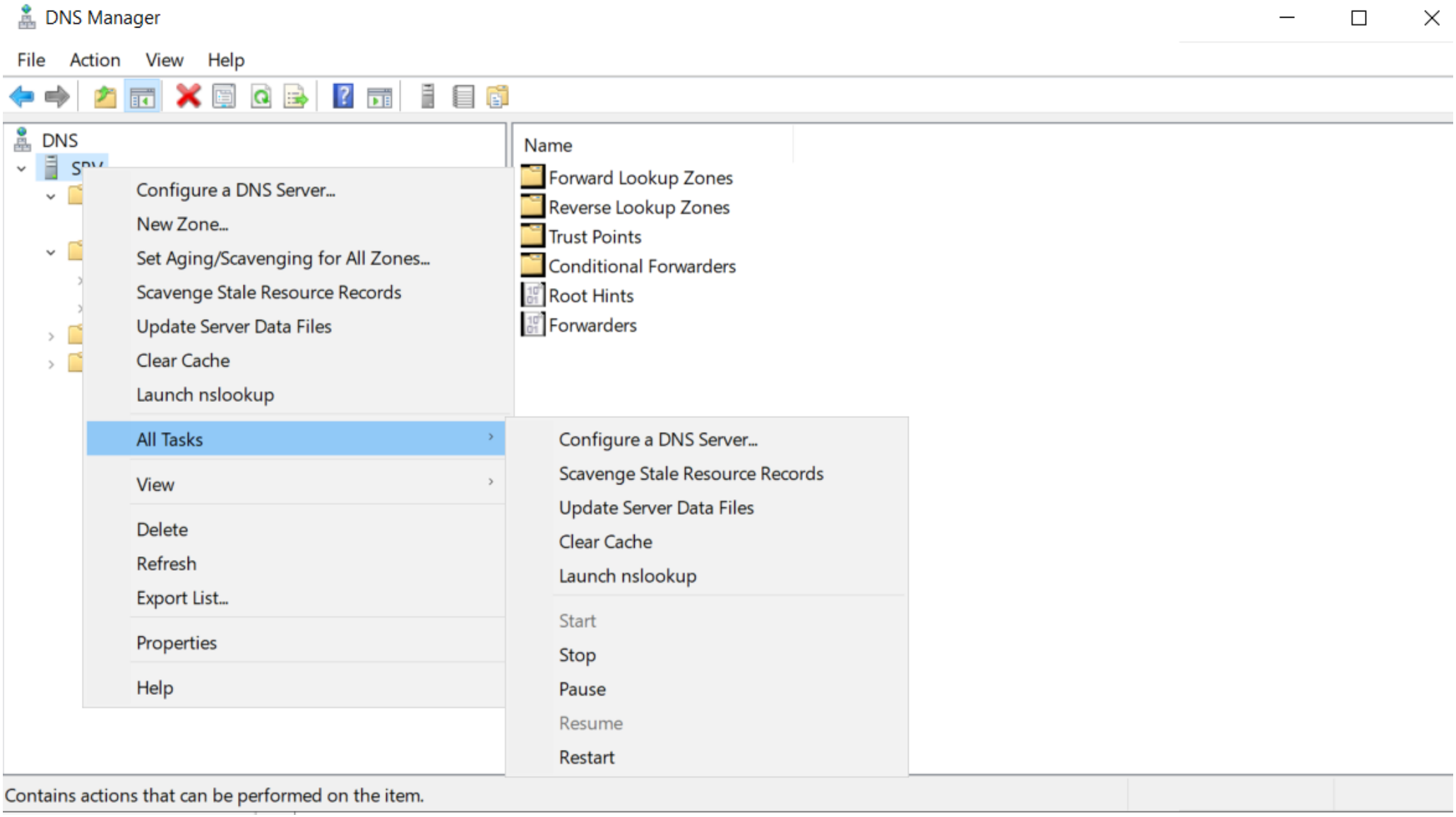
Далее делаем записи CNAME


DNS Manager
File
Action
View
Help
DNS
SRV
Forward Lookup Zone
int.demo.wsr
Reverse Lookup Zone
100.16.172.in-addr
100.168.192.in-add
Trust Points
Conditional Forwarde
New Resource Record
Alias (CNAME)
Alias name (uses parent domain if left blank):
ntp
Fully qualified domain name (FQDN):
ntp.int.demo.wsr.
Fully qualified domain name (FQDN) for target host:
srv.int.demo.wsr
Browse...
OK
Cancel
Data
hority (SOA)
er (NS)
[1], srv., hostmas
srv.
192.168.100.100
172.16.100.100
192.168.100.200
192.168.100.254
172.16.100.254
192.168.100.100
172.16.100.100

Итого


DNS Manager
File Action View Help
DNS
SRV
Forward Lookup Zones
int.demo.wsr
Reverse Lookup Zones
100.16.172.in-addr.arpa
100.168.192.in-addr.arpa
Trust Points
Conditional Forwarders
Name Type Data
(same as parent folder) Start of Authority (SOA) [1], srv., hostmaster.
(same as parent folder) Name Server (NS) srv.
web-l Host (A) 192.168.100.100
web-r Host (A) 172.16.100.100
srv Host (A) 192.168.100.200
rtr-l Host (A) 192.168.100.254
rtr-l Host (A) 172.16.100.254
webapp Host (A) 192.168.100.100
webapp Host (A) 172.16.100.100
ntp Alias (CNAME) srv.int.demo.wsr
dns Alias (CNAME) srv.int.demo.wsr

Перезапустить DNS



Тоже самое с помощью PowerShell

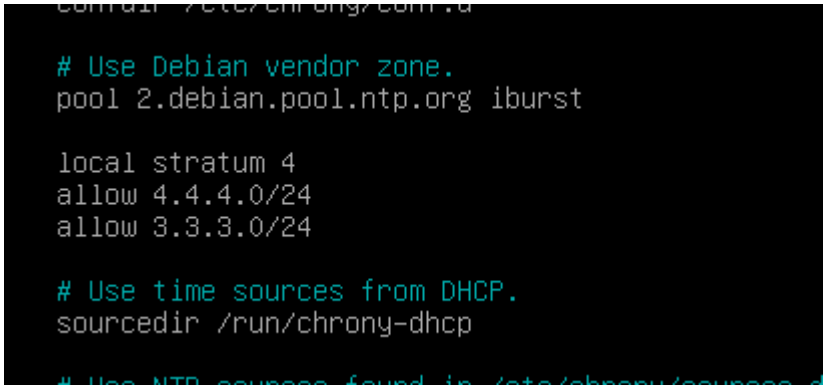
```
Add-DnsServerResourceRecordA -Name "web-l" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "192.168.100.100" -CreatePtr
Add-DnsServerResourceRecordA -Name "web-r" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "172.16.100.100" -CreatePtr
Add-DnsServerResourceRecordA -Name "srv" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "192.168.100.200" -CreatePtr
Add-DnsServerResourceRecordA -Name "rtr-l" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "192.168.100.254" -CreatePtr
Add-DnsServerResourceRecordA -Name "rtr-r" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "172.16.100.254" -CreatePtr
```

```
Add-DnsServerResourceRecordCName -Name "webapp1" -HostNameAlias "web-l.int.demo.wsr" -ZoneName "int.demo.wsr"
Add-DnsServerResourceRecordCName -Name "webapp2" -HostNameAlias "web-r.int.demo.wsr" -ZoneName "int.demo.wsr"
Add-DnsServerResourceRecordCName -Name "ntp" -HostNameAlias "srv.int.demo.wsr" -ZoneName "int.demo.wsr"
Add-DnsServerResourceRecordCName -Name "dns" -HostNameAlias "srv.int.demo.wsr" -ZoneName "int.demo.wsr"
```

3. Выполните настройку первого уровня системы синхронизации времени:

ISP NTP

```
apt install -y chrony
nano /etc/chrony/chrony.conf
local stratum 4
allow 4.4.4.0/24
allow 3.3.3.0/24
```



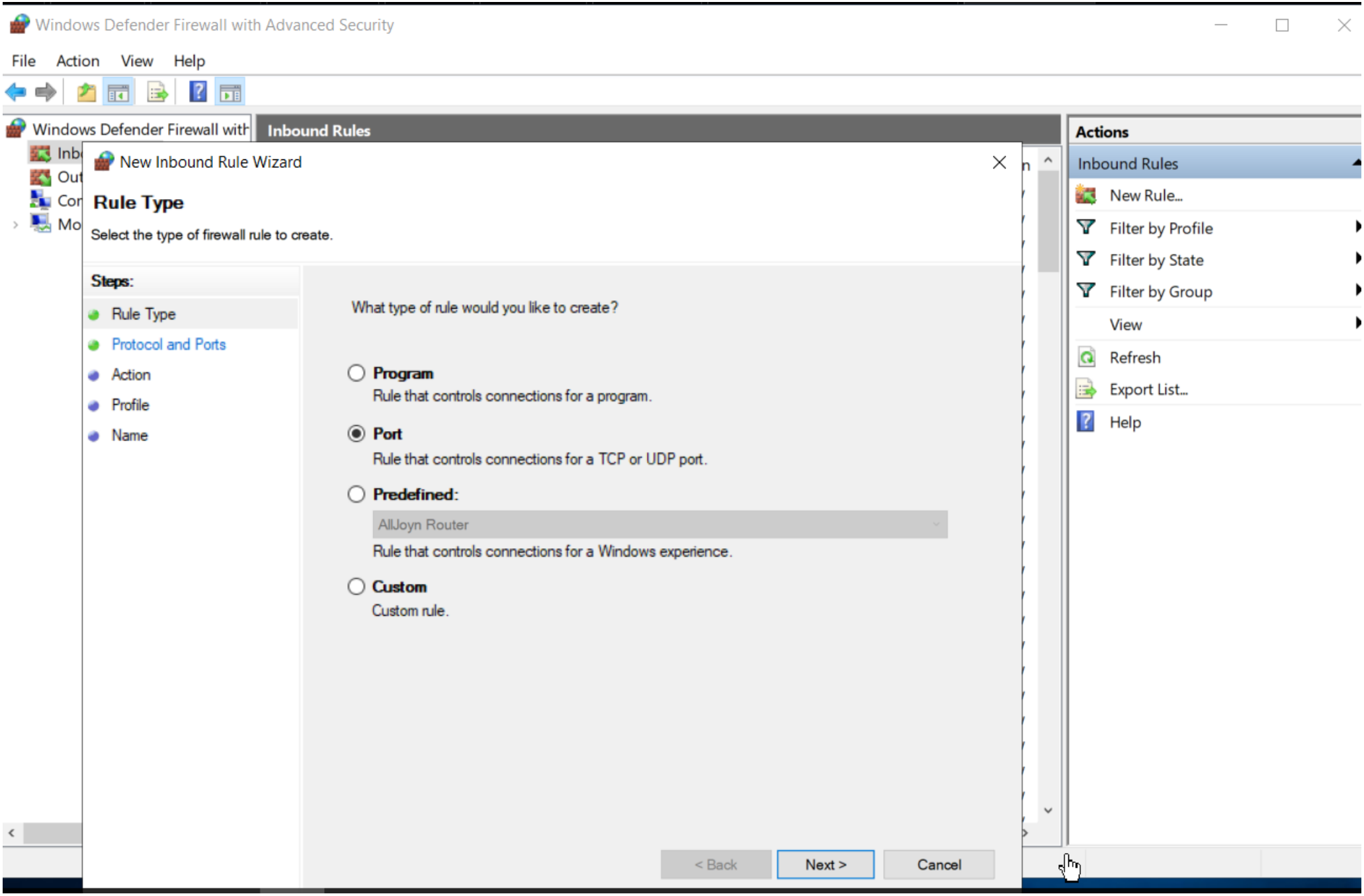
systemctl restart chronyd

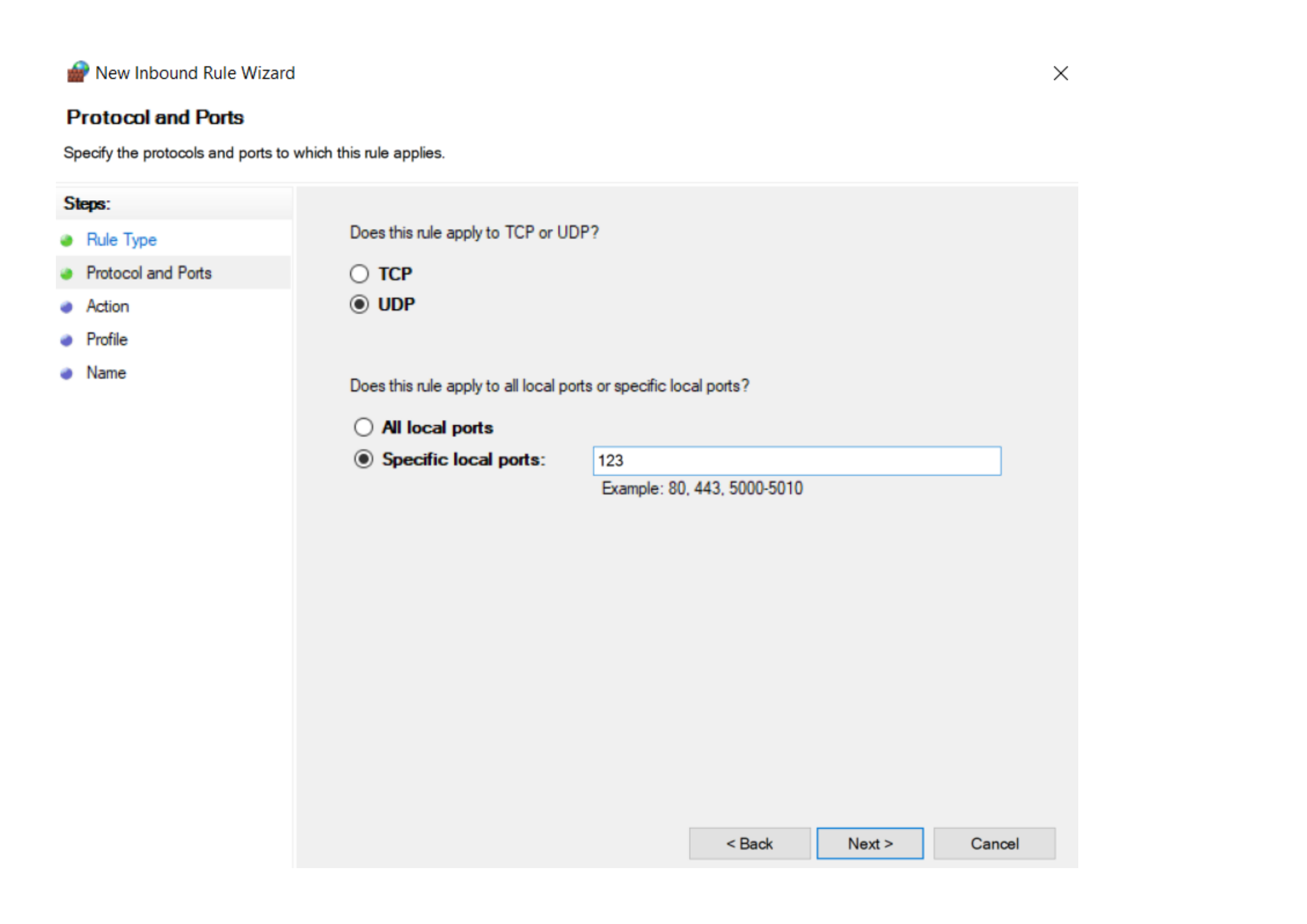
4. Выполните конфигурацию службы второго уровня времени на SRV

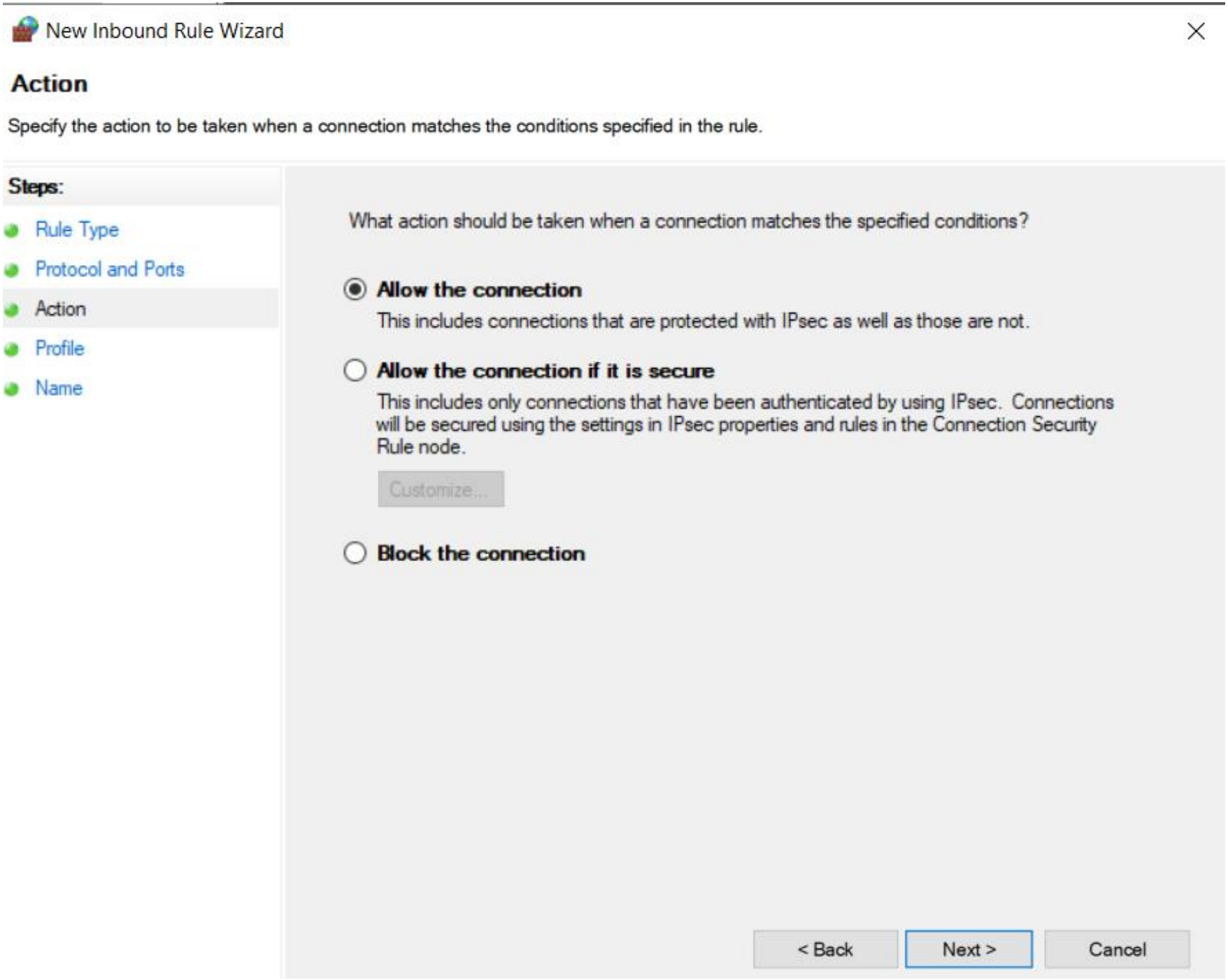
SRV NTP

Меню пуск, выбрать “Windows Administrative Tools” = > “Windows Defender Firewall with Advanced Security”

Inboard Rules = > New Rules


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
123
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel

When does this rule apply?

☑ **Domain**

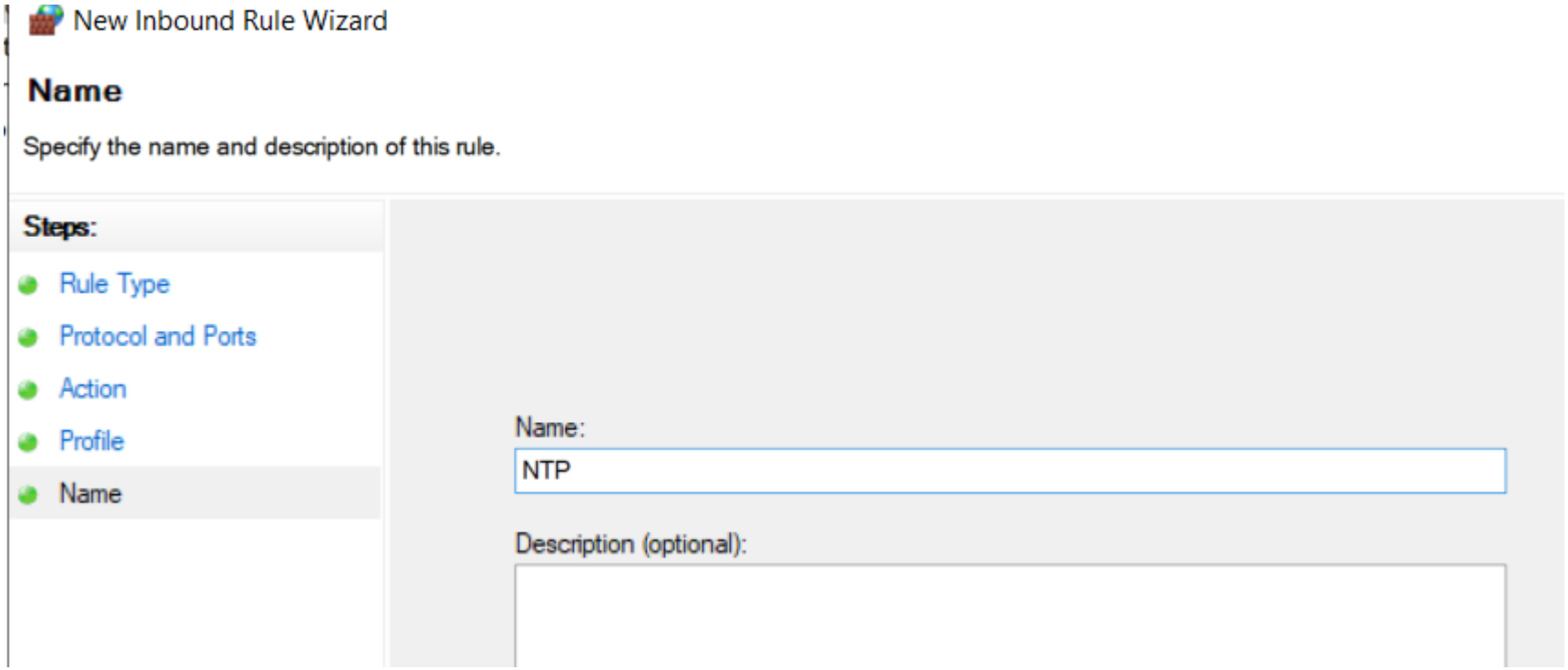
Applies when a computer is connected to its corporate domain.

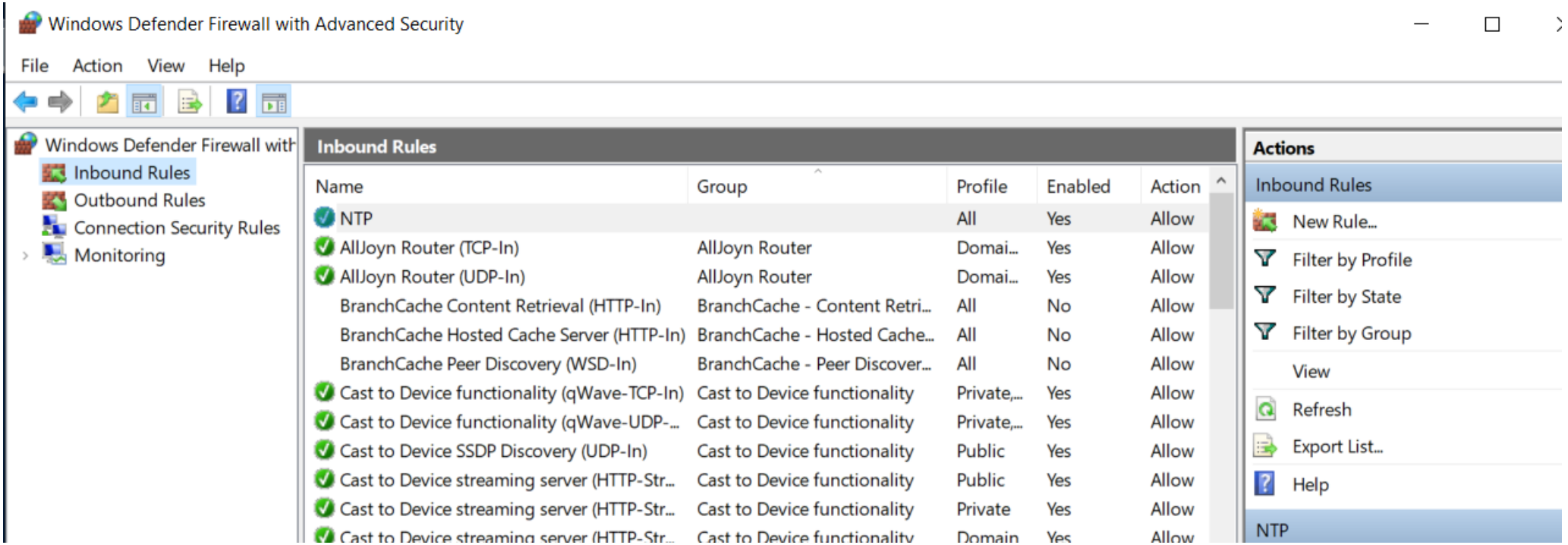
☑ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**

Applies when a computer is connected to a public network location.

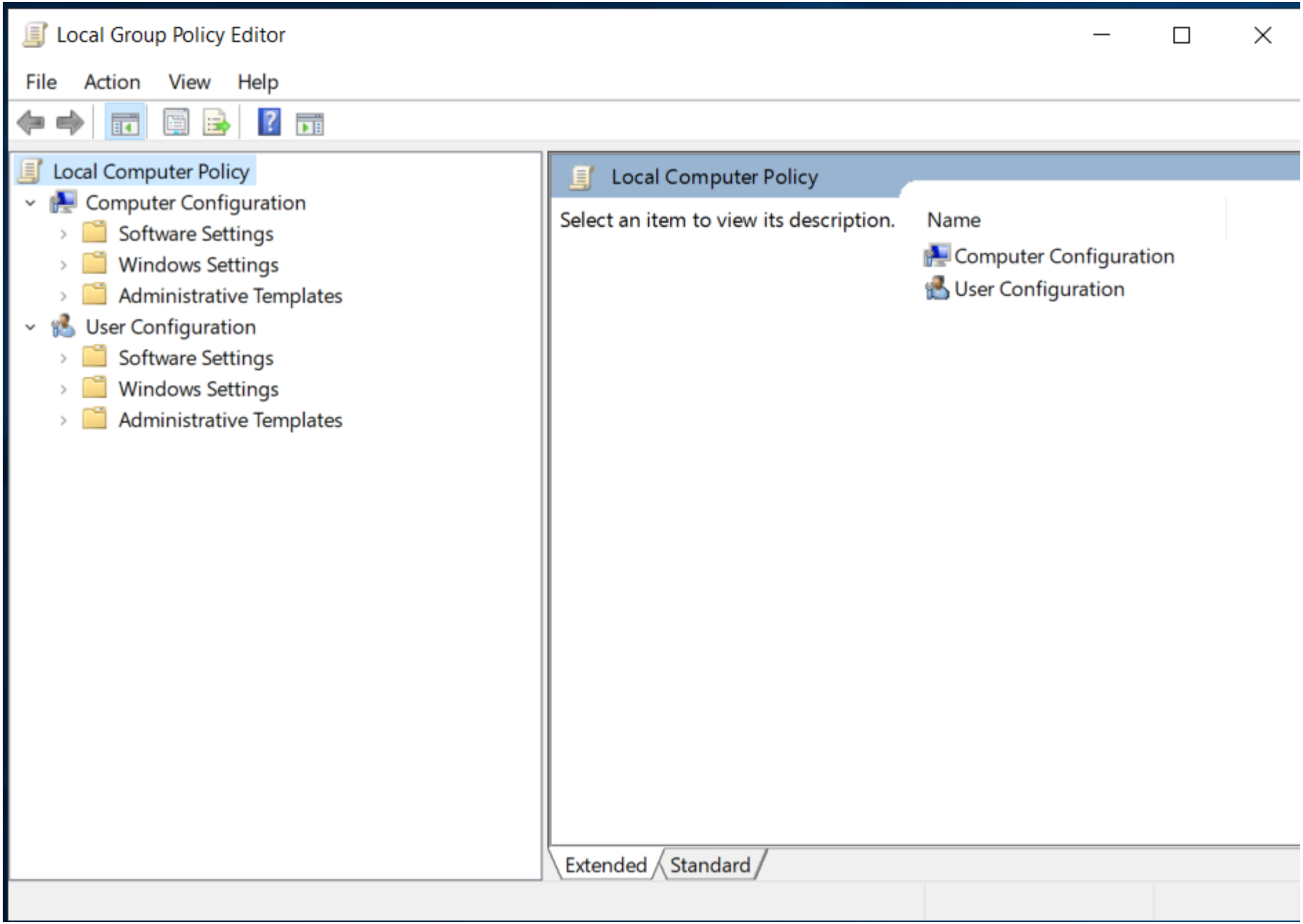




Тоже самое, через PowerShell:

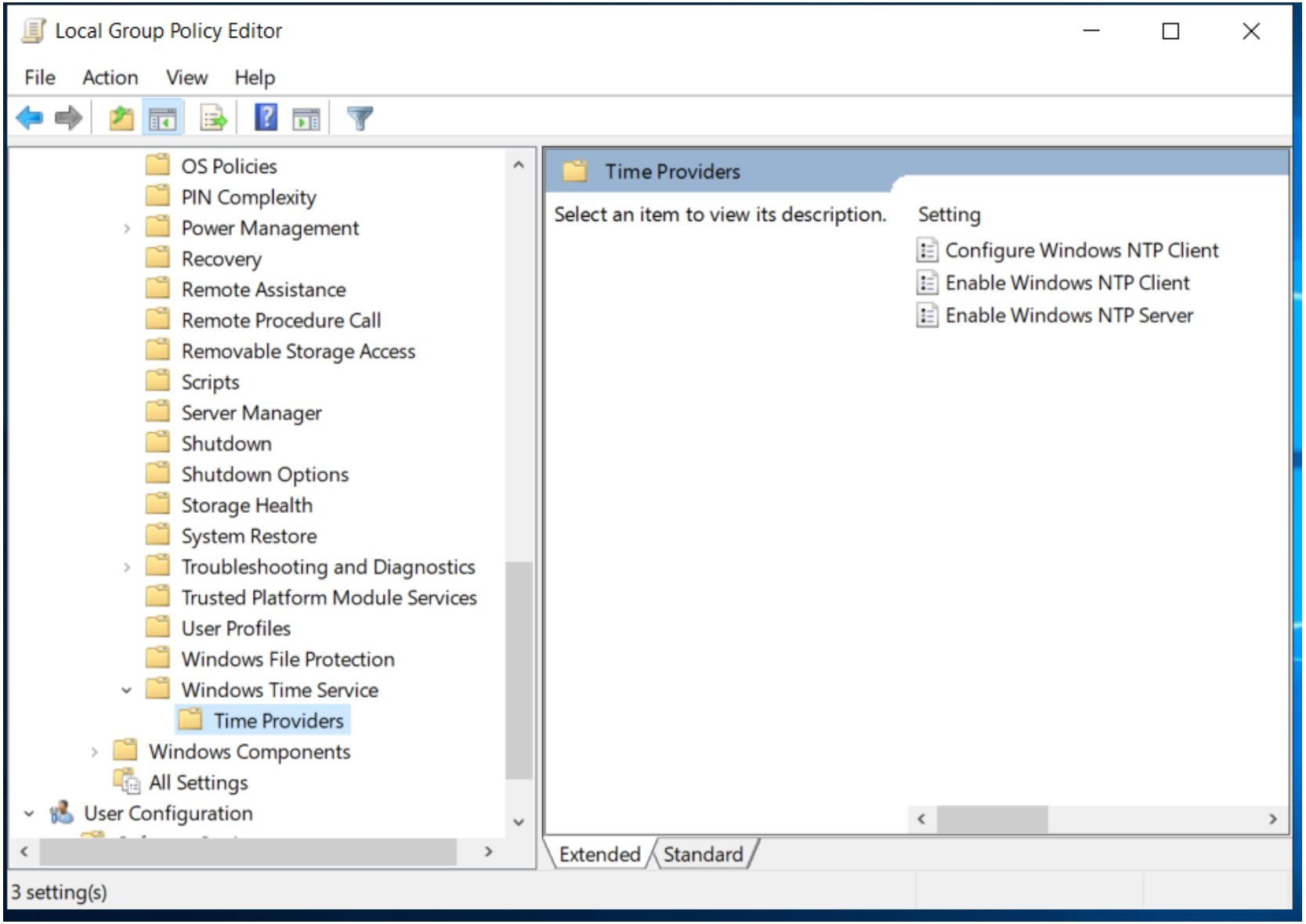
New-NetFirewallRule -DisplayName "NTP" -Direction Inbound -LocalPort 123 -Protocol UDP -Action Allow

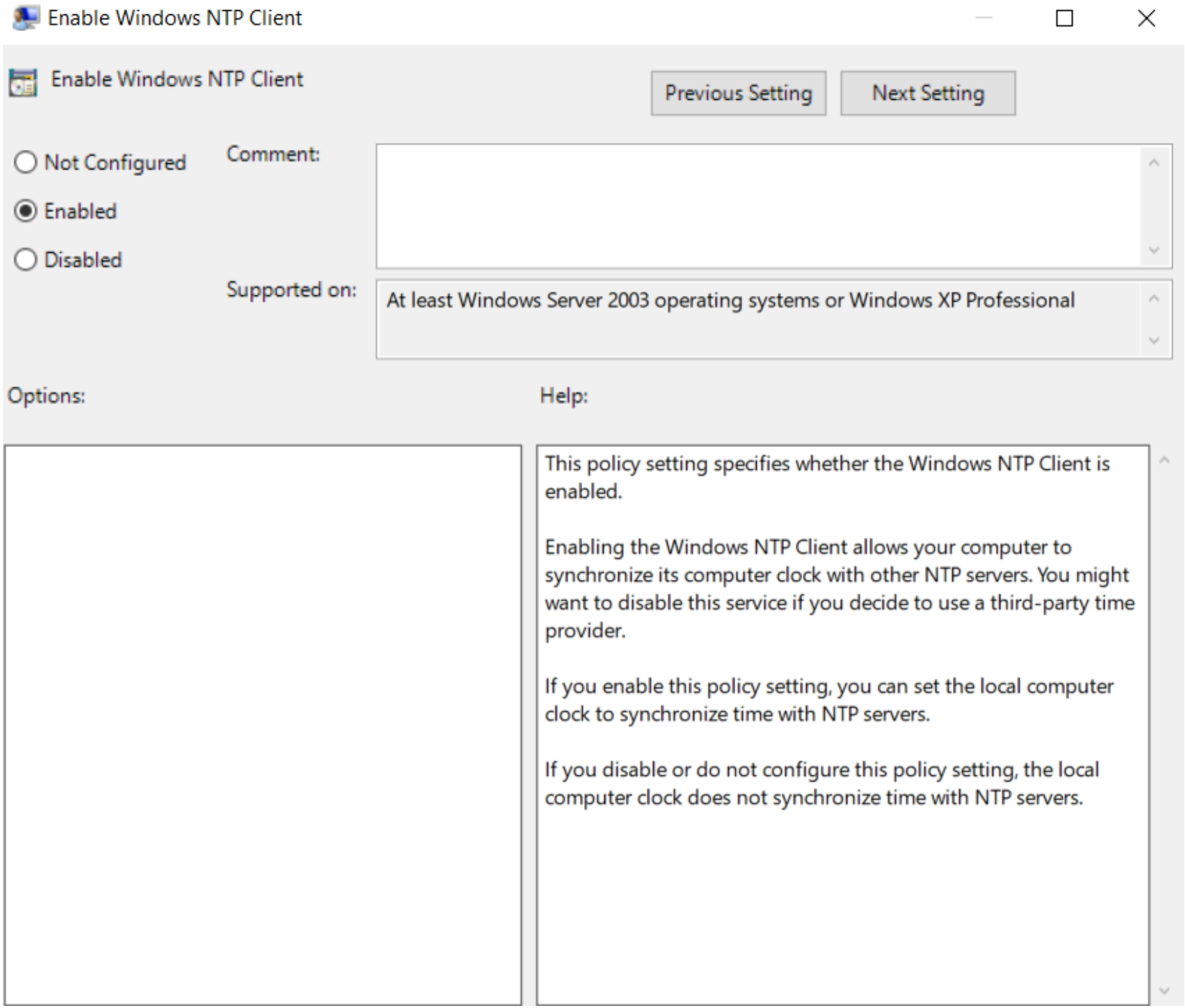
В меню пуск, Windows Systen = > выбираем элемент «Run» и вводим gpedit.msc, либо через командную строку.

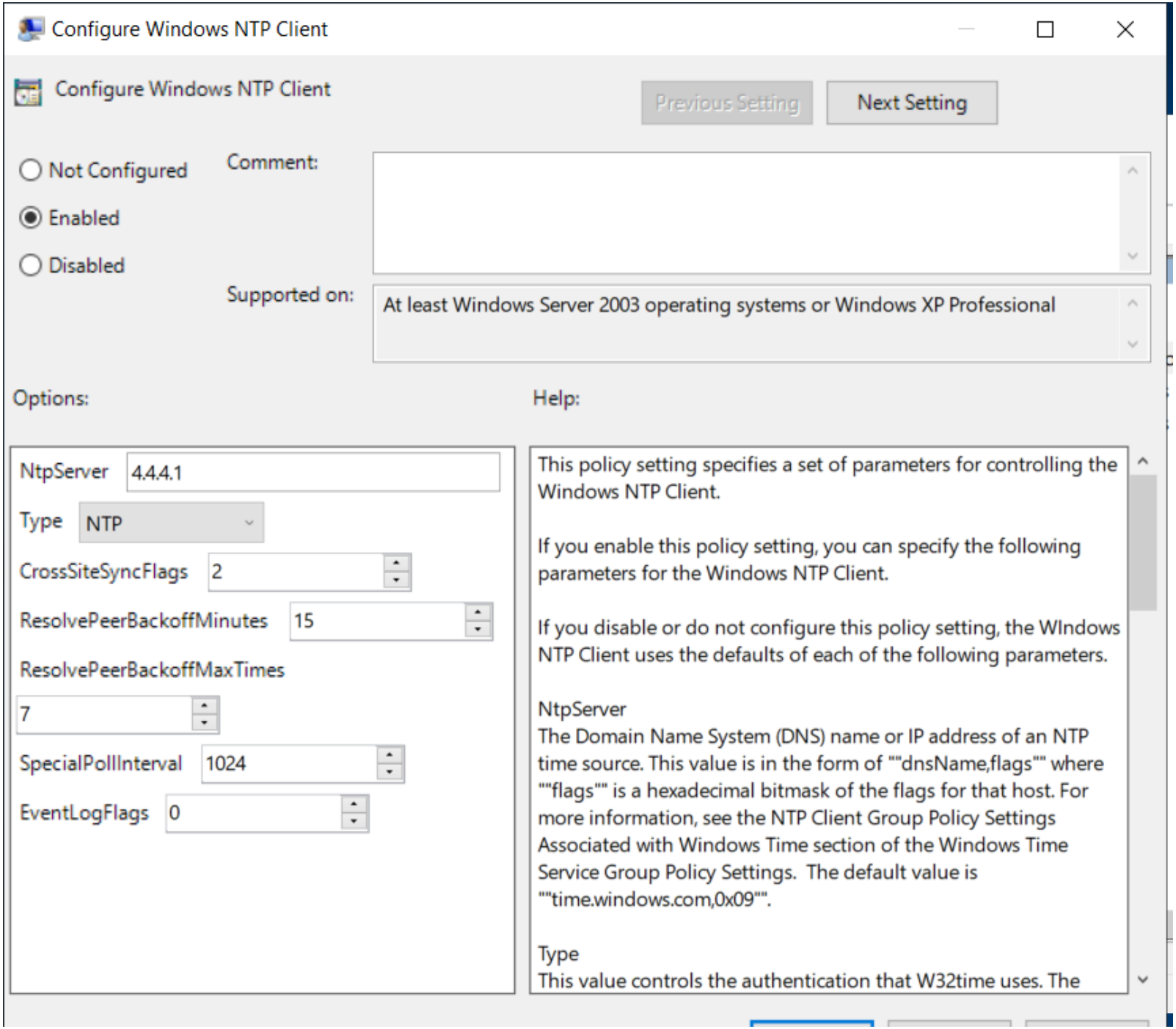

Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Local Computer Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard

Computer Configuration => Administrative Templates => System => Windows Time Service =>

= > Time Providers

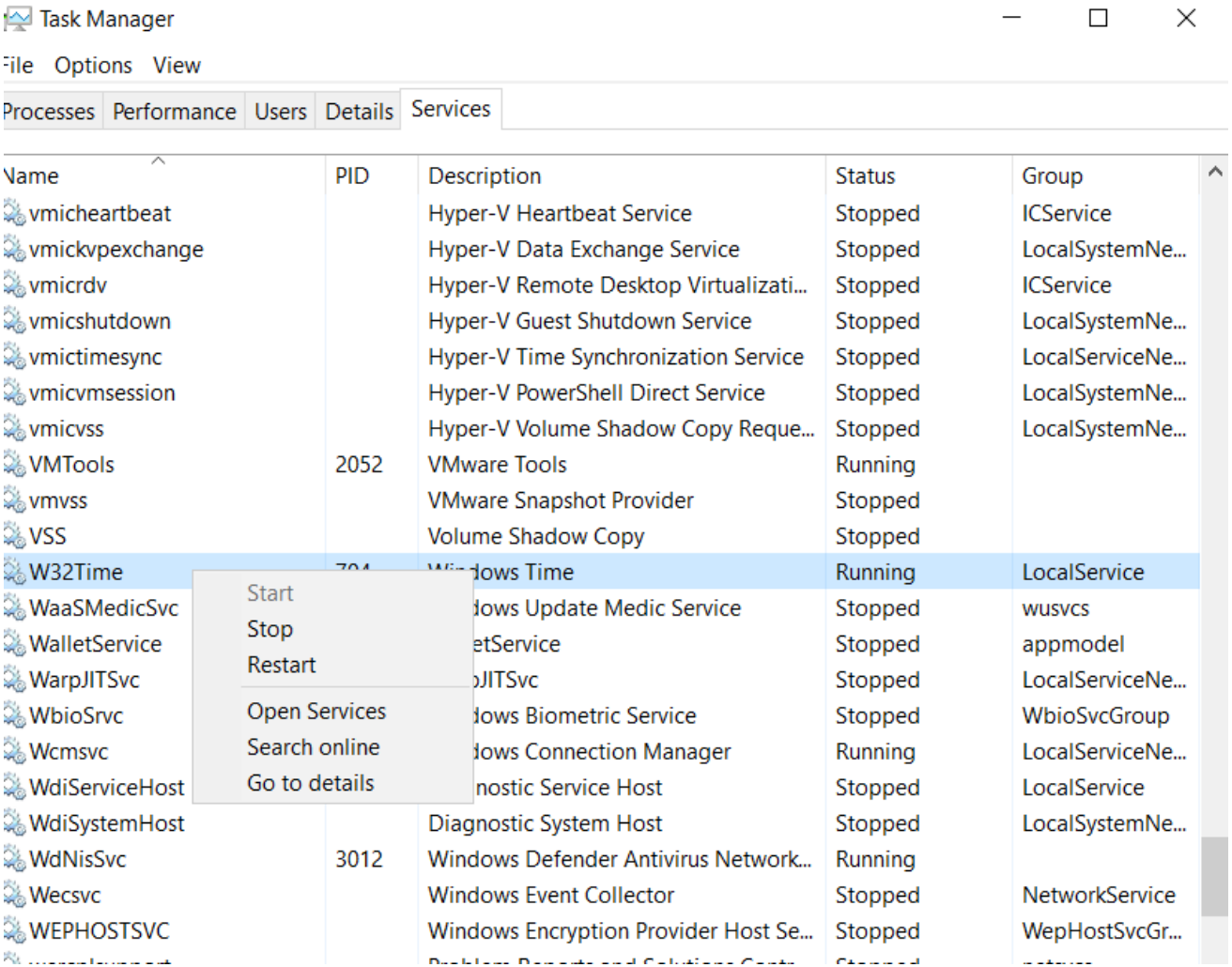



Enable Windows NTP Client
Enable Windows NTP Client
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2003 operating systems or Windows XP Professional
Options:
Help:
This policy setting specifies whether the Windows NTP Client is enabled.
Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider.
If you enable this policy setting, you can set the local computer clock to synchronize time with NTP servers.
If you disable or do not configure this policy setting, the local computer clock does not synchronize time with NTP servers.


Configure Windows NTP Client
Configure Windows NTP Client
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2003 operating systems or Windows XP Professional
Options:
Help:
NtpServer
4.4.4.1
Type
NTP
CrossSiteSyncFlags
2
ResolvePeerBackoffMinutes
15
ResolvePeerBackoffMaxTimes
7
SpecialPollInterval
1024
EventLogFlags
0
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

Меню пуск, “Windows System” => Task Manager => More details => Services

Зайти в службы и перезапустить Службу времени “W32Time”, проверить что бы был автозапуск



Тоже самое, через PowerShell:

w32tm /query /status
Start-Service W32Time
w32tm /config /manualpeerlist:4.4.4.1 /syncfromflags:manual /reliable:yes /update
Restart-Service W32Time

CLI NTP

CLI настраивается аналогично SRV

Тоже самое, через PowerShell:

New-NetFirewallRule -DisplayName "NTP" -Direction Inbound -LocalPort 123 -Protocol UDP -Action Allow

Start-Service W32Time
w32tm /config /manualpeerlist:4.4.4.1 /syncfromflags:manual /reliable:yes /update
Restart-Service W32Time

Set-Service -Name W32Time -StartupType Automatic

RTR-L NTP

ip domain name int.demo.wsr
ip name-server 192.168.100.200
ntp server ntp.int.demo.wsr
do wr

RTR-R NTP

ip domain name int.demo.wsr
ip name-server 192.168.100.200
ntp server ntp.int.demo.wsr
do wr

WEB-L NTP

apt-cdrom add
apt install -y chrony

открыть файл , закоментить одну строку и две вписать

nano /etc/chrony/chrony.conf
pool ntp.int.demo.wsr iburst
allow 192.168.100.0/24

```
confdir /etc/chrony/conf.d

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

allow 192.168.100.0/24

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

systemctl restart chrony

WEB-R NTP

apt-cdrom add
apt install -y chrony
nano /etc/chrony/chrony.conf

pool ntp.int.demo.wsr iburst
allow 192.168.100.0/24

```
# Use Debian vendor zone.
#pool 2.debian.pool.ntp.org iburst
pool ntp.int.demo.wsr iburst

allow 192.168.100.0/24
# Use time sources from DHCP.
sourcedir /run/chrony-dhcp
```

systemctl restart chrony

5. Реализуйте файловый SMB-сервер на базе SRV

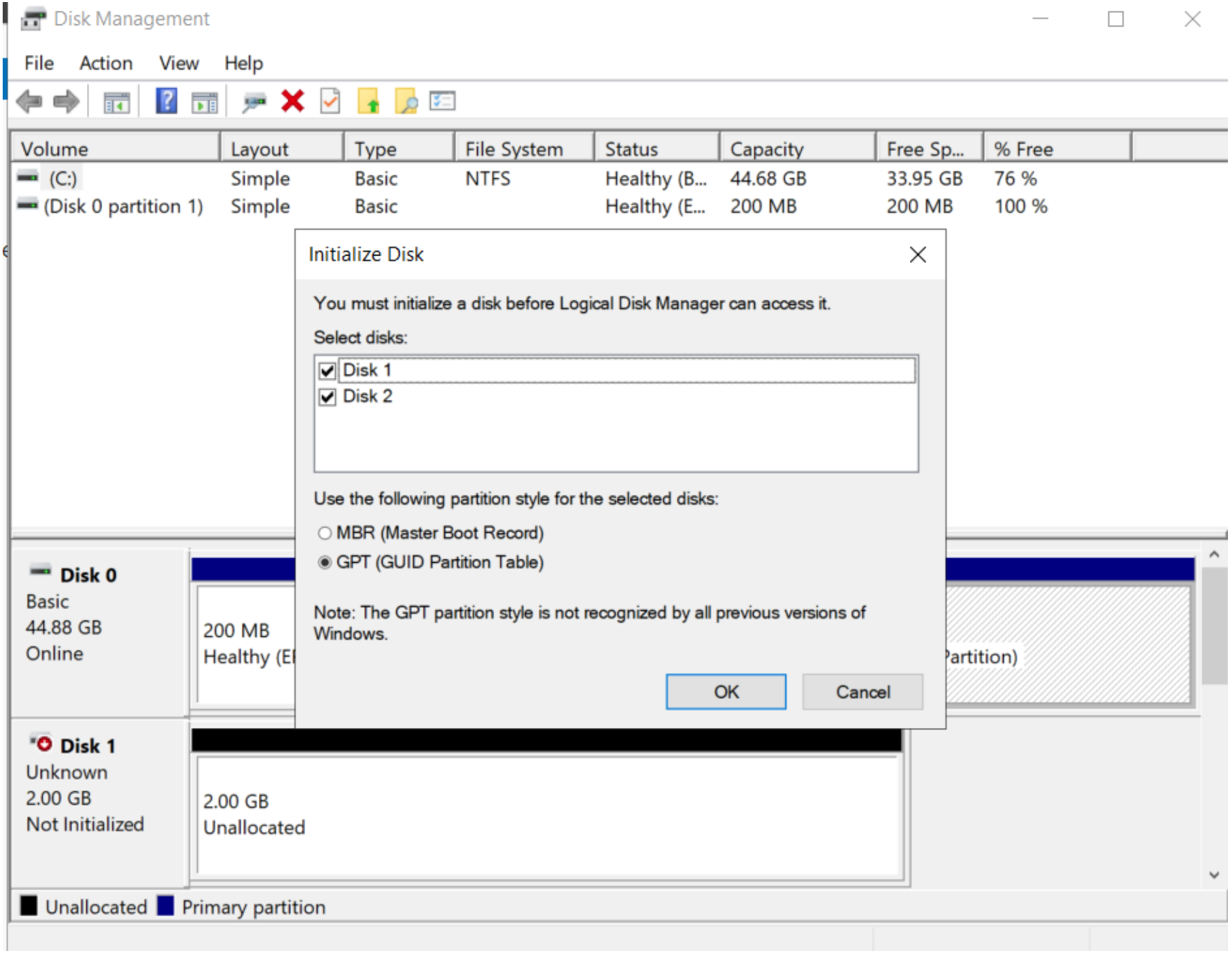
SRV RAID1

Открыть папку на панели задач, открыть “Control Panel” => System and Security => Administrative Tools =>

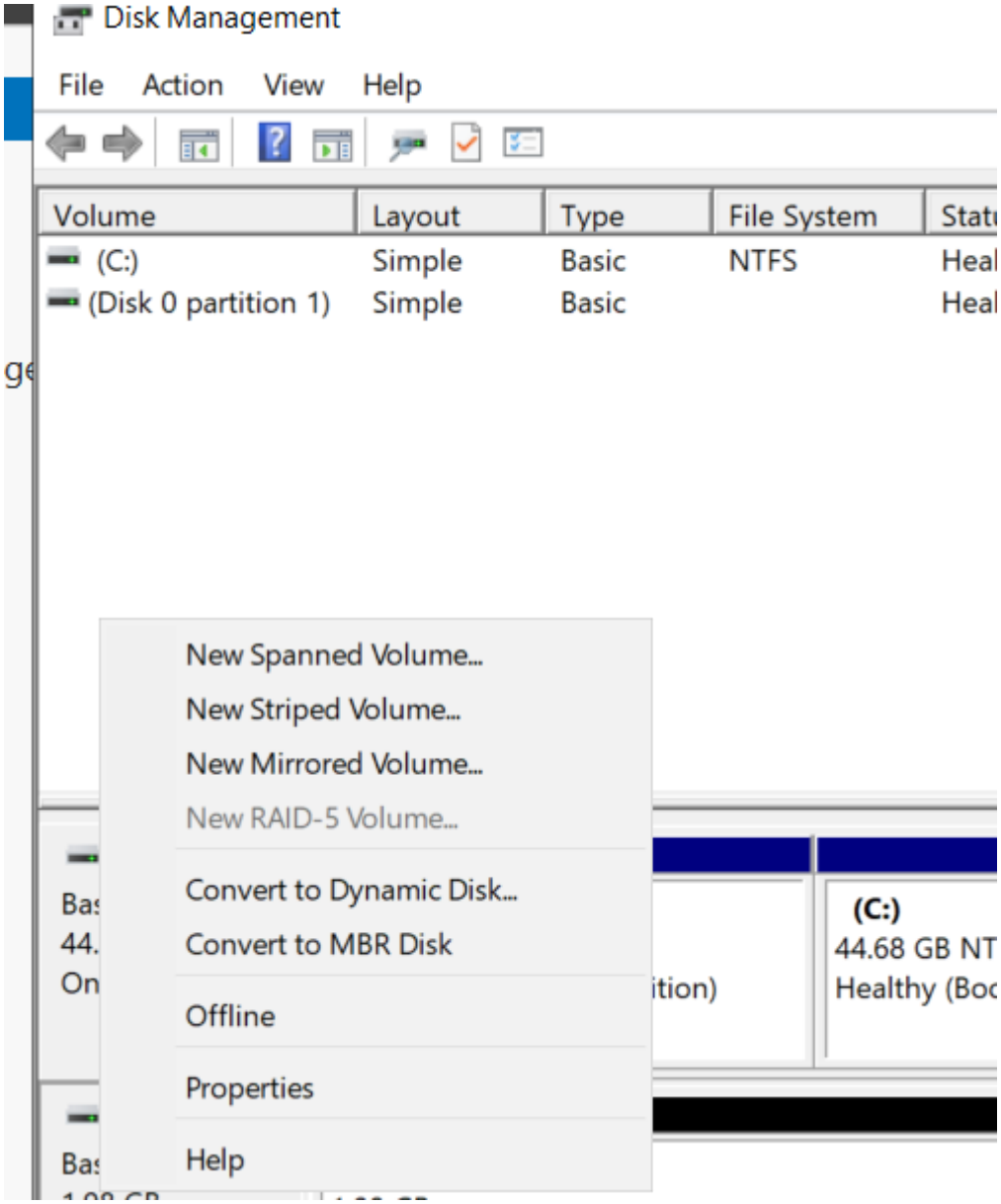
= > Create and format hard disk partitions

Правой клавишей на диск => Online

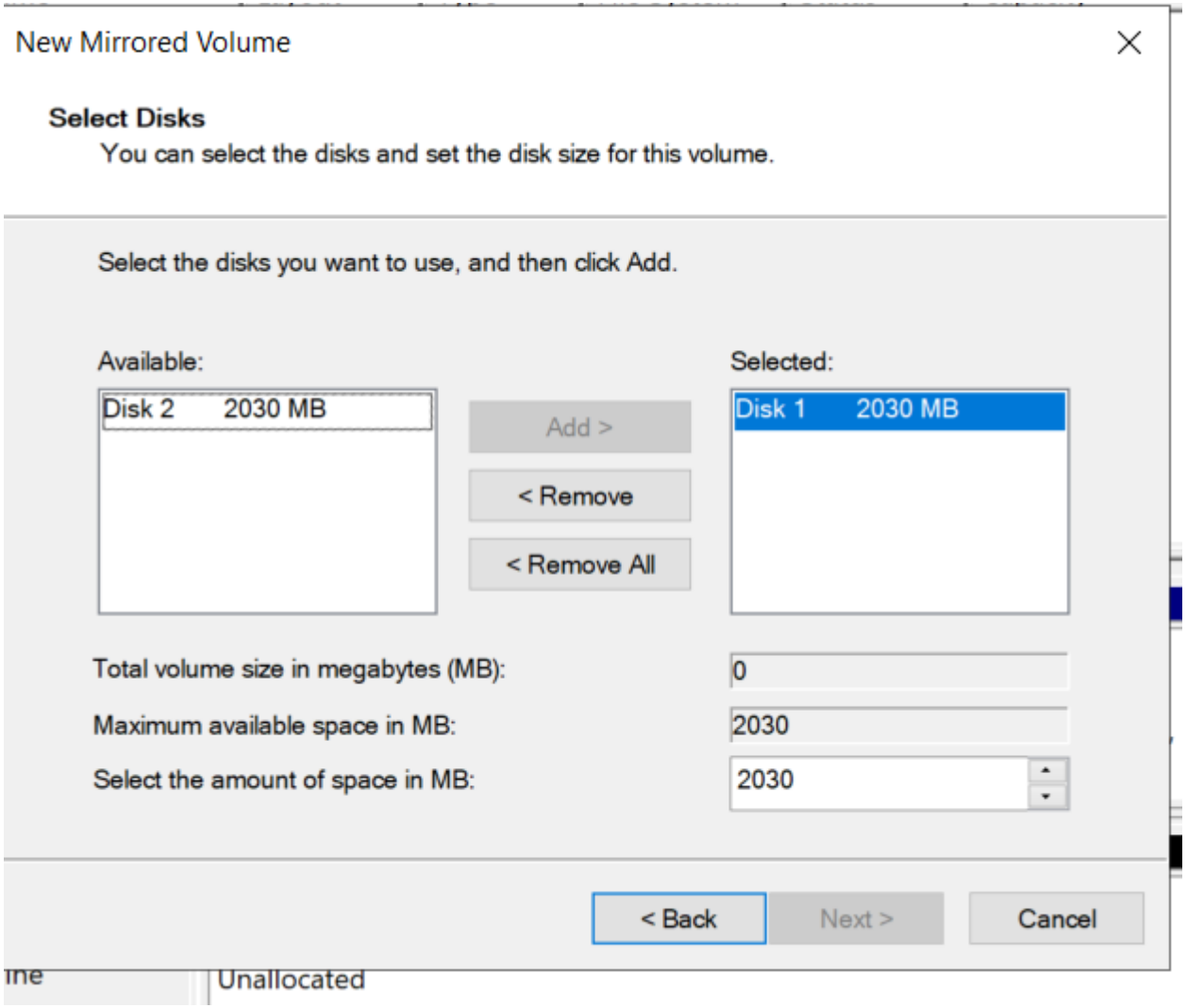
Правой клавишей на диск => Initialize Disk

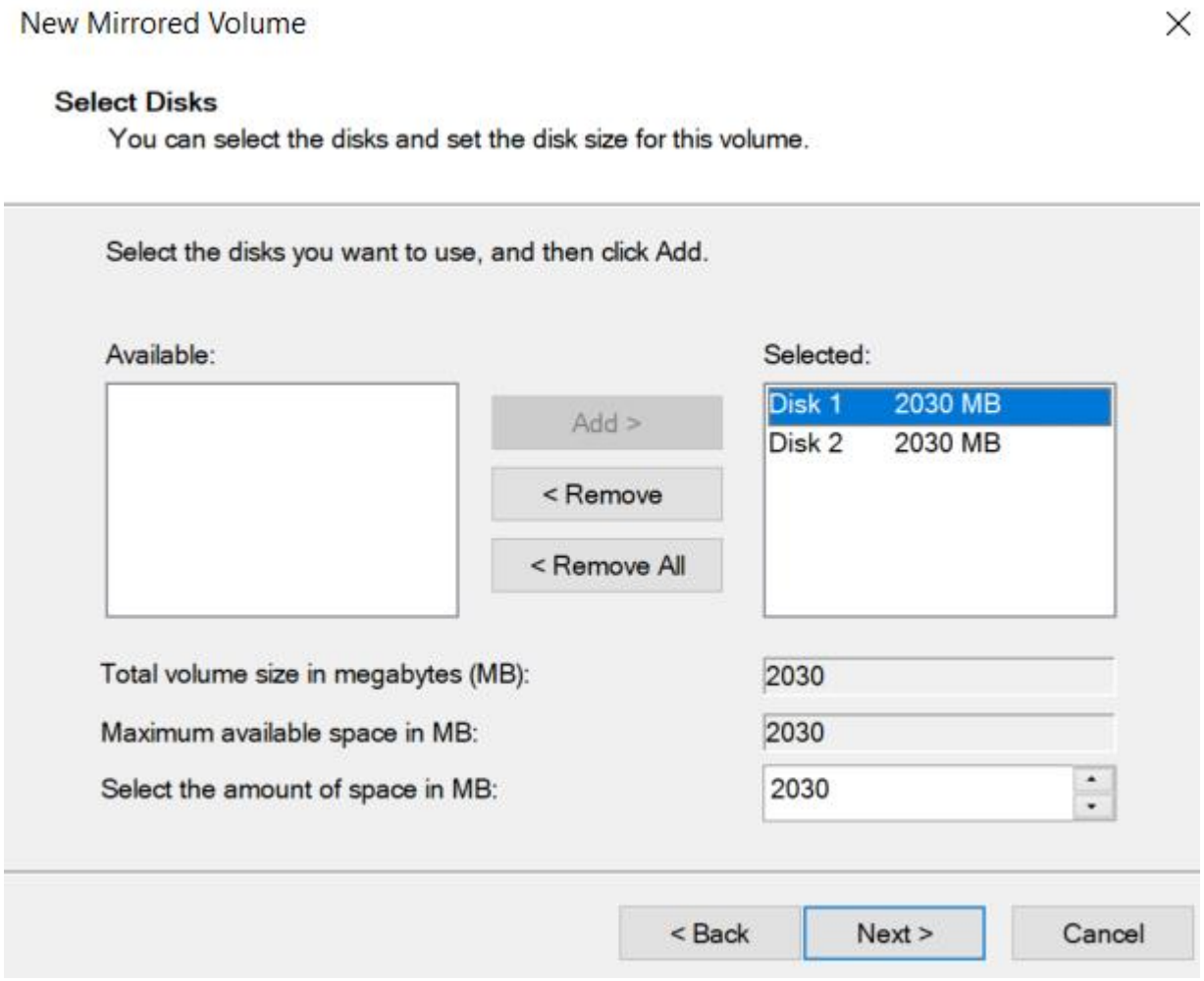

Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Sp... % Free
(C:) Simple Basic NTFS Healthy (B... 44.68 GB 33.95 GB 76 %
(Disk 0 partition 1) Simple Basic Healthy (E... 200 MB 200 MB 100 %
Initialize Disk
You must initialize a disk before Logical Disk Manager can access it.
Select disks:
Disk 1
Disk 2
Use the following partition style for the selected disks:
MBR (Master Boot Record)
GPT (GUID Partition Table)
Note: The GPT partition style is not recognized by all previous versions of Windows.
OK
Cancel
Disk 0
Basic
44.88 GB
Online
200 MB
Healthy (E
Disk 1
Unknown
2.00 GB
Not Initialized
2.00 GB
Unallocated
Unallocated
Primary partition

Правой клавишей на Disk 1 = > Выбрать «New Mirrored Volume»

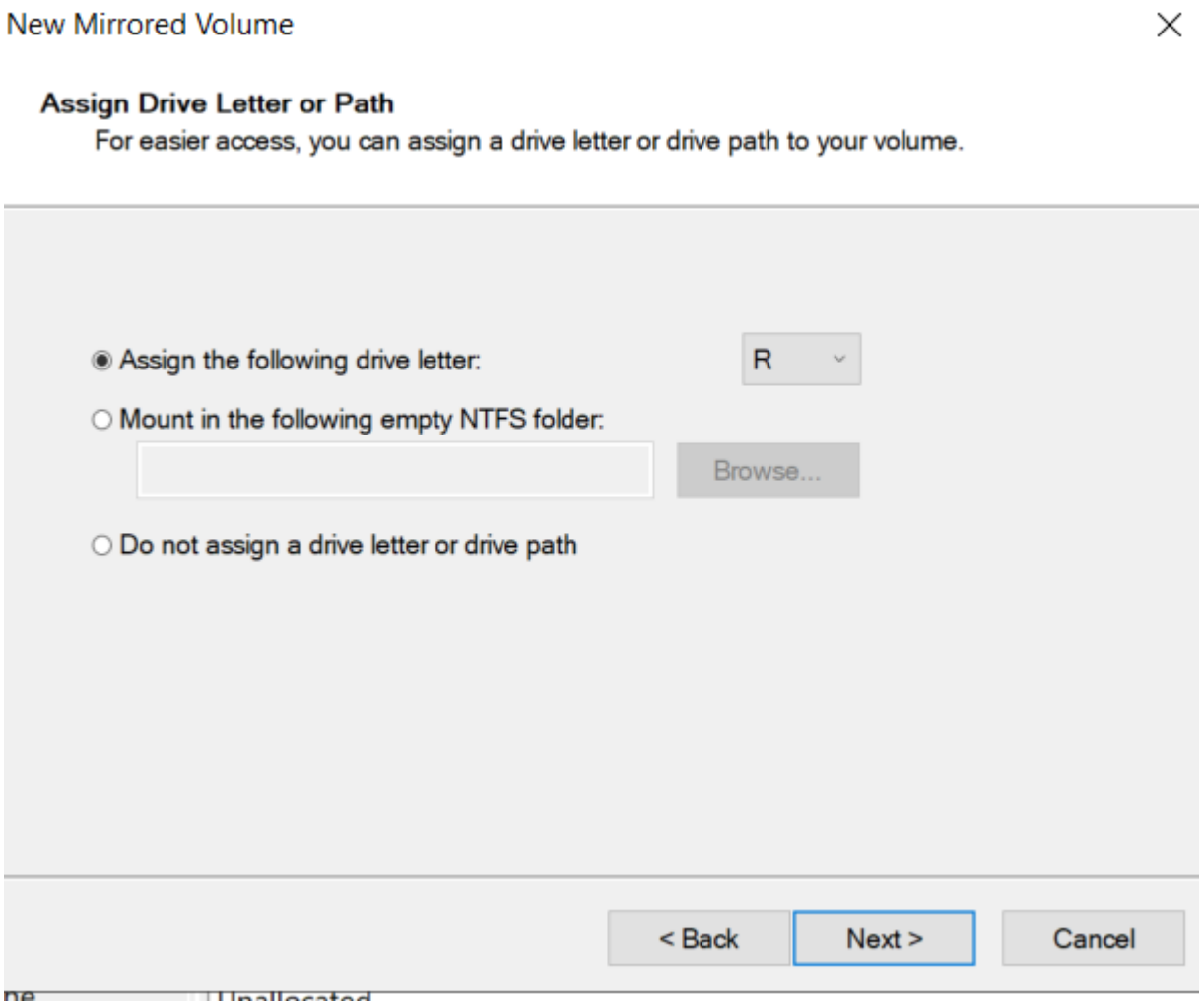


В колонке слева выбрать Диск 2 и добавить в правую колонку

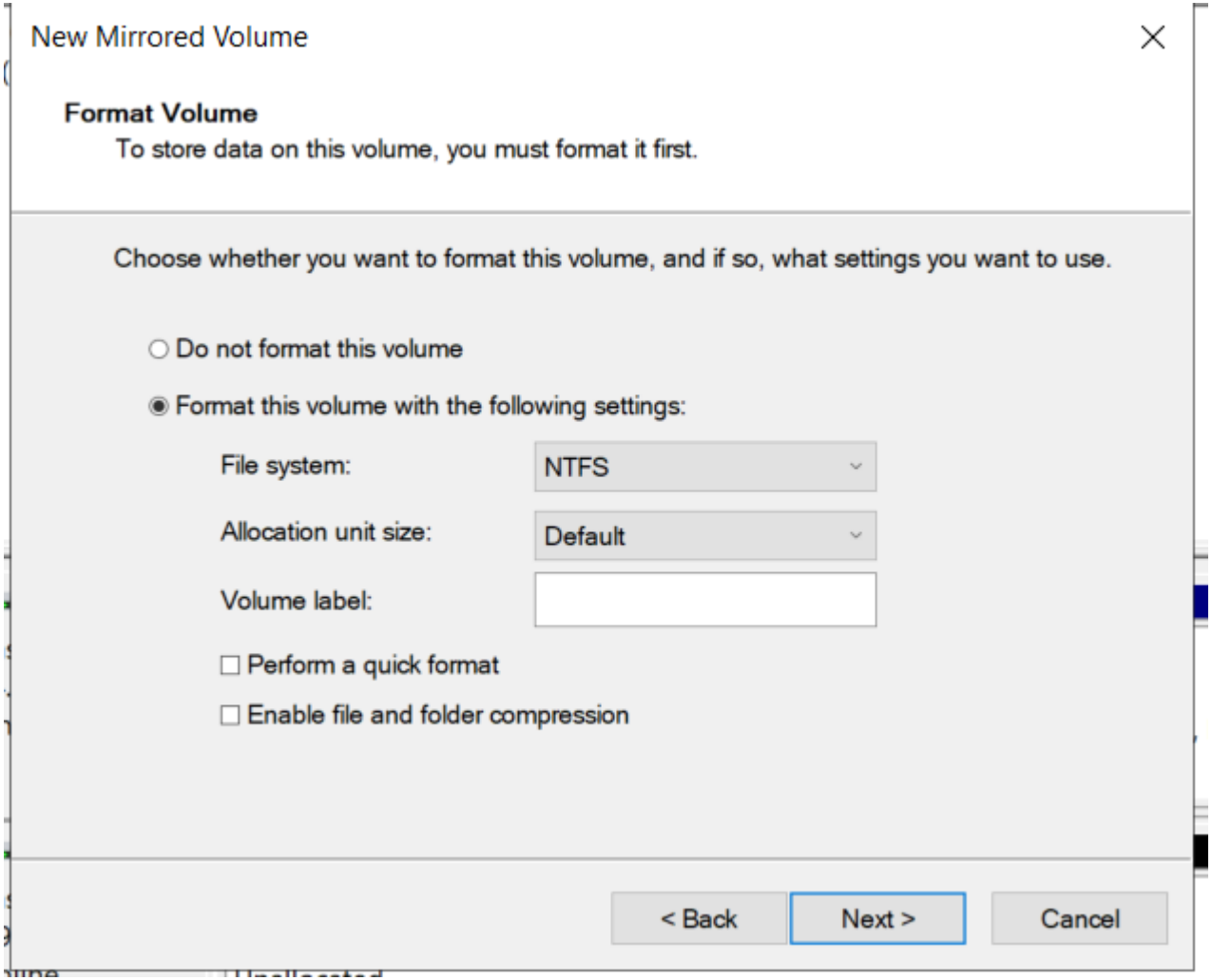




букву выбрать “R”



Можно стереть значение в “Volume label”

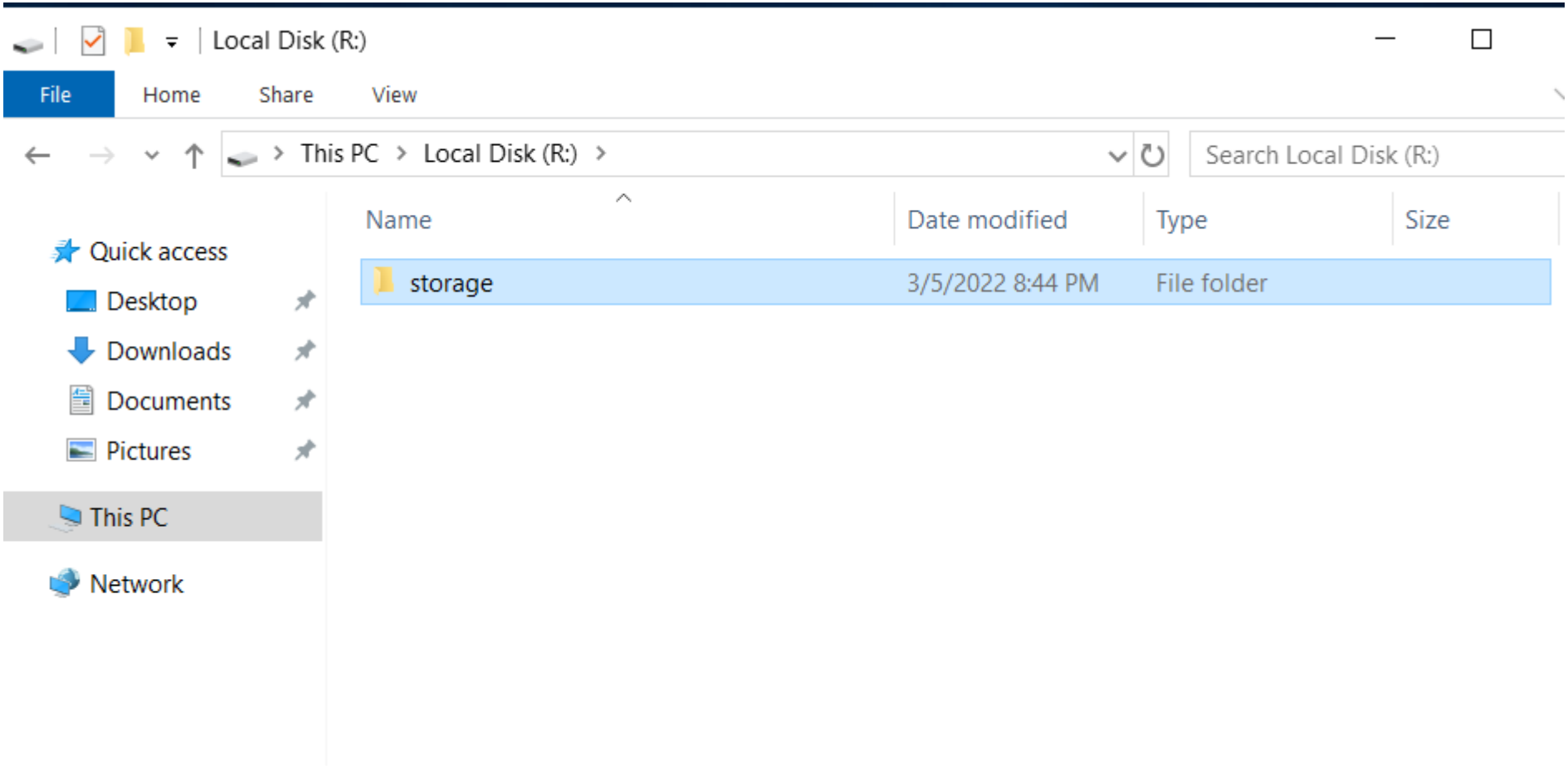

New Mirrored Volume
Format Volume
To store data on this volume, you must format it first.
Choose whether you want to format this volume, and if so, what settings you want to use.
Do not format this volume
Format this volume with the following settings:
File system:
NTFS
Allocation unit size:
Default
Volume label:
Perform a quick format
Enable file and folder compression
< Back
Next >
Cancel

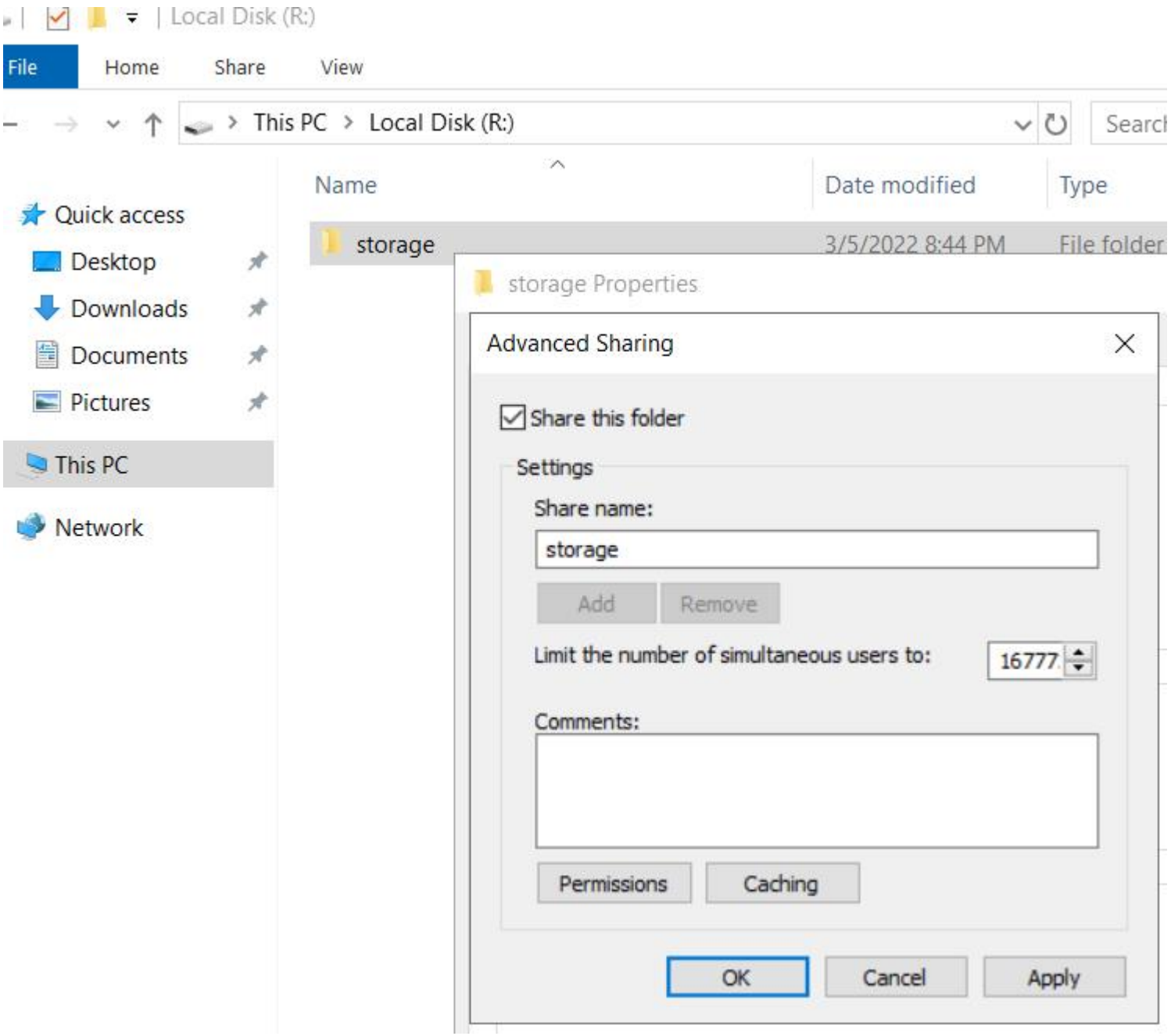
Тоже самое, через PowerShell:

```
get-disk
set-disk -Number 1 -IsOffline $false
set-disk -Number 2 -IsOffline $false

New-StoragePool -FriendlyName "POOLRAID1" -StorageSubsystemFriendlyName "Windows Storage*" -PhysicalDisks (Get-PhysicalDisk -CanPool $true)

New-VirtualDisk -StoragePoolFriendlyName "POOLRAID1" -FriendlyName "RAID1" -ResiliencySettingName Mirror -UseMaximumSize

Initialize-Disk -FriendlyName "RAID1"

New-Partition -DiskNumber 3 -UseMaximumSize -DriveLetter R

Format-Volume -DriveLetter R
```

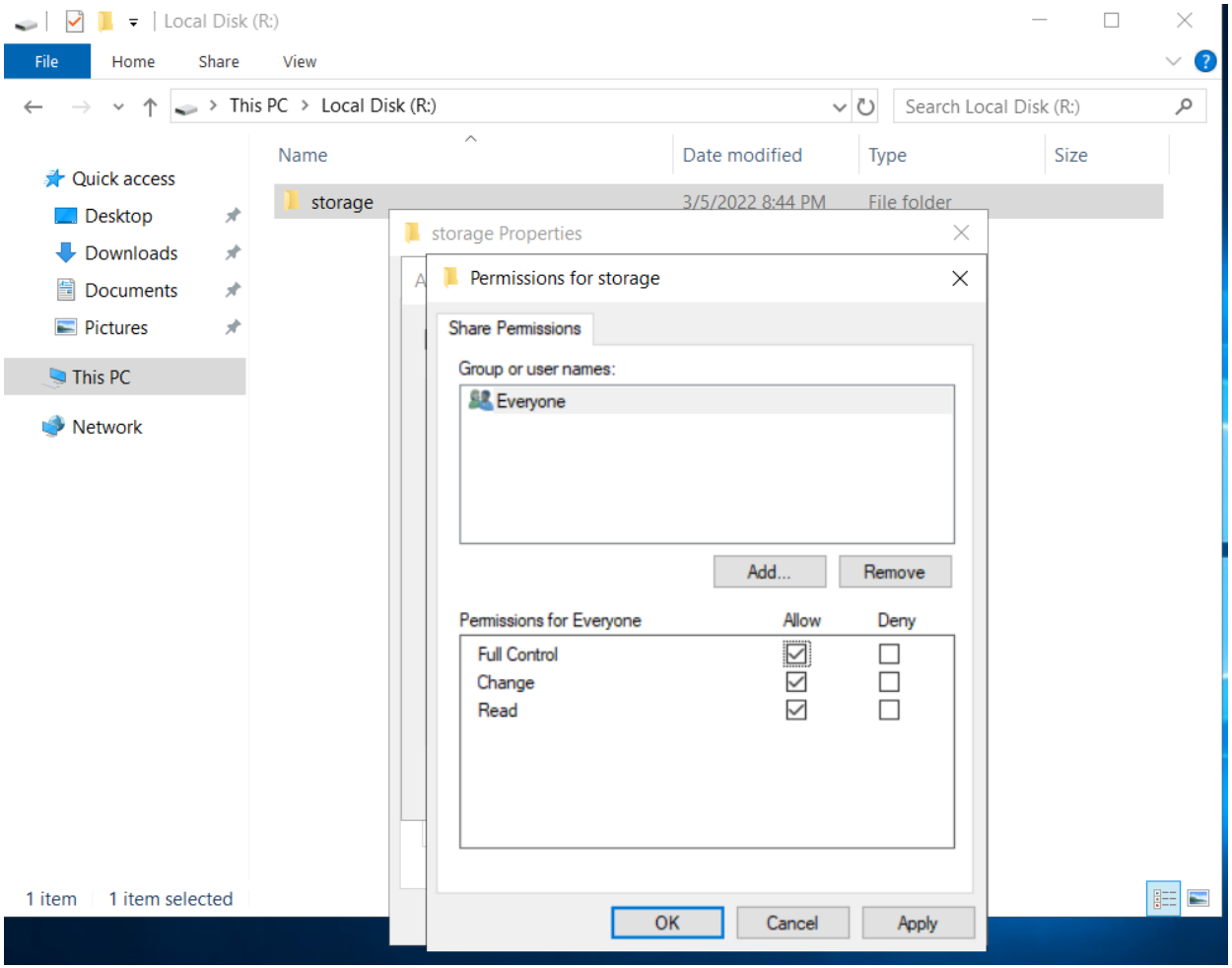
SRV NFS

Создать папку в соответствии с заданием




Local Disk (R:)
File
Home
Share
View
This PC
Local Disk (R:)
Search
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
storage
3/5/2022 8:44 PM
File folder
storage Properties
Advanced Sharing
Share this folder
Settings
Share name:
storage
Add
Remove
Limit the number of simultaneous users to:
16777
Comments:
Permissions
Caching
OK
Cancel
Apply

Выбрать “Permissions”



Тоже самое, через PowerShell:

Install-WindowsFeature -Name FS-FileServer -IncludeManagementTools

New-SmbShare -Name "SMB" -Path "R:\storage" -FullAccess "Everyone"

6. Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:

WEB-L SMB

Установить диск и смонтировать

apt-cdrom add

Установить приложение:

apt install -y cifs-utils

Создать новый файл

nano /root/.smbclient

Записать в файл:

username=Administrator
password=P@ssw0rd

Открыть файл:

nano /etc/fstab

В конец добавить строку:

//srv.int.demo.wsr/storage /opt/share cifs user,rw,_netdev,credentials=/root/.smbclient 0 0

Создать папку куда будет монтироваться общая папка

mkdir /opt/share

Произвести монтирование:

mount -a

WEB-R SMB

Смонтировать диск
apt-cdrom add

Установить приложение

apt install -y cifs-utils

Создать новый файл

nano /root/.smbclient

Записать в файл:

username=Administrator
password=Pa$$w0rd

Открыть файл:

nano /etc/fstab

В конец добавить строку:

//srv.int.demo.wsr/storage /opt/share cifs user,rw,_netdev,credentials=/root/.smbclient 0 0

Создать папку куда будет монтироваться общая папка

mkdir /opt/share

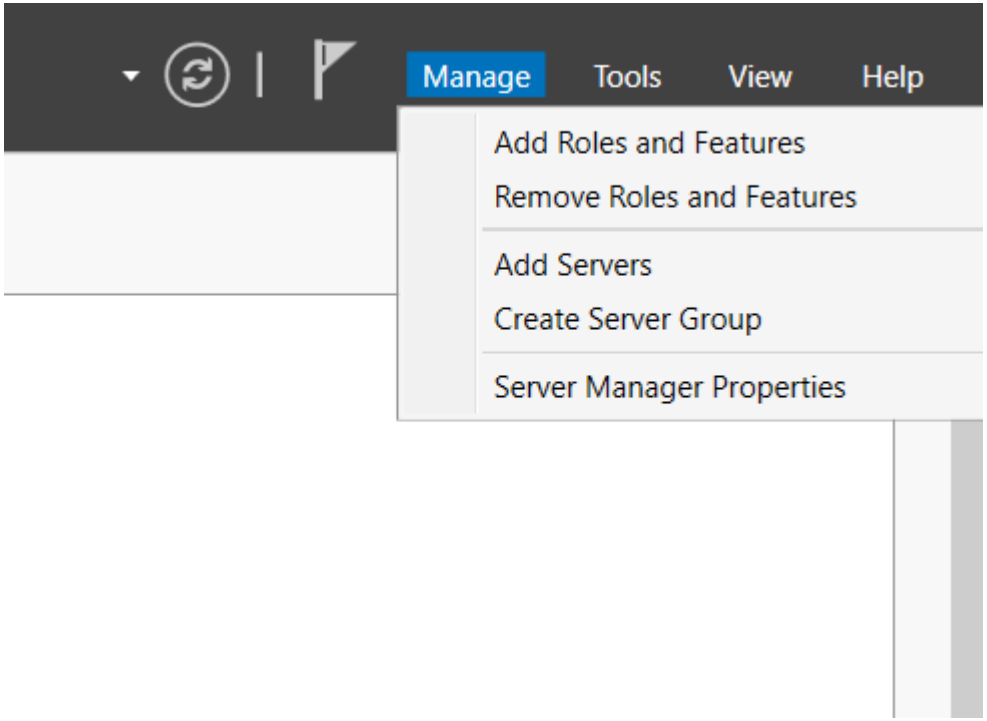
Произвести монтирование:

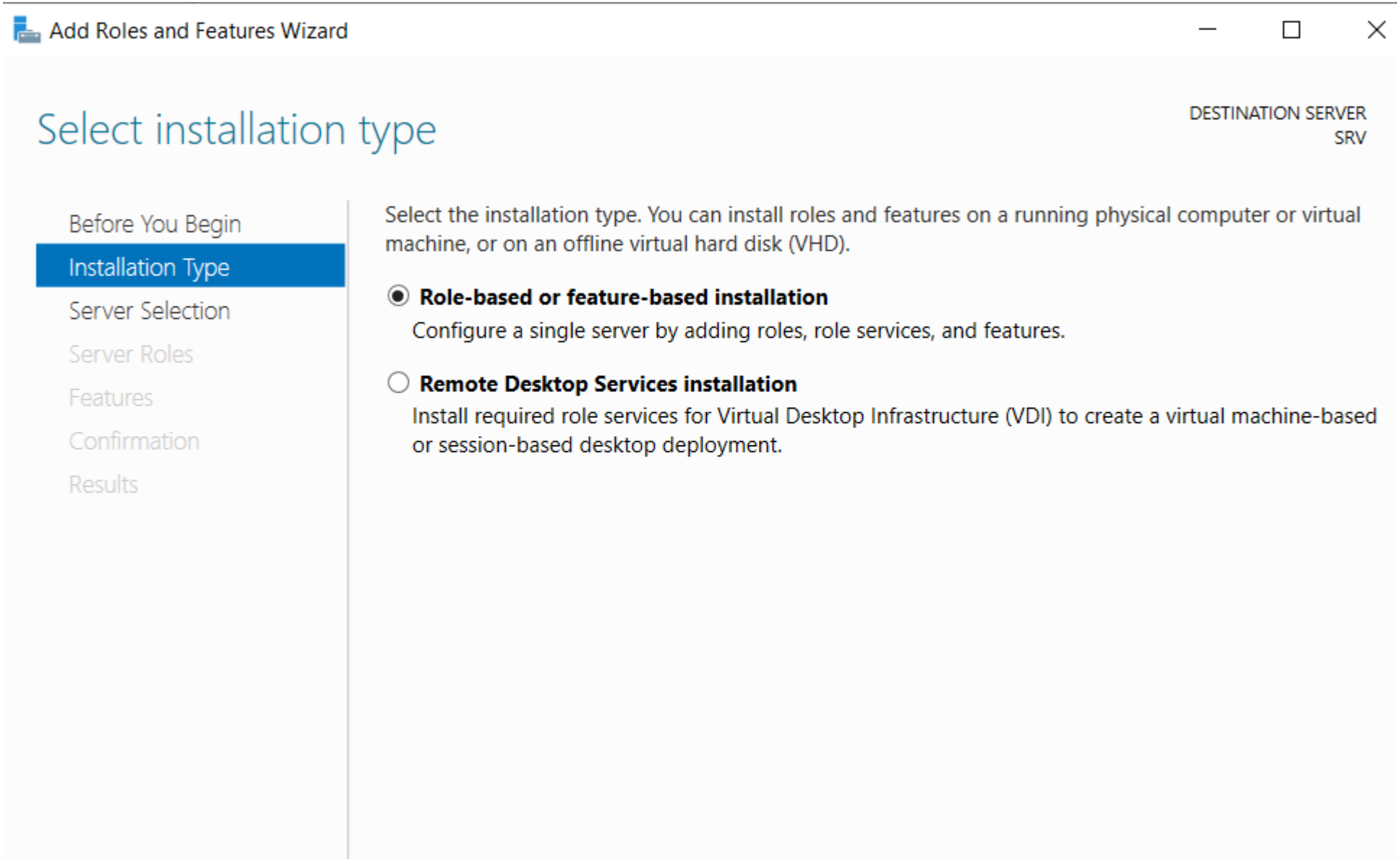
mount -a

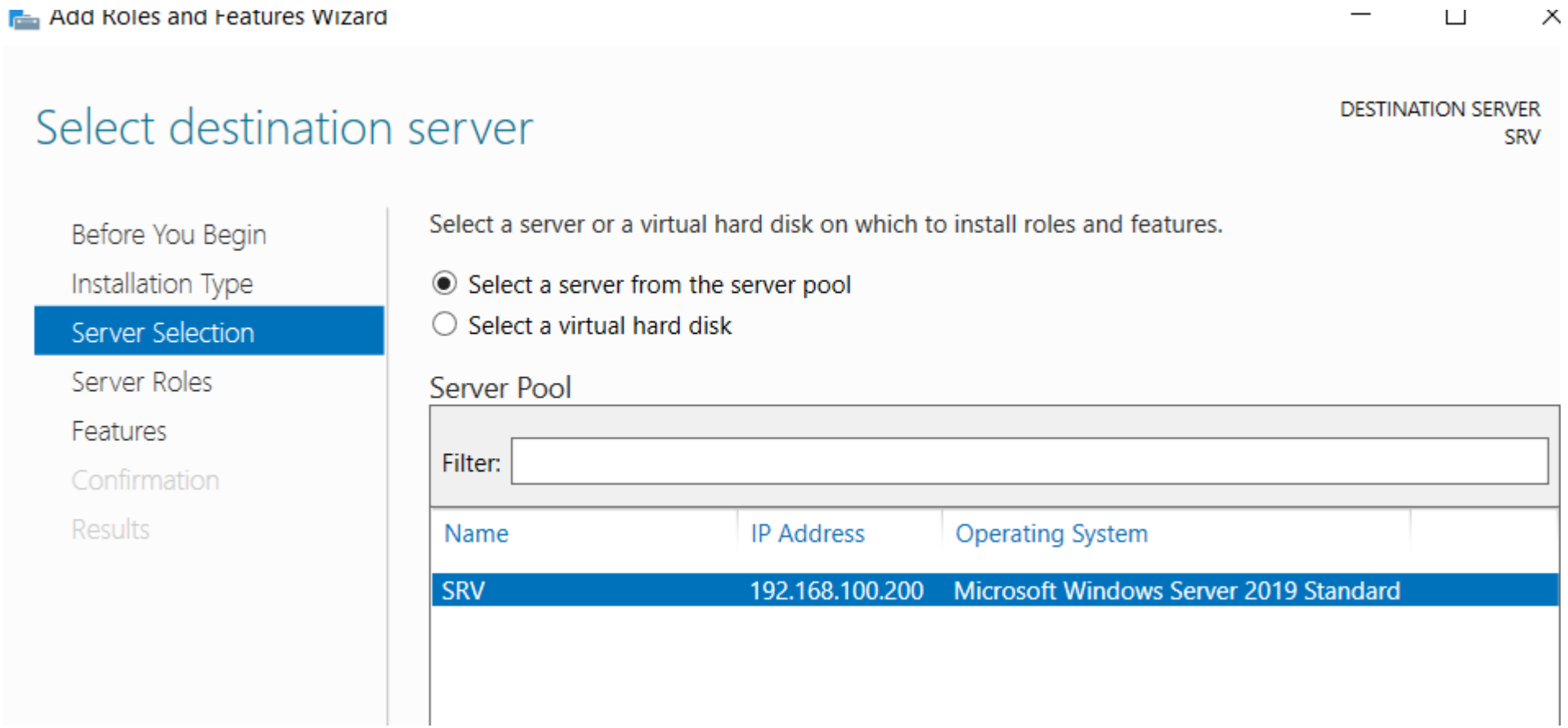
7. Выполните настройку центра сертификации на базе SRV:

SRV ADCS

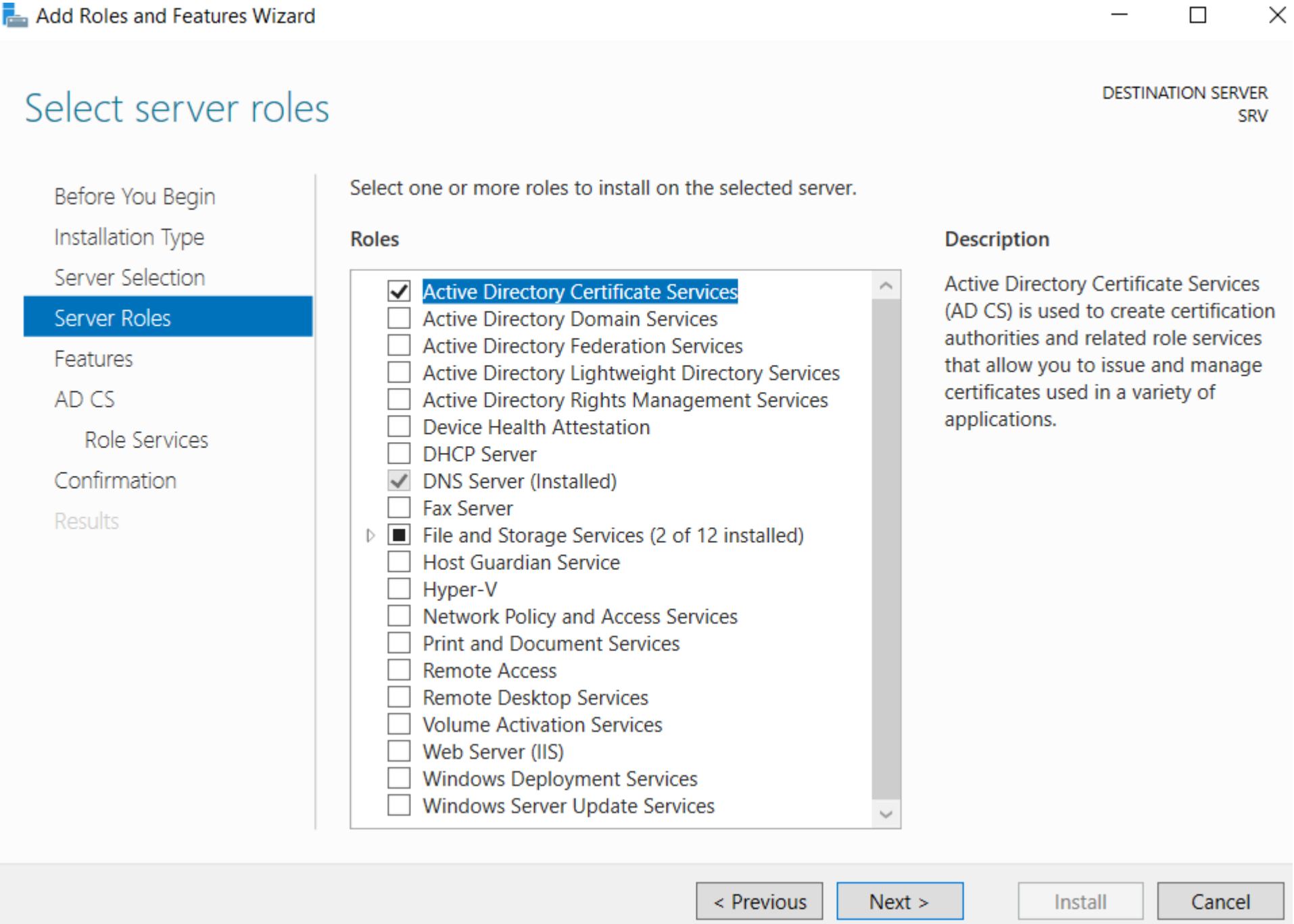
Запустить “Server Manager” и установить роль Центра Сертификации

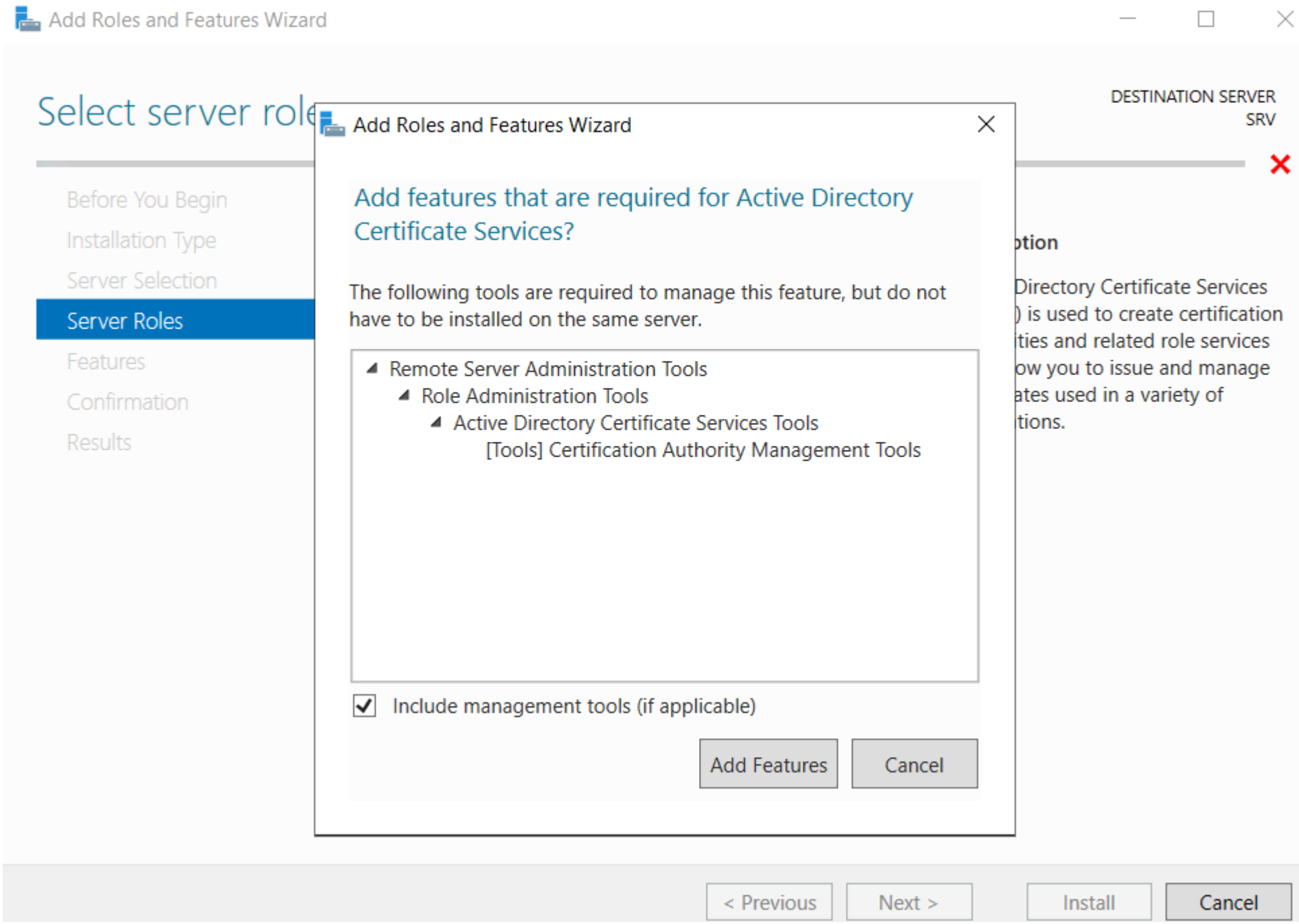

Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties

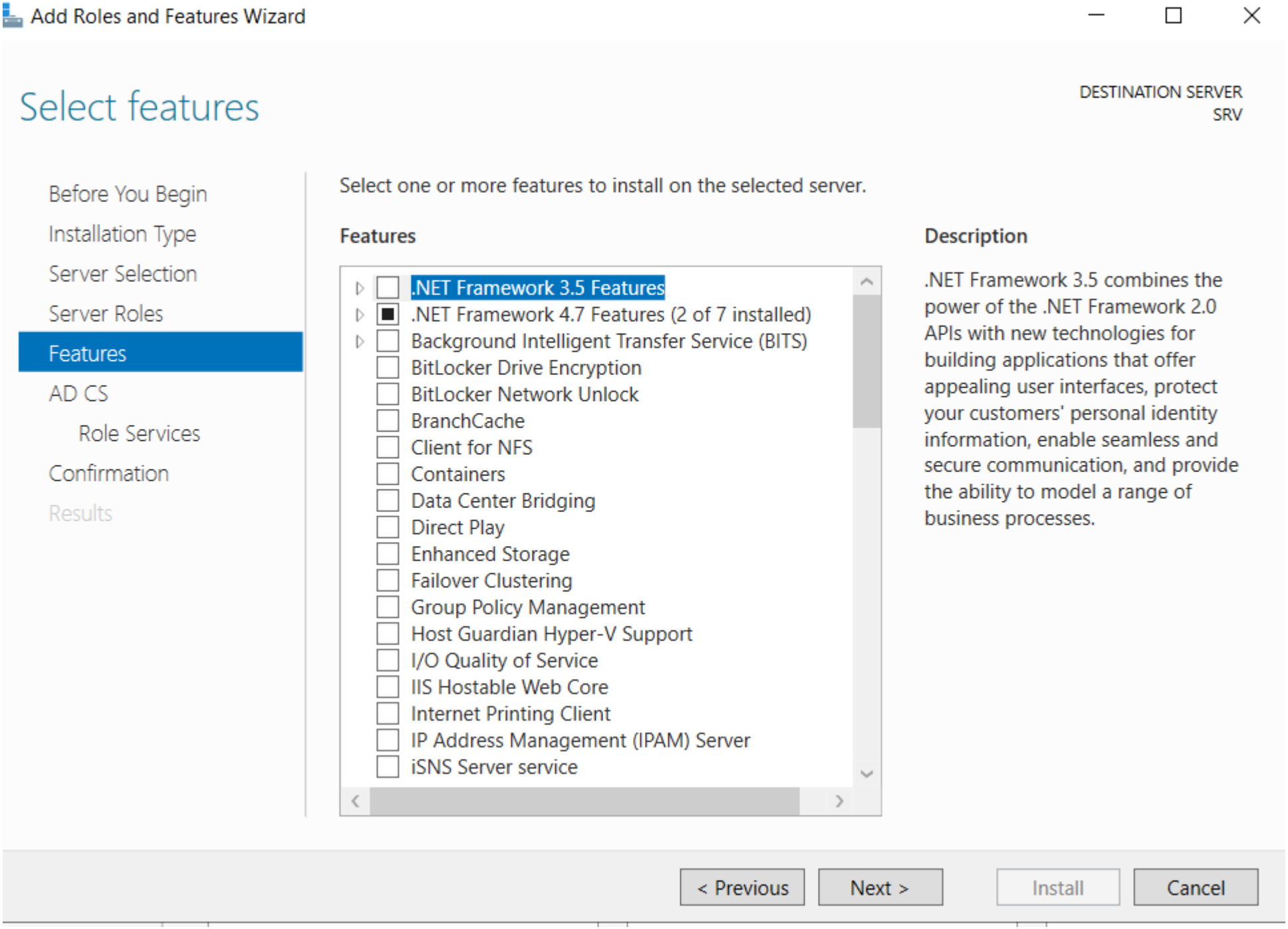

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



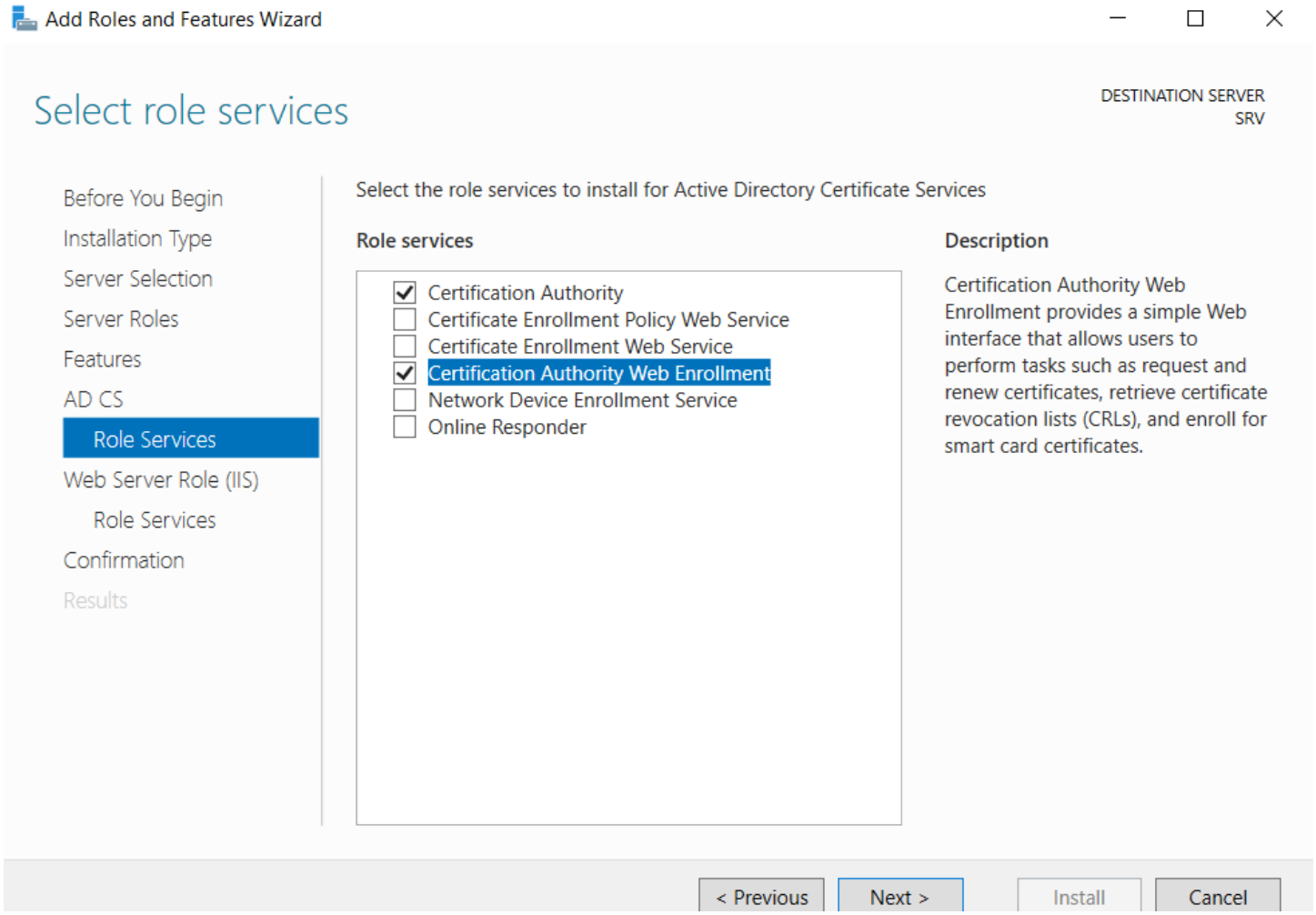
Установить “Active Directory Certificate Services”

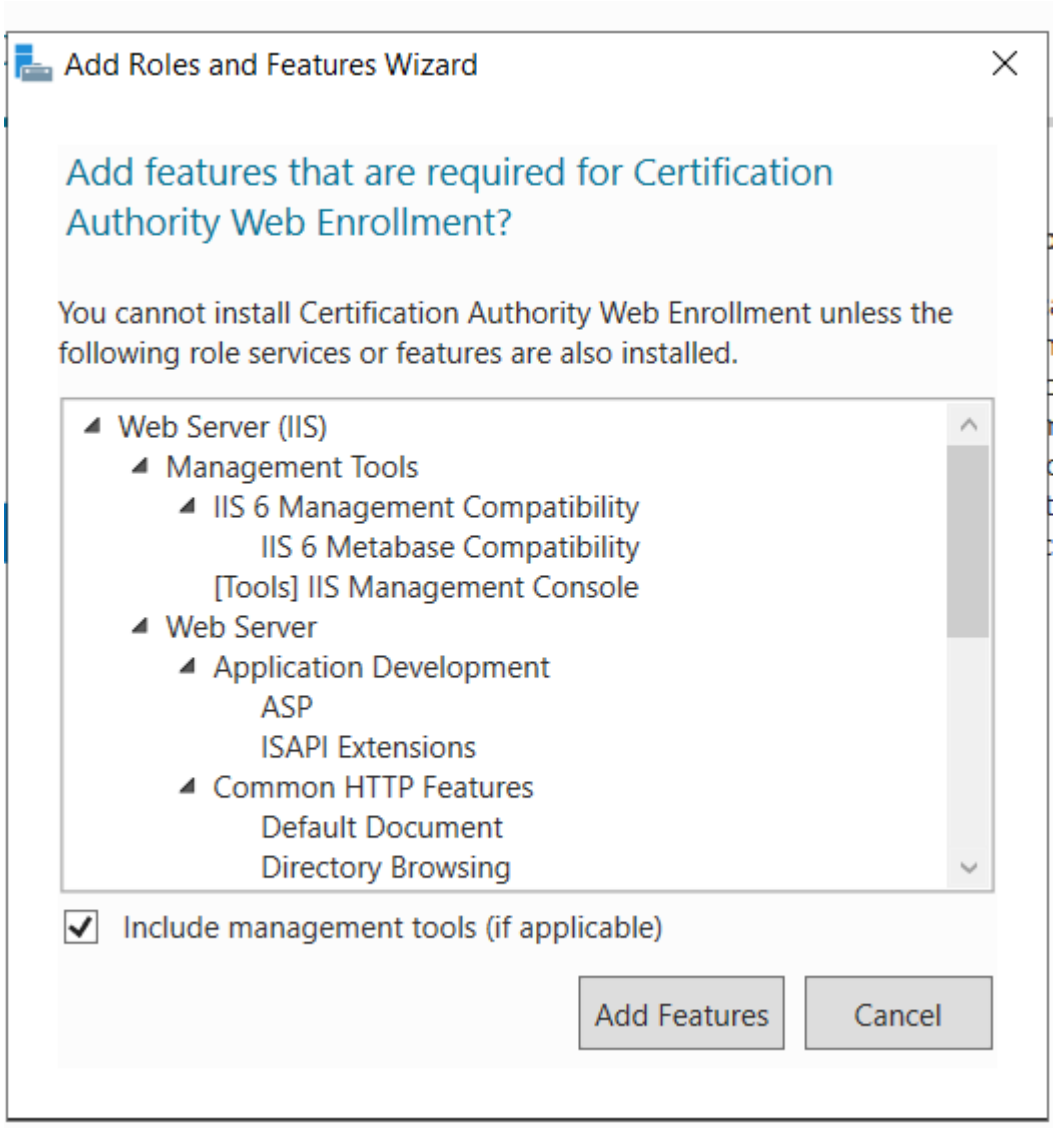

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select server role
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Certificate Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
[Tools] Certification Authority Management Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel

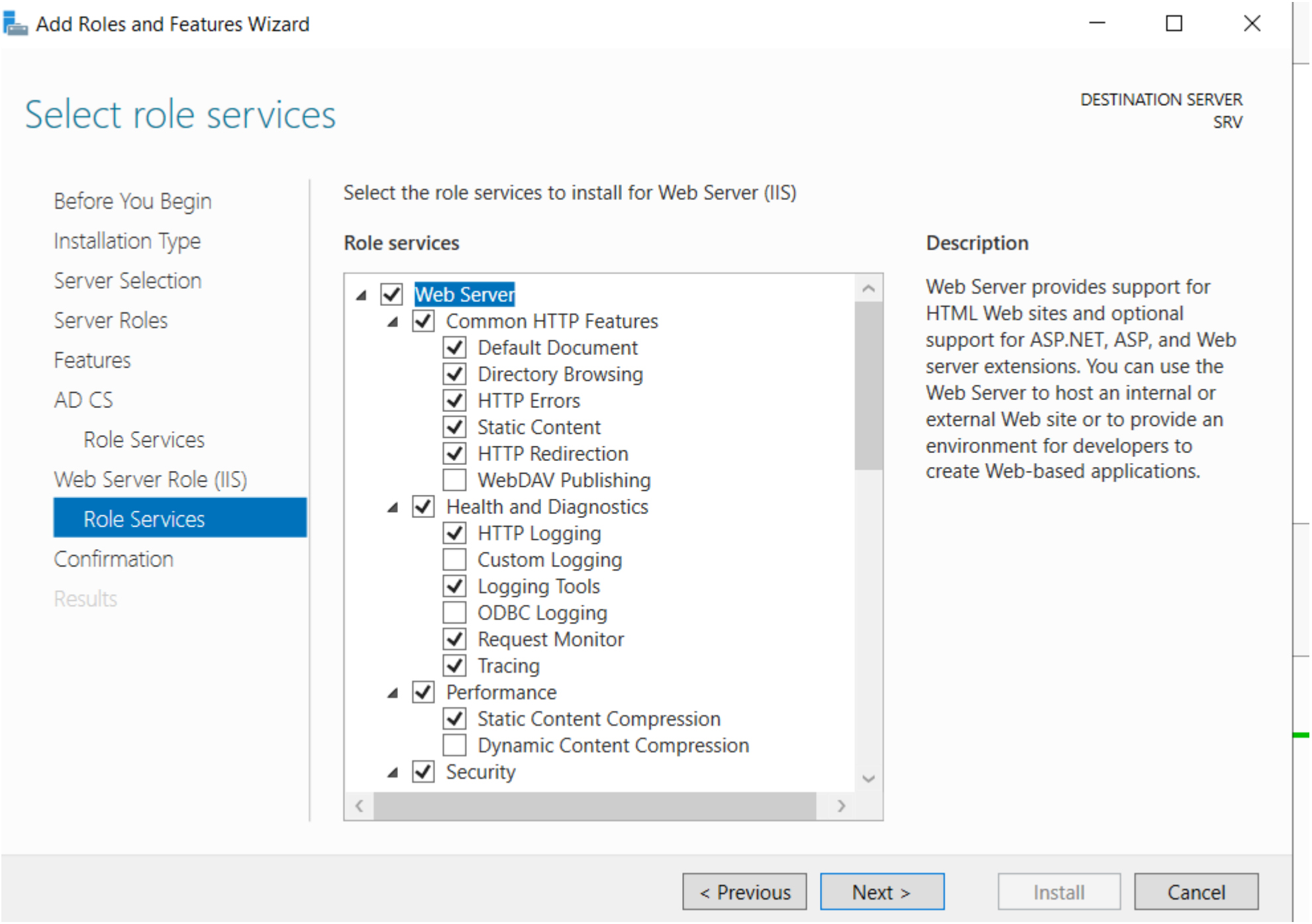

Add Roles and Features Wizard
Select features
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.7 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

Установить роль сервиса “Certification Authority Web Enrollment”





Далее везде “Next” и в конце Install


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
SRV
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
SRV

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
  - Role Services
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
- Certification Authority
- Certification Authority Web Enrollment

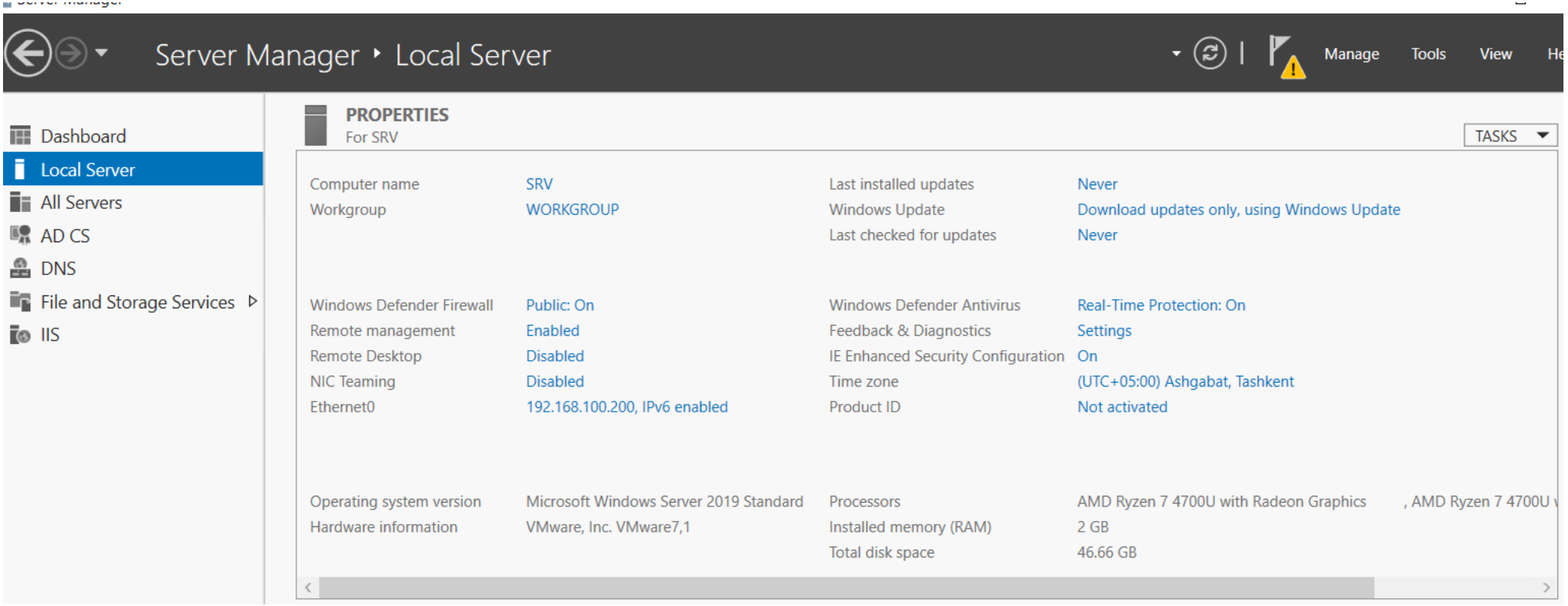
Remote Server Administration Tools
- Role Administration Tools
  - Active Directory Certificate Services Tools
    - Certification Authority Management Tools

Web Server (IIS)
- Management Tools
  - IIS 6 Management Compatibility

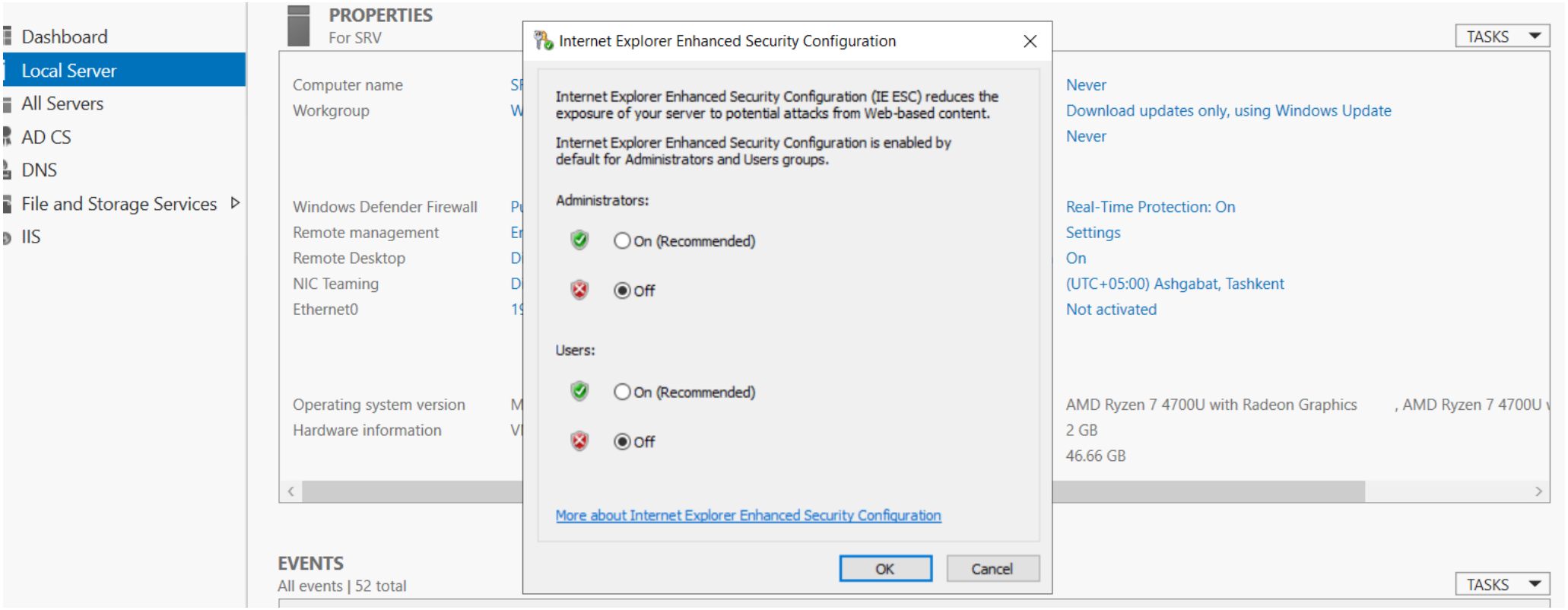
Export configuration settings
Specify an alternate source path

< Previous | Next > | Install | Cancel

Открыть “Server Manager” => “Local Server” => Нажать на On в строке “IE Enhanced Security Configuration”



Поставить в положение “Off”



В Server Manager выбрать Флажок и сообщение “Configure Active Directory Certificate Services on the”

AD CS Configuration

Credentials

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Confirmation
- Progress
- Results

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

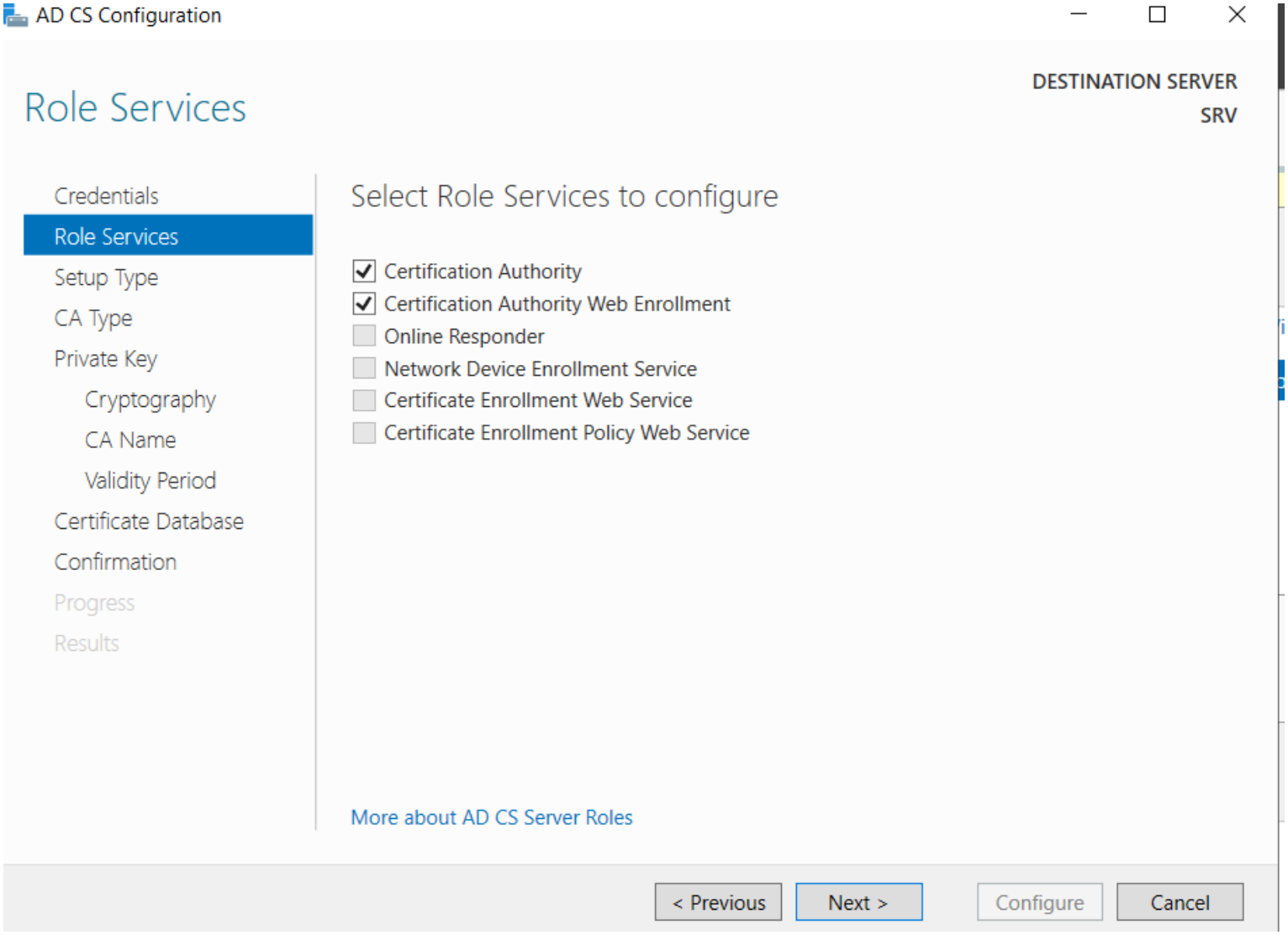
- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: SRV\Administrator Change...

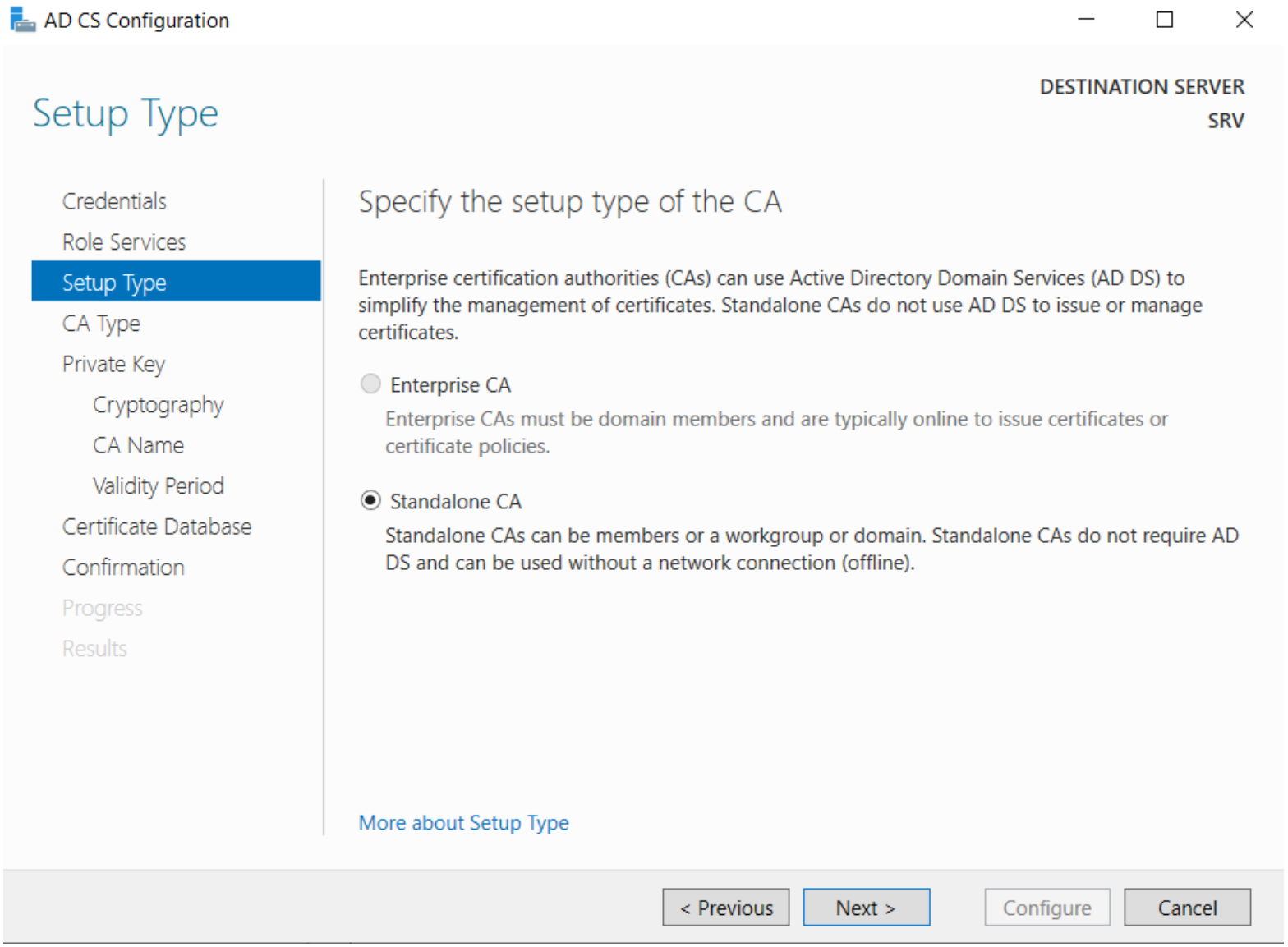
More about AD CS Server Roles

< Previous | Next > | Configure | Cancel

Выбрать два пункта:



Выбрать “Standalone CA”



AD CS Configuration

CA Type

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

(•) Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

( ) Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

< Previous | Next > | Configure | Cancel

AD CS Configuration

Private Key

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- **Private Key**
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

(•) Create a new private key

Use this option if you do not have a private key or want to create a new private key.

( ) Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

( ) Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

( ) Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

< Previous | Next > | Configure | Cancel

AD CS Configuration

Cryptography for CA

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the cryptographic options

Select a cryptographic provider:

RSA#Microsoft Software Key Storage Provider

Key length:

2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

< Previous | Next > | Configure | Cancel

AD CS Configuration

CA Name

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Demo.wsr

Distinguished name suffix:

Preview of distinguished name:

CN=Demo.wsr

More about CA Name

< Previous | Next > | Configure | Cancel

AD CS Configuration

Validity Period

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 3/6/2027 10:54:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

More about Validity Period

< Previous | Next > | Configure | Cancel

AD CS Configuration

CA Database

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the database locations

Certificate database location:

C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

More about CA Database

< Previous | Next > | Configure | Cancel

AD CS Configuration

Confirmation

DESTINATION SERVER
SRV

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

To configure the following roles, role services, or features, click Configure.

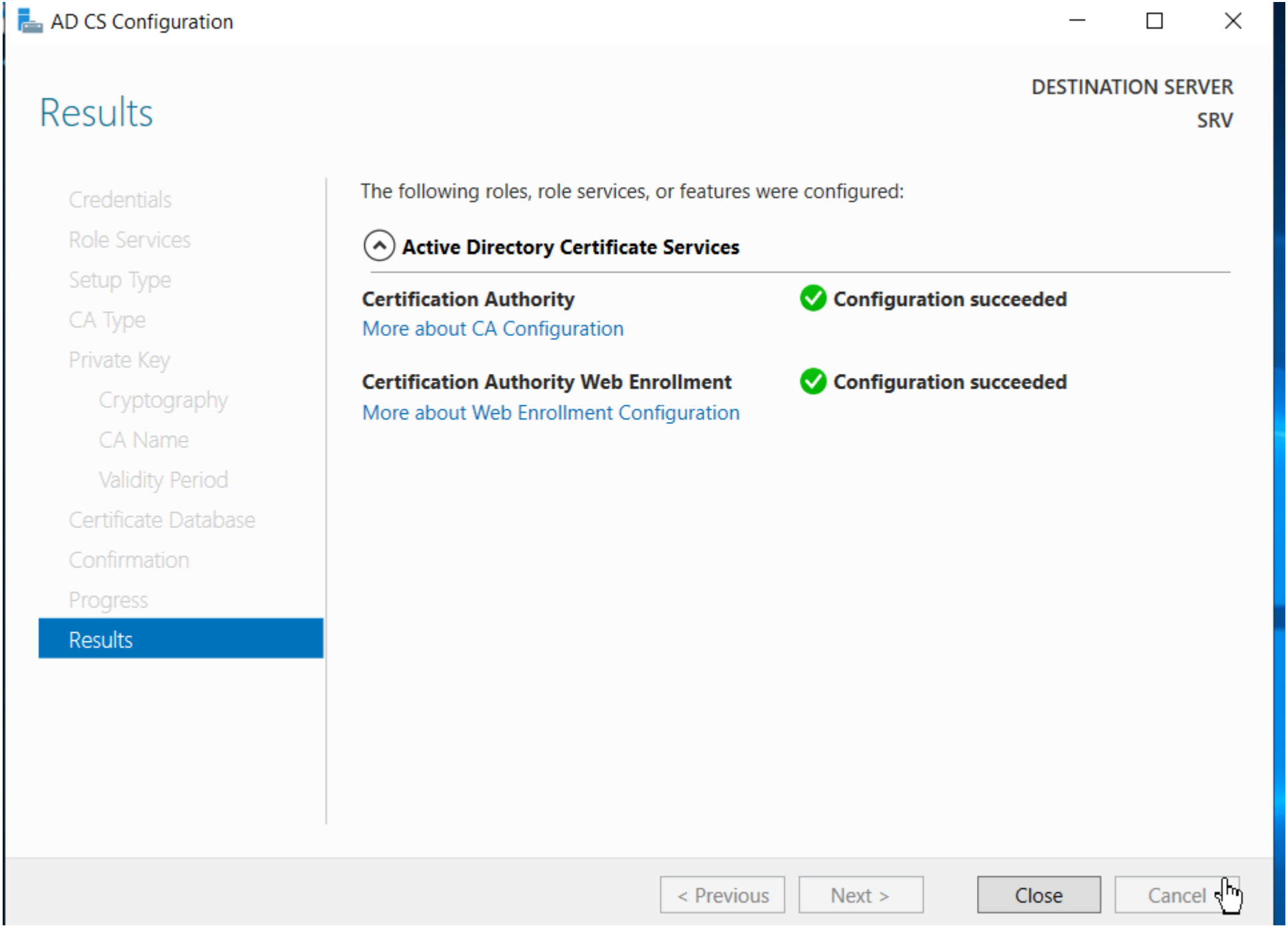
Active Directory Certificate Services

Certification Authority

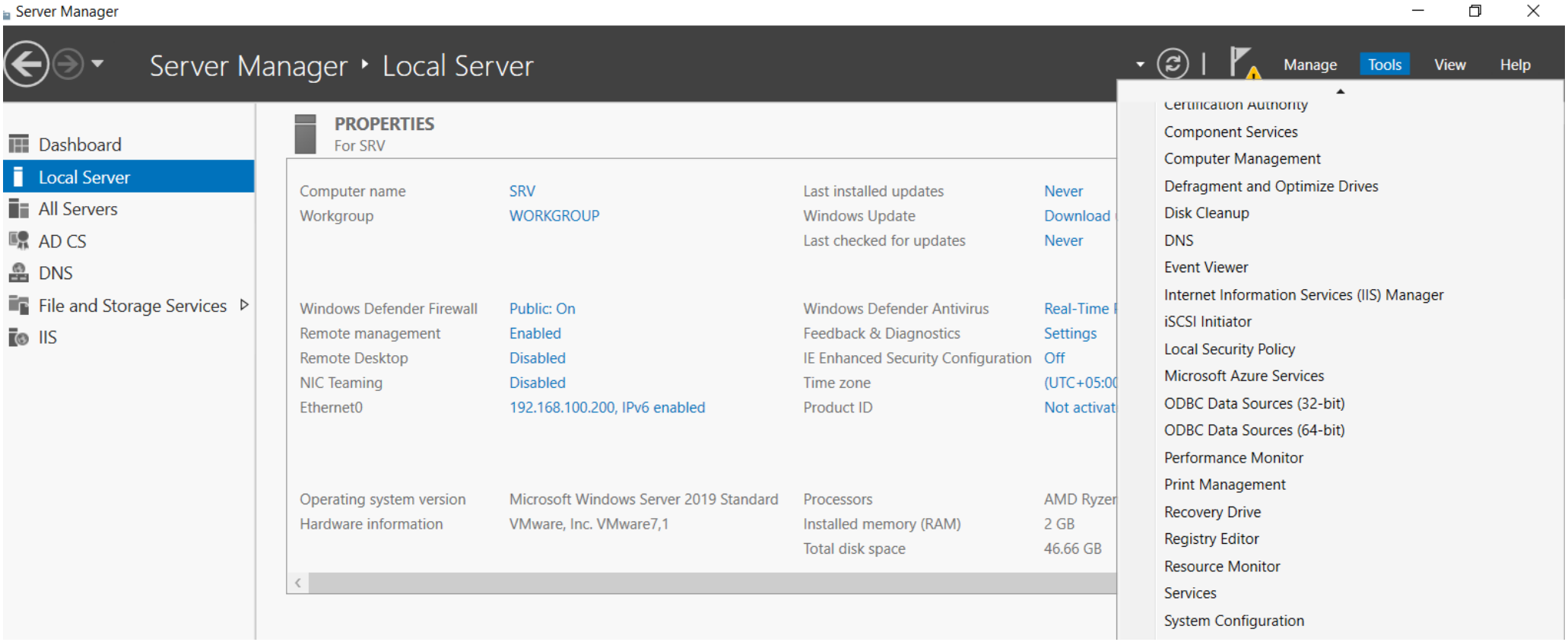
CA Type:	Standalone Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	3/6/2027 10:54:00 AM
Distinguished Name:	CN=Demo.wsr
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Certification Authority Web Enrollment

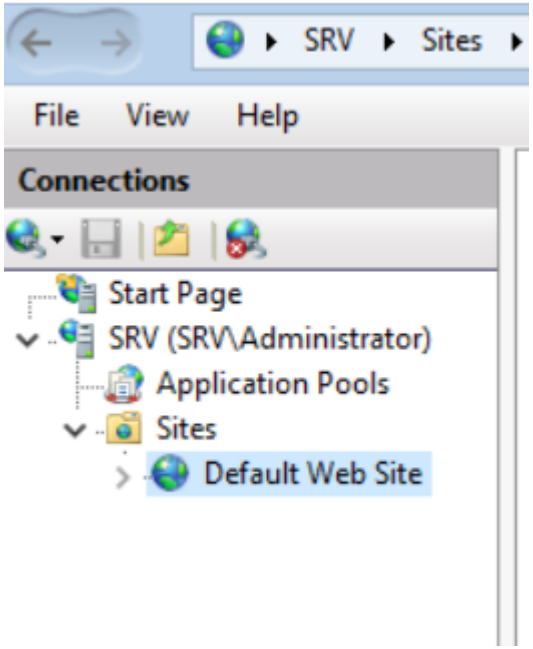
< Previous | Next > | Configure | Cancel


AD CS Configuration
Results
DESTINATION SERVER
SRV
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
The following roles, role services, or features were configured:
Active Directory Certificate Services
Certification Authority
Configuration succeeded
More about CA Configuration
Certification Authority Web Enrollment
Configuration succeeded
More about Web Enrollment Configuration
< Previous
Next >
Close
Cancel

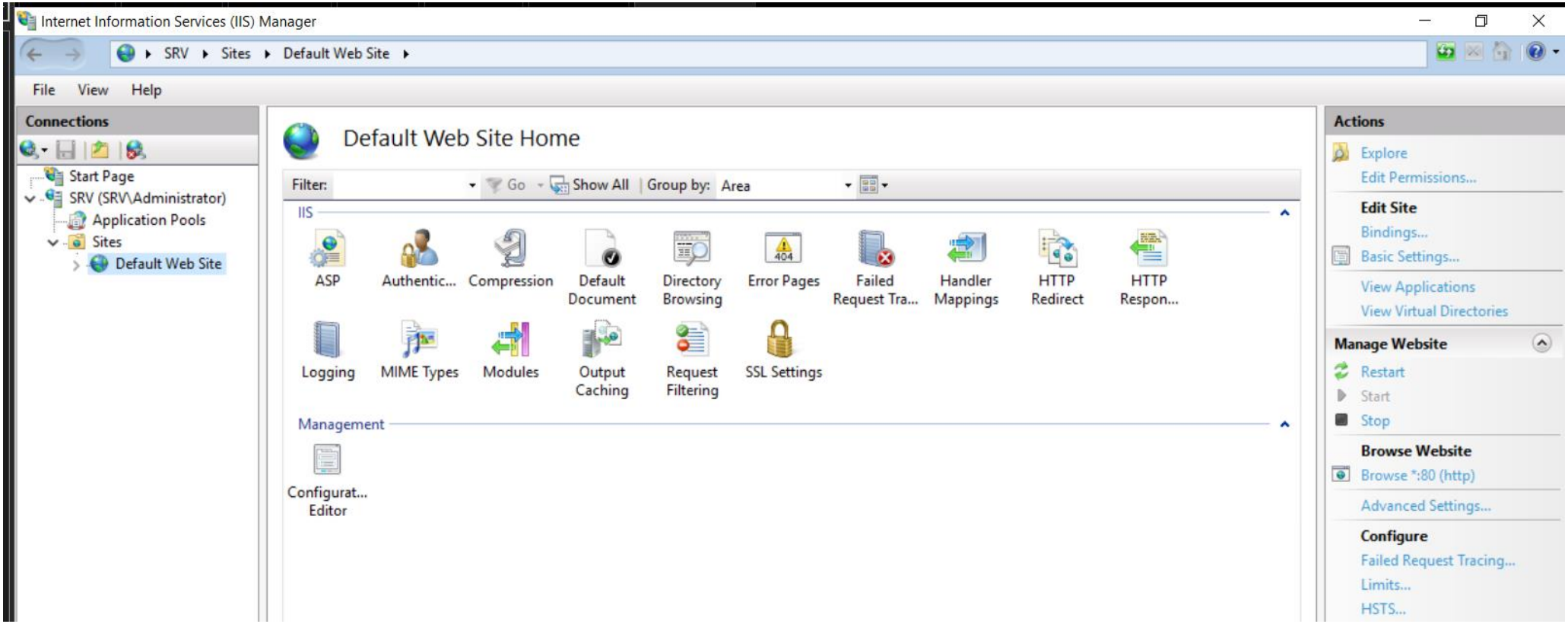
В Server Manager выбрать Tools => Internet Information Services (IIS) Manager

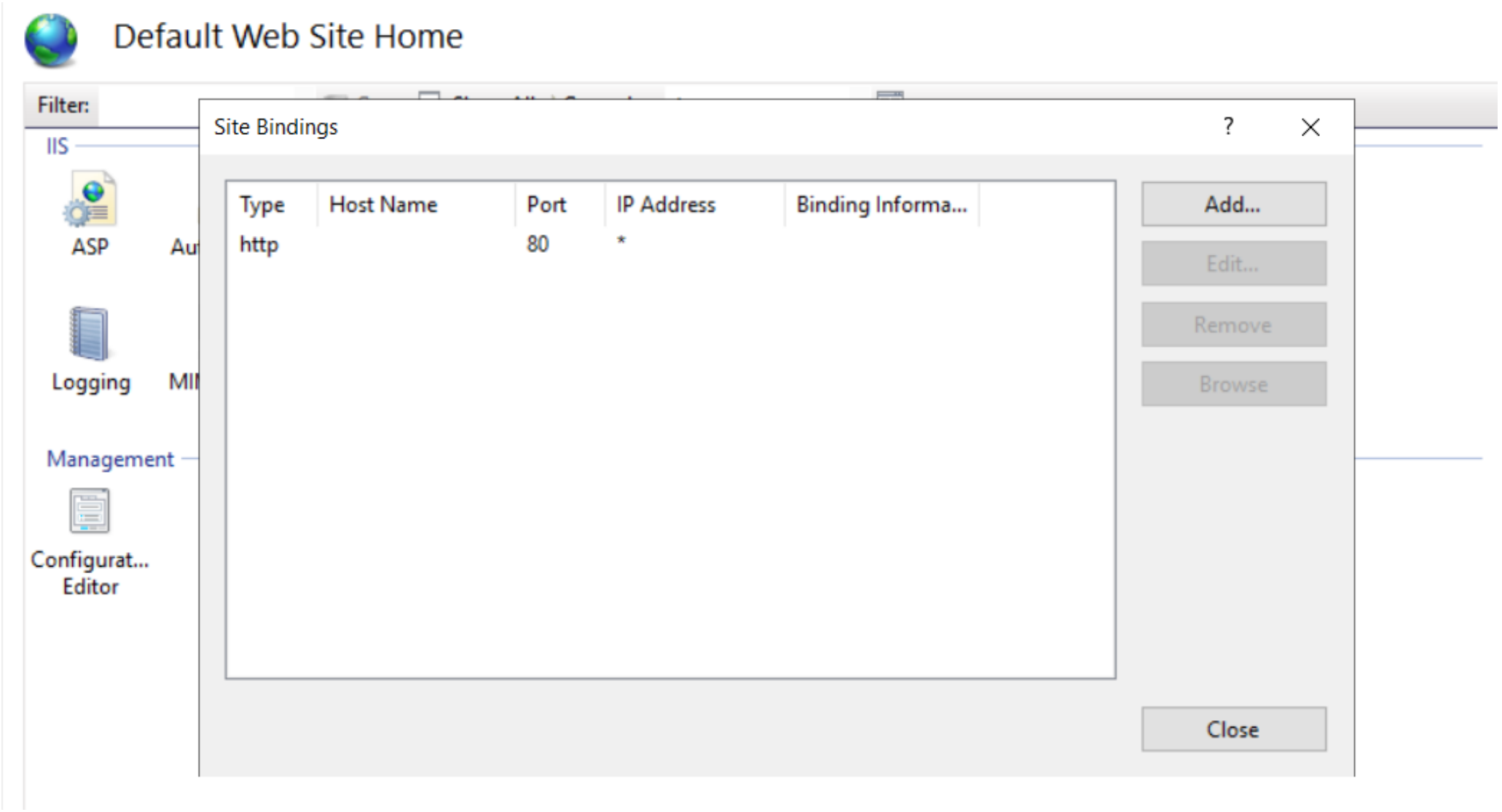


Слева выбрать SRV => Sites => Default Web Site

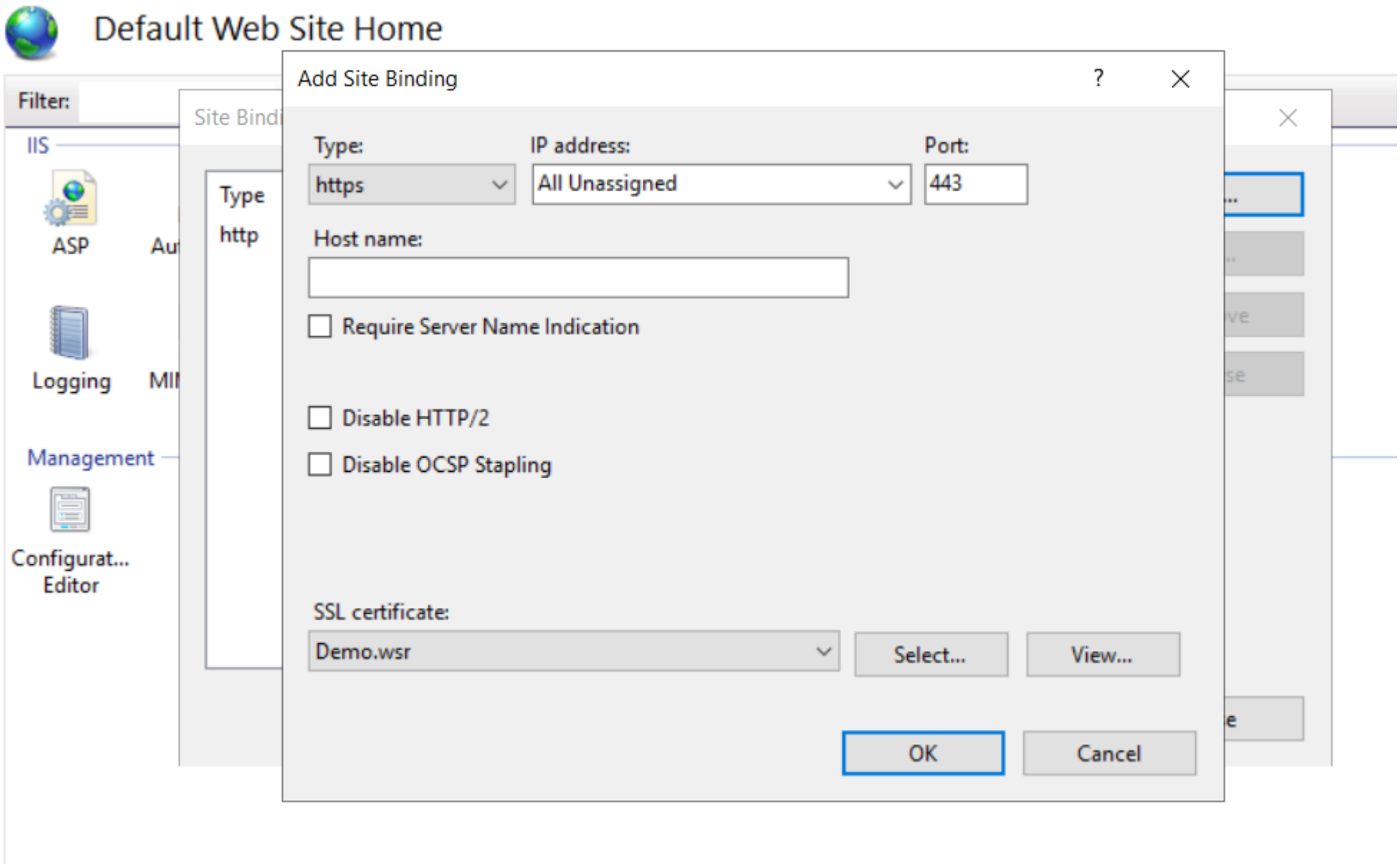


С права выбрать Bindings

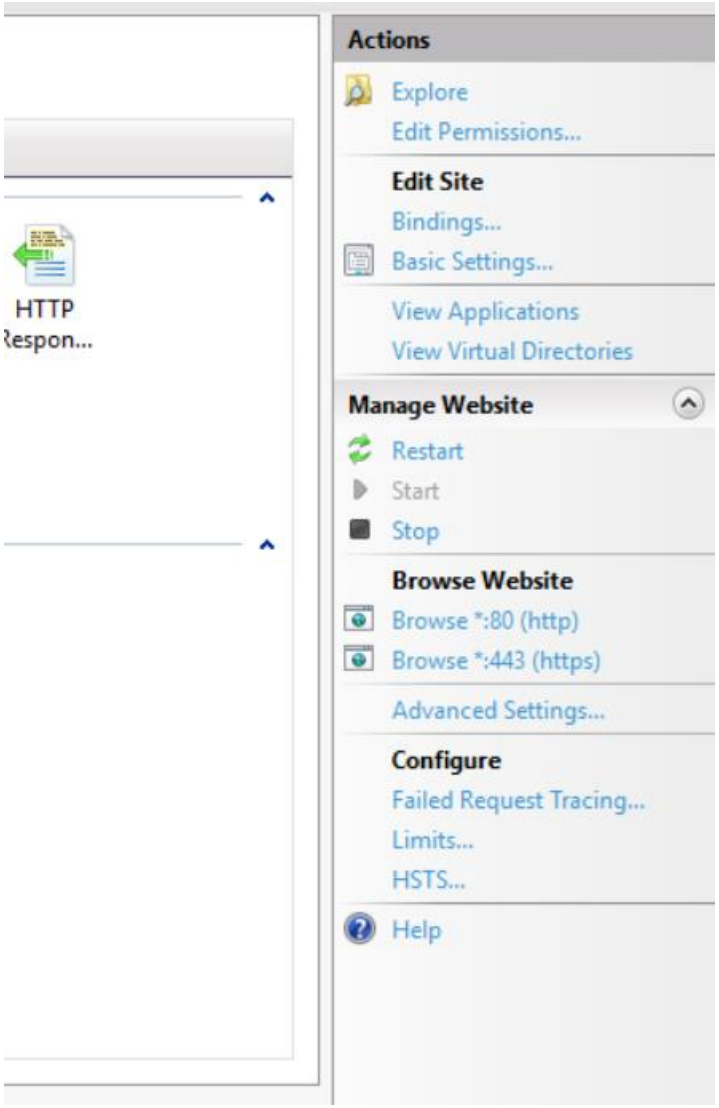

Internet Information Services (IIS) Manager
SRV ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
SRV (SRV\Administrator)
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
IIS
ASP
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
HSTS...


Default Web Site Home
Filter:
IIS
ASP
Logging
Management
Configurat...
Editor
Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
http
80
*
Add...
Edit...
Remove
Browse
Close

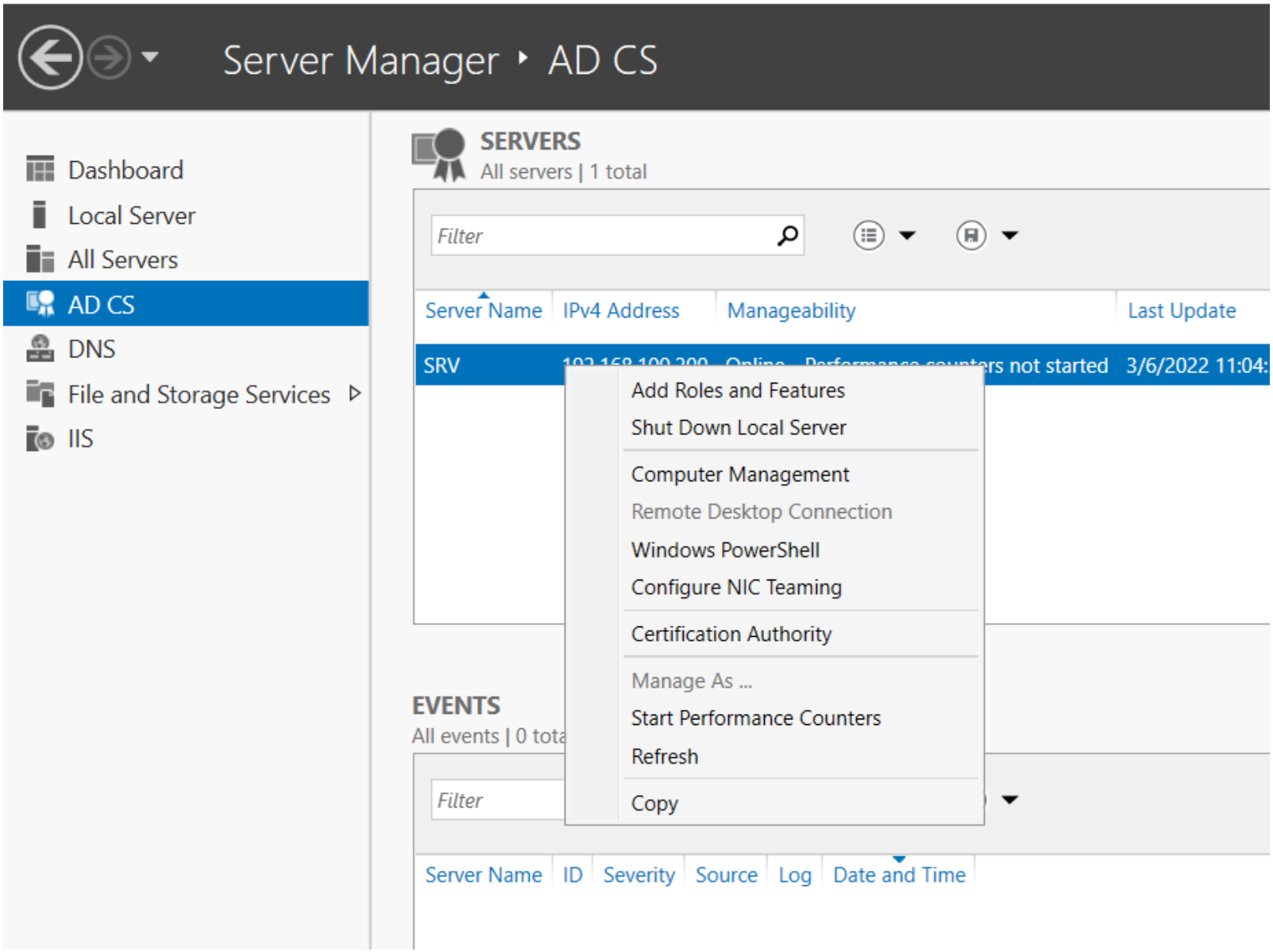
Выбрать “Add”

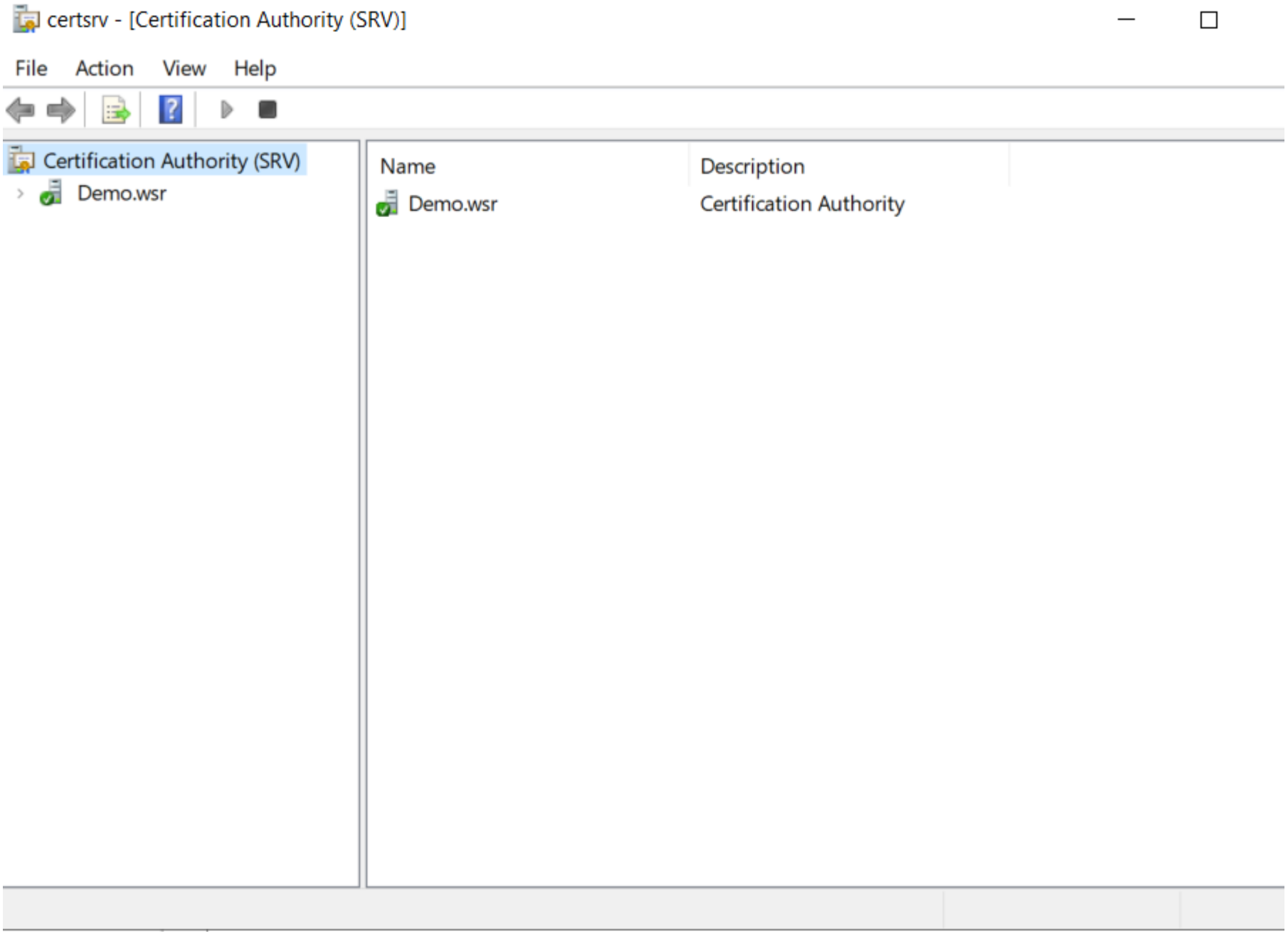

Default Web Site Home
Filter:
IIS
ASP
Logging
Management
Configurat...
Editor
Site Bindi
Type
http
Add Site Binding
Type:
https
IP address:
All Unassigned
Port:
443
Host name:
Require Server Name Indication
Disable HTTP/2
Disable OCSP Stapling
SSL certificate:
Demo.wsr
Select...
View...
OK
Cancel

Выбрать Restart

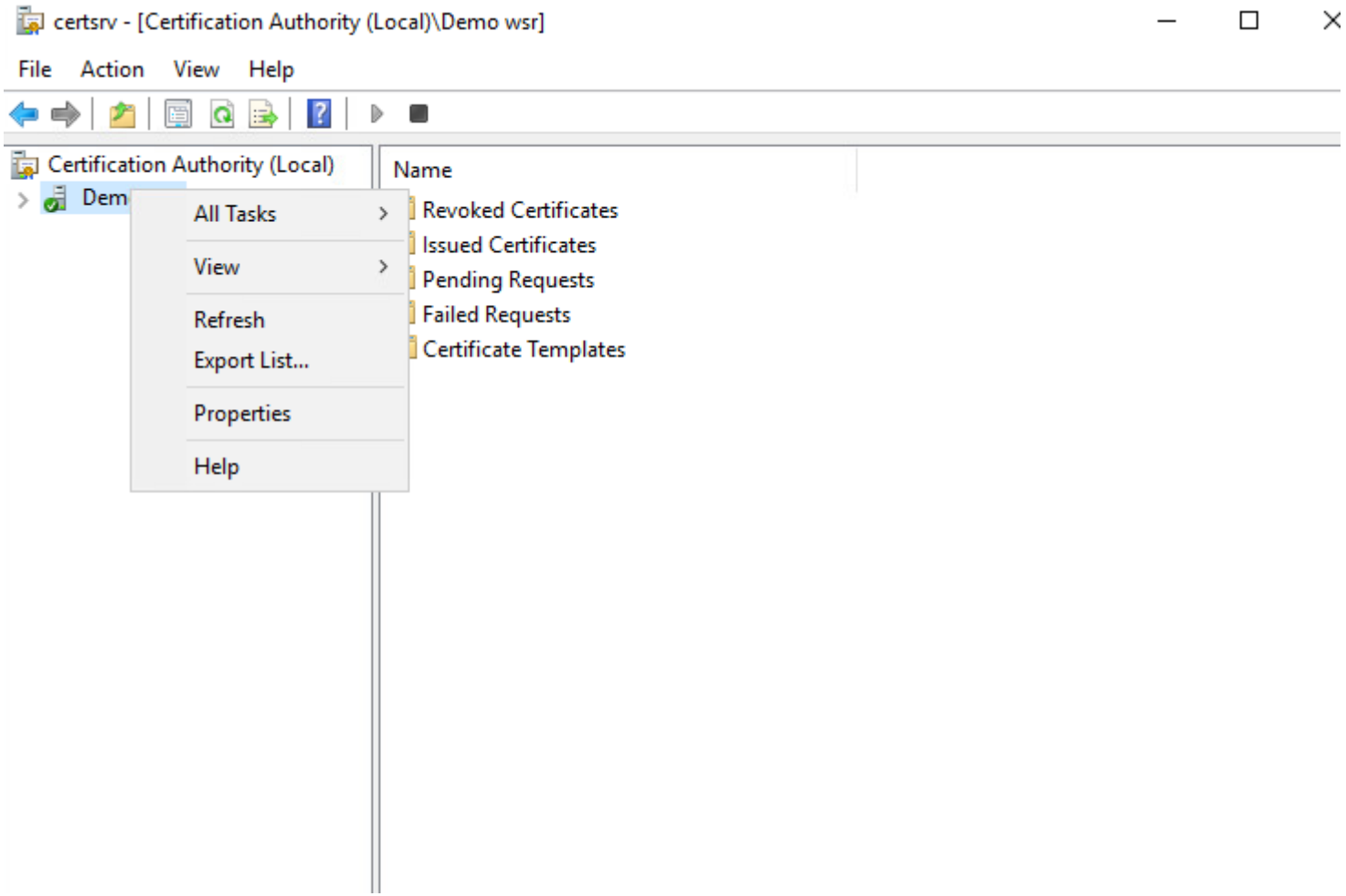


В Server Manager выбрать AD CS => нажать правой клавишей на SRV и выбрать “Certification Authority”

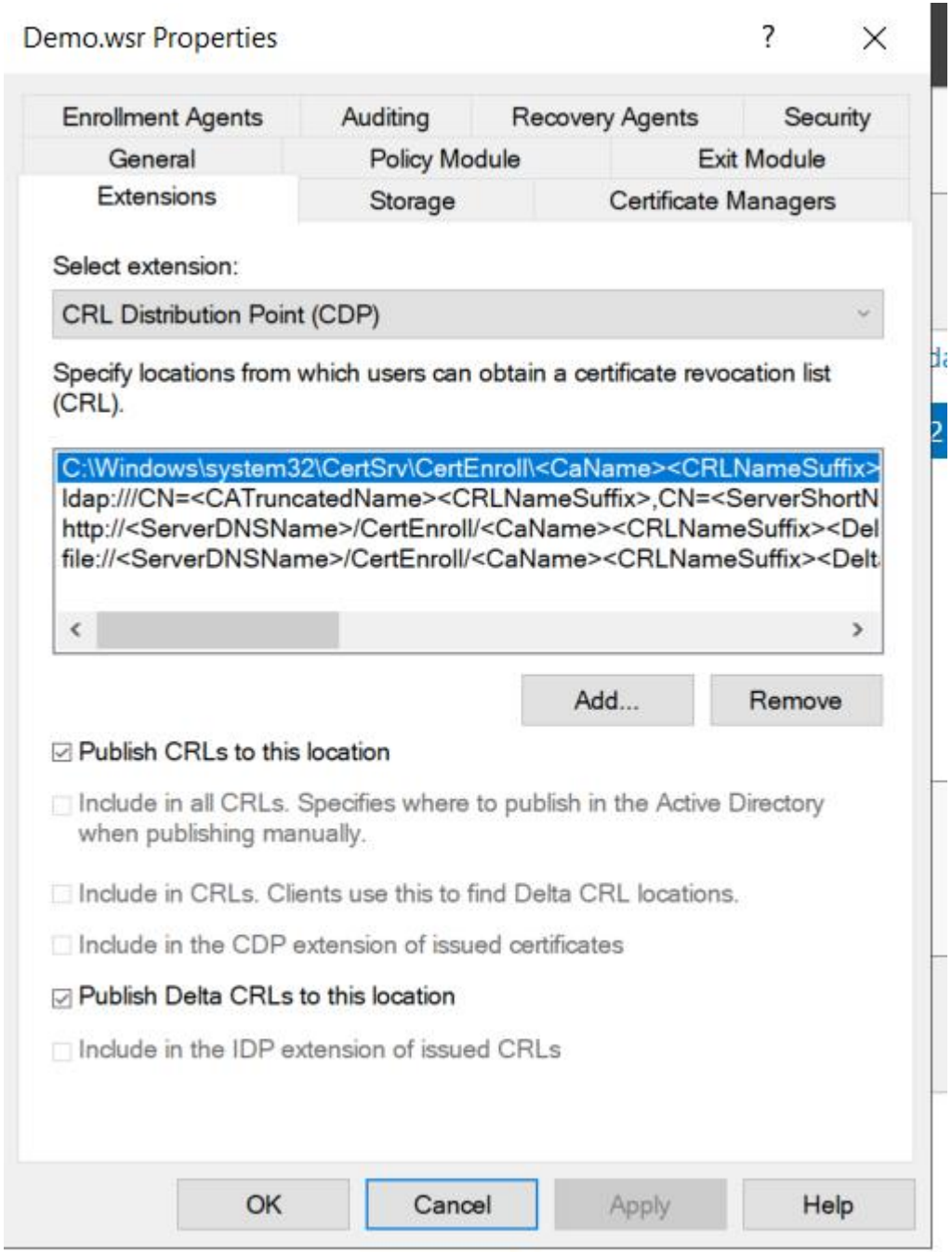


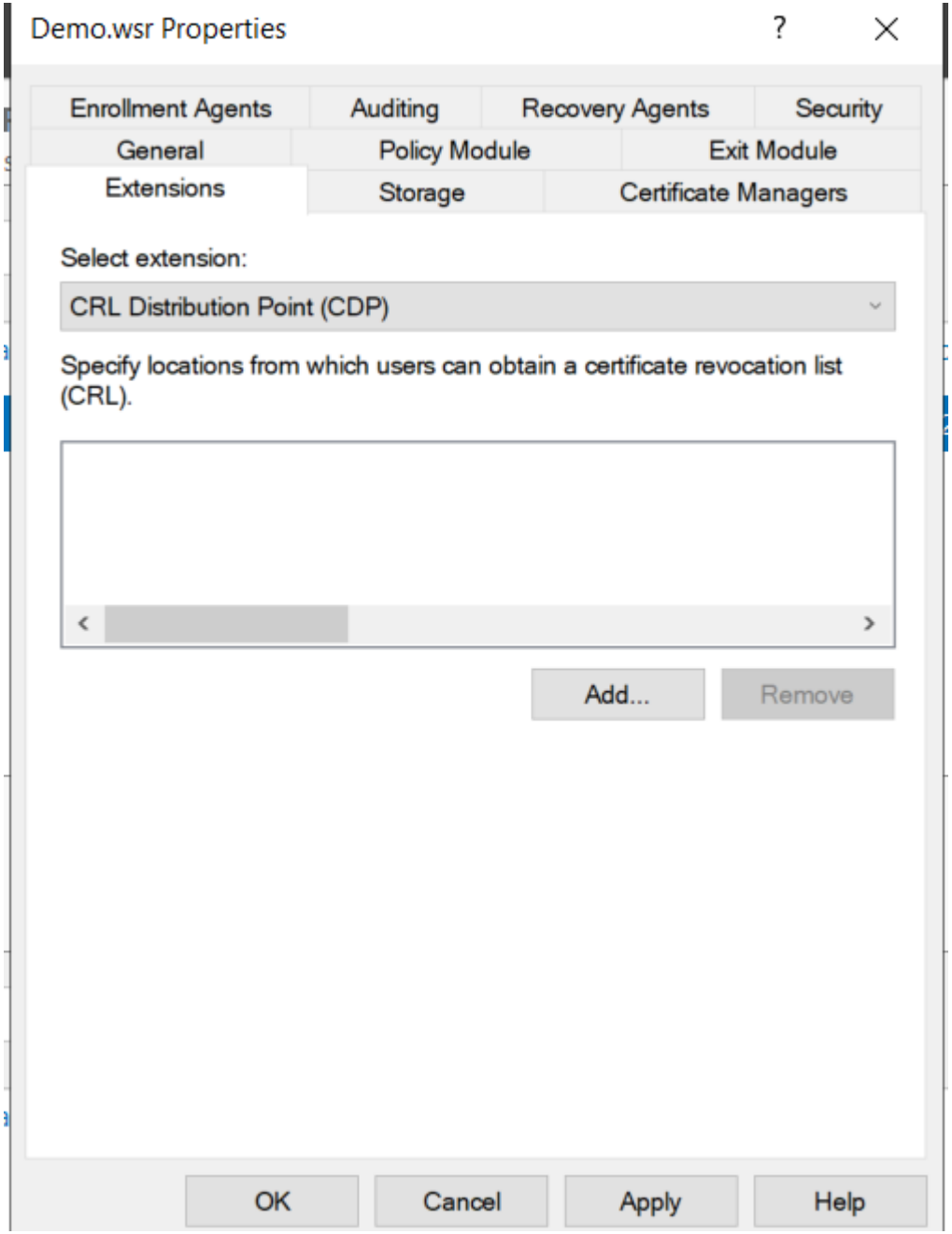

certsrv - [Certification Authority (SRV)]
File
Action
View
Help
Certification Authority (SRV)
Demo.wsr
Name
Description
Demo.wsr
Certification Authority

Правой клавишей на “Demo.wsr” и выбрать “Properties”

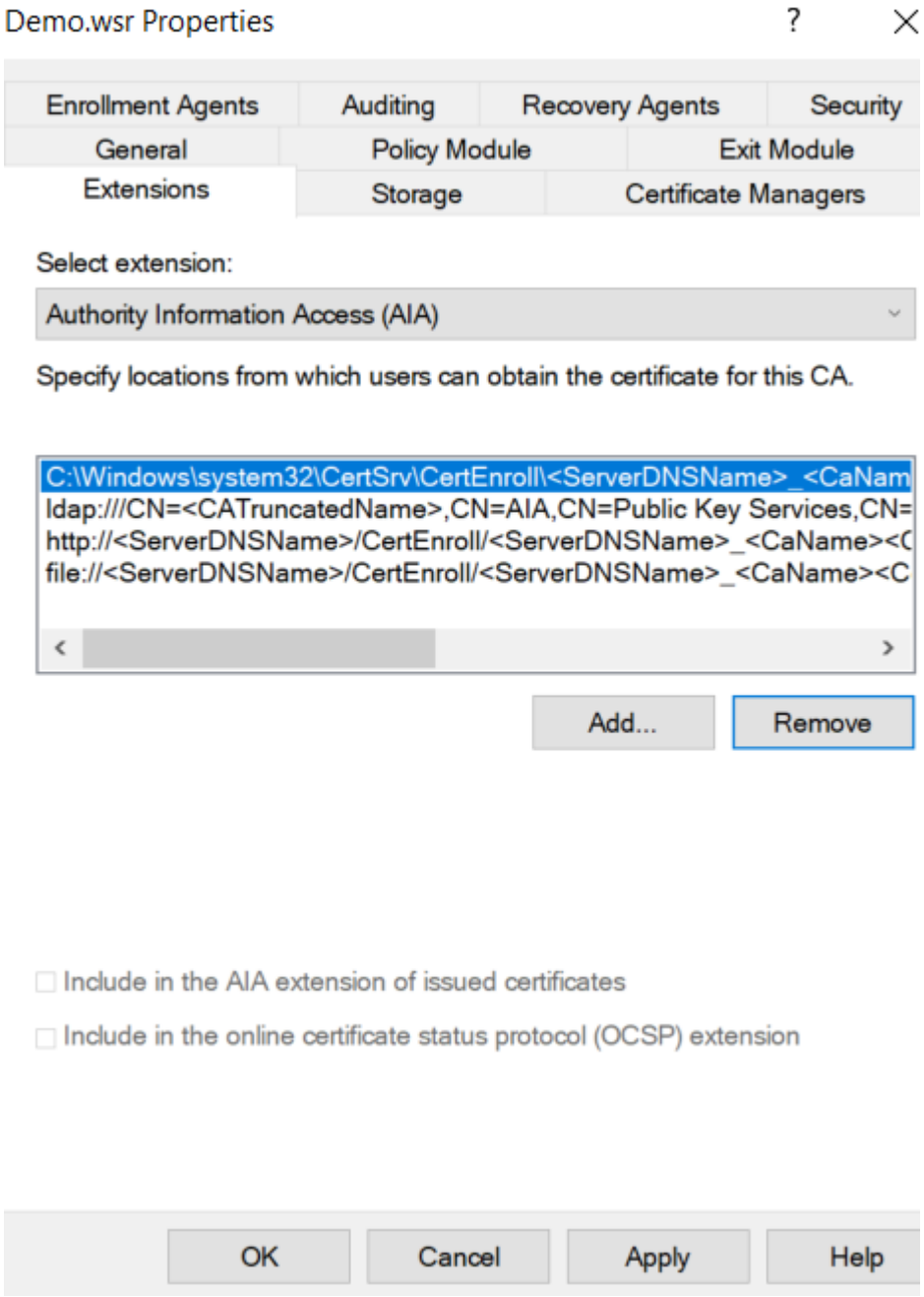


Выбрать вкладку “Extensions” и удалить все ключи

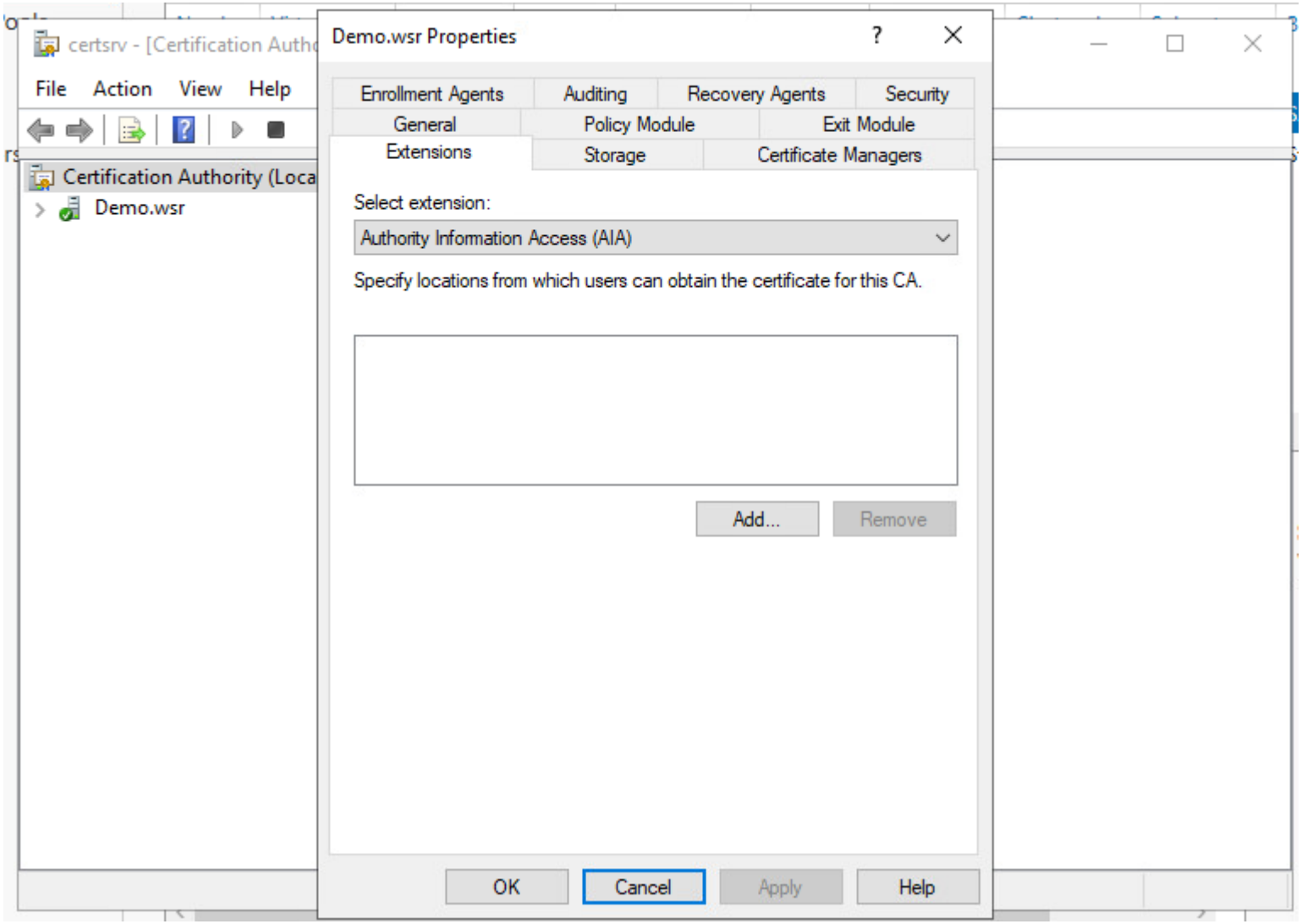

Demo.wsr Properties
Enrollment Agents
Auditing
Recovery Agents
Security
General
Policy Module
Exit Module
Extensions
Storage
Certificate Managers
Select extension:
CRL Distribution Point (CDP)
Specify locations from which users can obtain a certificate revocation list (CRL).
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortN
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Del
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delt
Add...
Remove
Publish CRLs to this location
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.
Include in CRLs. Clients use this to find Delta CRL locations.
Include in the CDP extension of issued certificates
Publish Delta CRLs to this location
Include in the IDP extension of issued CRLs
OK
Cancel
Apply
Help



Переключить в Select extensions на Authority Information Access (AIA)


Demo.wsr Properties
Enrollment Agents
Auditing
Recovery Agents
Security
General
Policy Module
Exit Module
Extensions
Storage
Certificate Managers
Select extension:
Authority Information Access (AIA)
Specify locations from which users can obtain the certificate for this CA.
C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNam
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><C
file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><C
Add...
Remove
Include in the AIA extension of issued certificates
Include in the online certificate status protocol (OCSP) extension
OK
Cancel
Apply
Help

Удалить все ключи



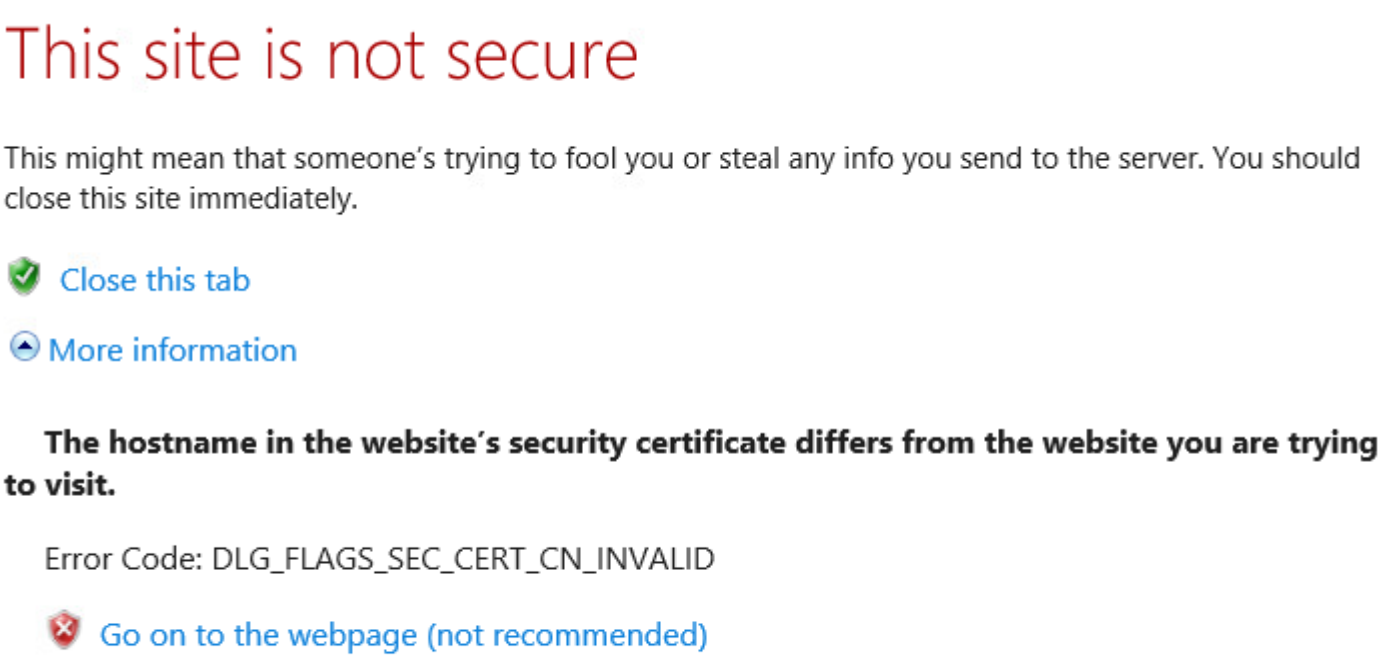
Применить и выйти

Открыть Internet Explorer

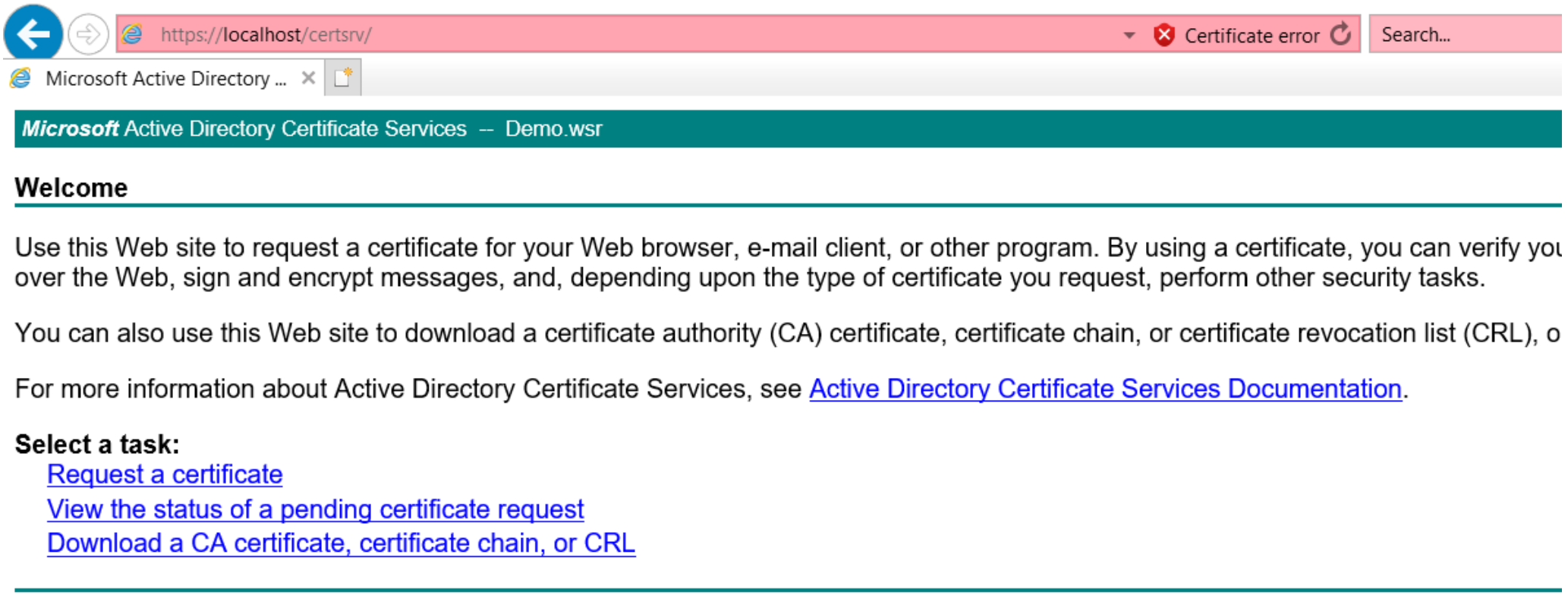
Перейти по адресу:

https://localhost/certsrv

Выбрать “More information”



Нажать “Go on to the webpage (not recommended)”



Выбрать “request a certificate”

Microsoft Active Directory Certificate Services -- Demo.wsr

Request a Certificate

Select the certificate type:

Web Browser Certificate

E-Mail Protection Certificate

Or, submit an advanced certificate request.

Выбрать “advanced certificate request”

Microsoft Active Directory Certificate Services -- Demo.wsr Home

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Выбрать “Create and submit a request to this CA”

https://localhost/certsrv/certrqma.asp Certificate error Search...

ocalhost

crosoft Active Directory Certificate Services -- Demo.wsr

vanced Certificate Request

ntifying Information:

Name:
E-Mail:
Company:
Department:
City:
State:
ountry/Region:

e of Certificate Needed:

Client Authentication Certificate

y Options:

Create new key set Use existing key set
CSP: Loading...
Key Usage: Exchange Signature Both
Key Size: 0 Min: Max: (common key sizes:)
Automatic key container name User specified k

Web Access Confirmation

This Web site is attempting to perform a digital certificate operation on your behalf:

https://localhost/certsrv/certrqma.asp

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

Yes No

Нажать “Yes”

Заполнить информацию:

Name: www.demo.wsr

Company: demo.wsr

Region: RU

Type of Certificate Needed: Server Authentication Certificate

Key Size: 2048

Mark keys as exportable

https://localhost/certsrv/certrqma.asp Certificate error Search...

Microsoft Active Directory ...

Advanced Certificate Request

Identifying Information:

Name: www.demo.wsr
E-Mail:
Company: demo.wsr
Department:
City:
State:
Country/Region: RU

Type of Certificate Needed:

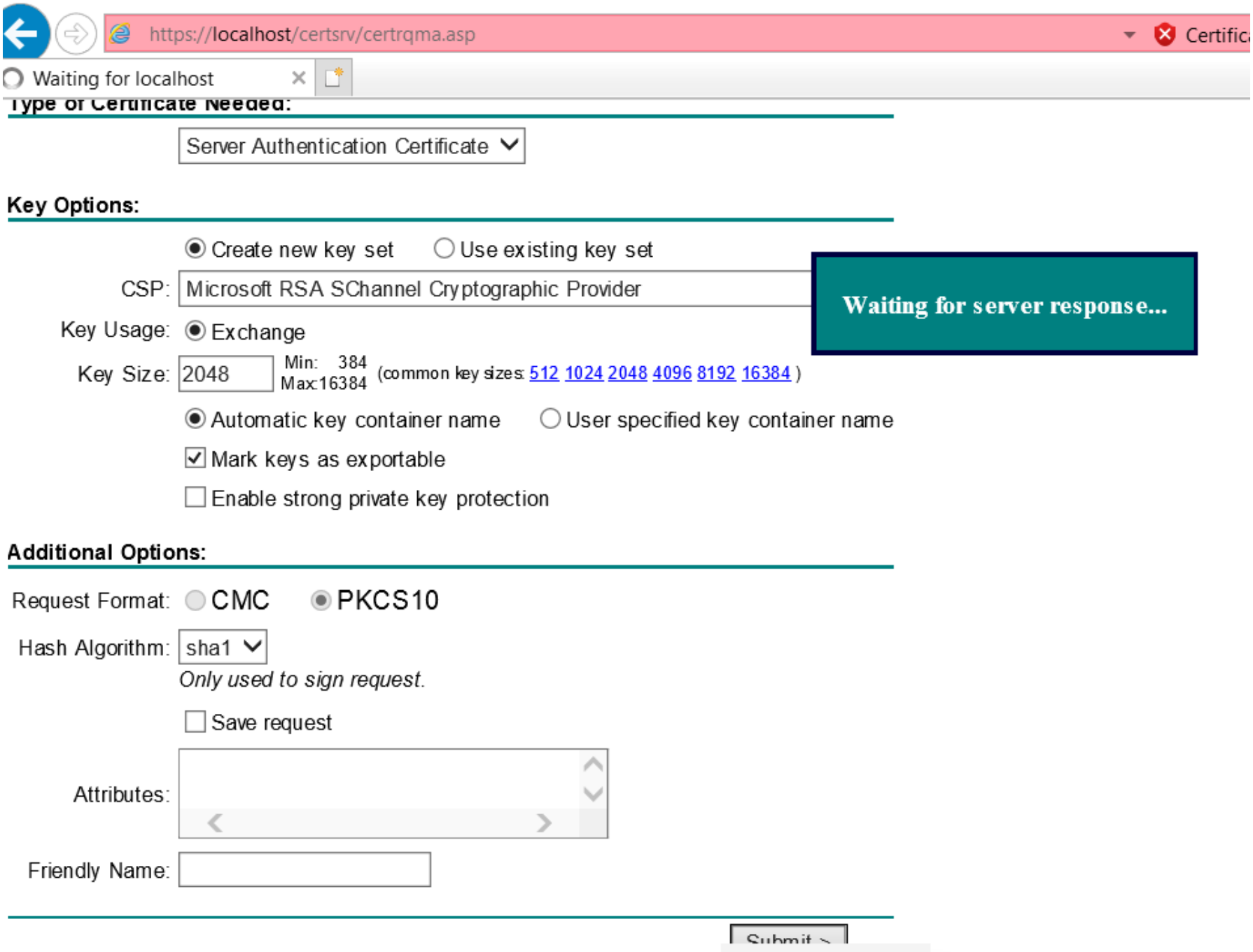
Server Authentication Certificate

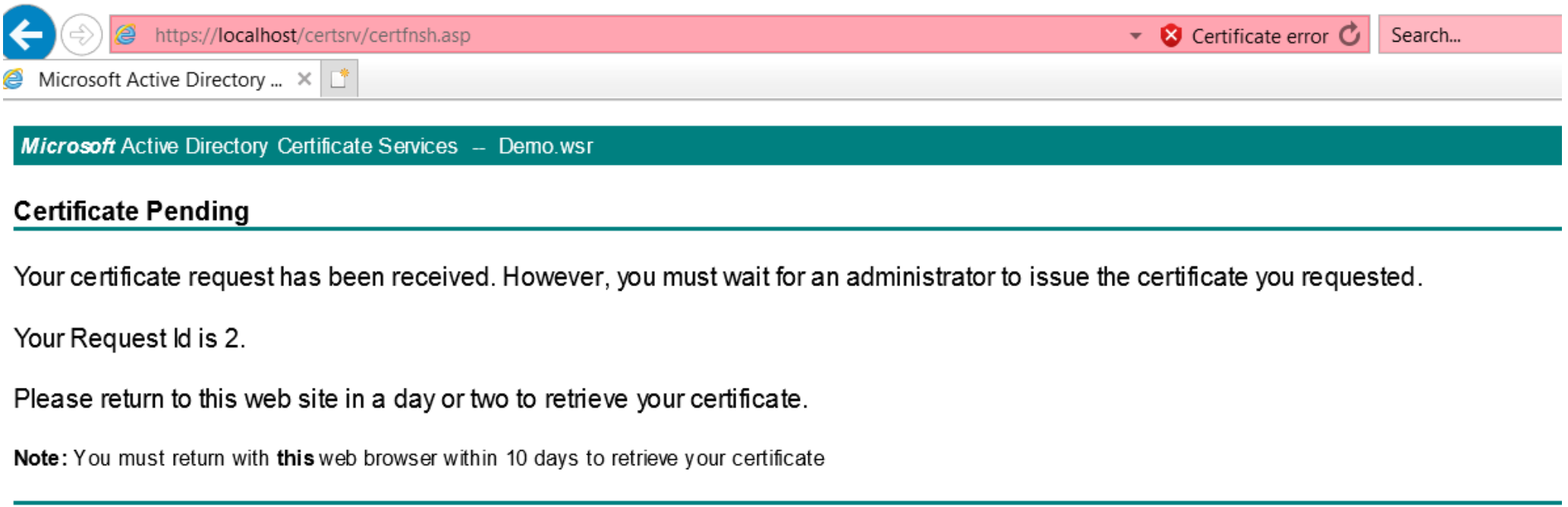
Key Options:

(•) Create new key set ( ) Use existing key set
CSP: Microsoft RSA SChannel Cryptographic Provider
Key Usage: (•) Exchange
Key Size: 2048 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)
(•) Automatic key container name ( ) User specified key container name
[x] Mark keys as exportable
[ ] Enable strong private key protection

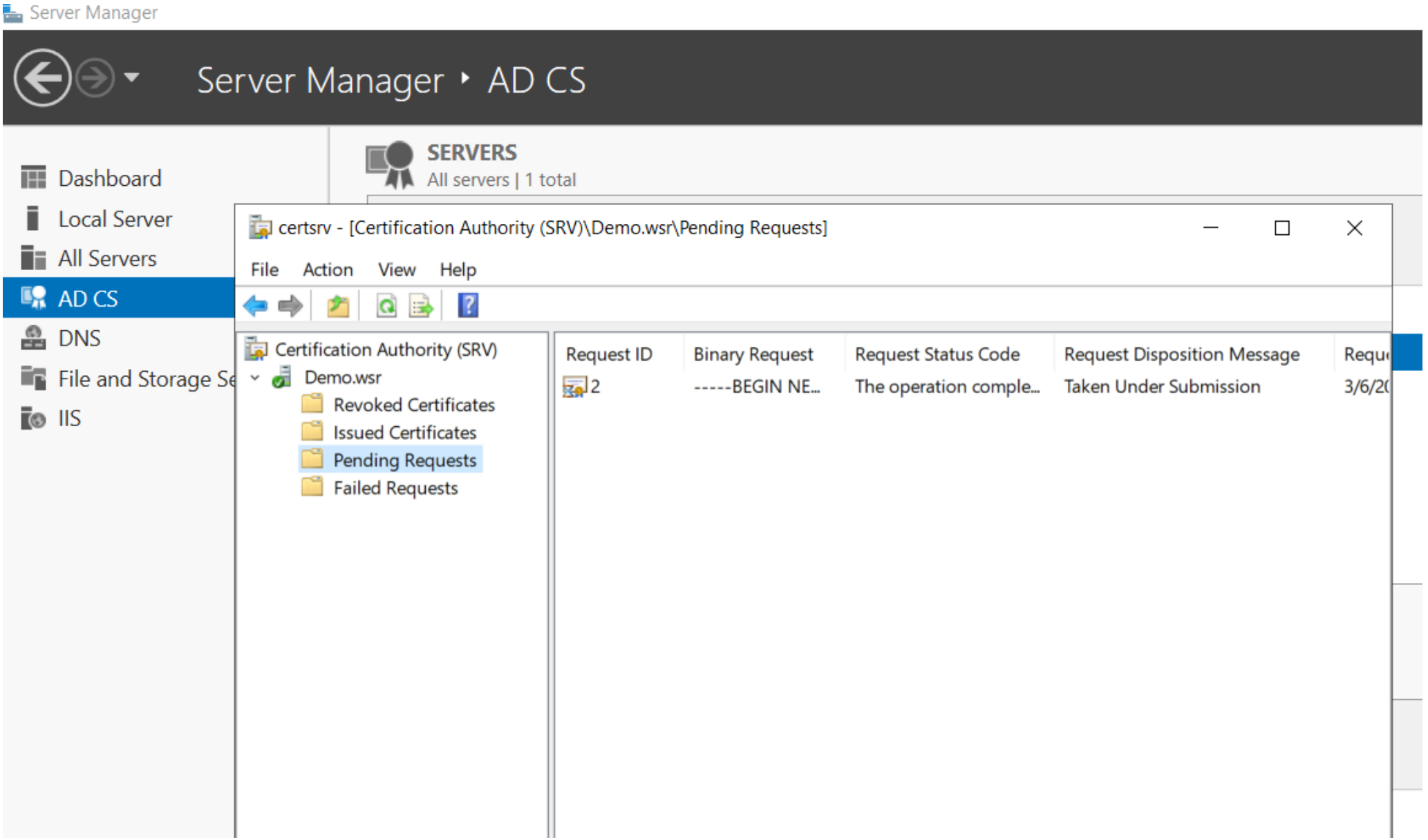
Additional Options:

Request Format: ( ) CMC (•) PKCS10

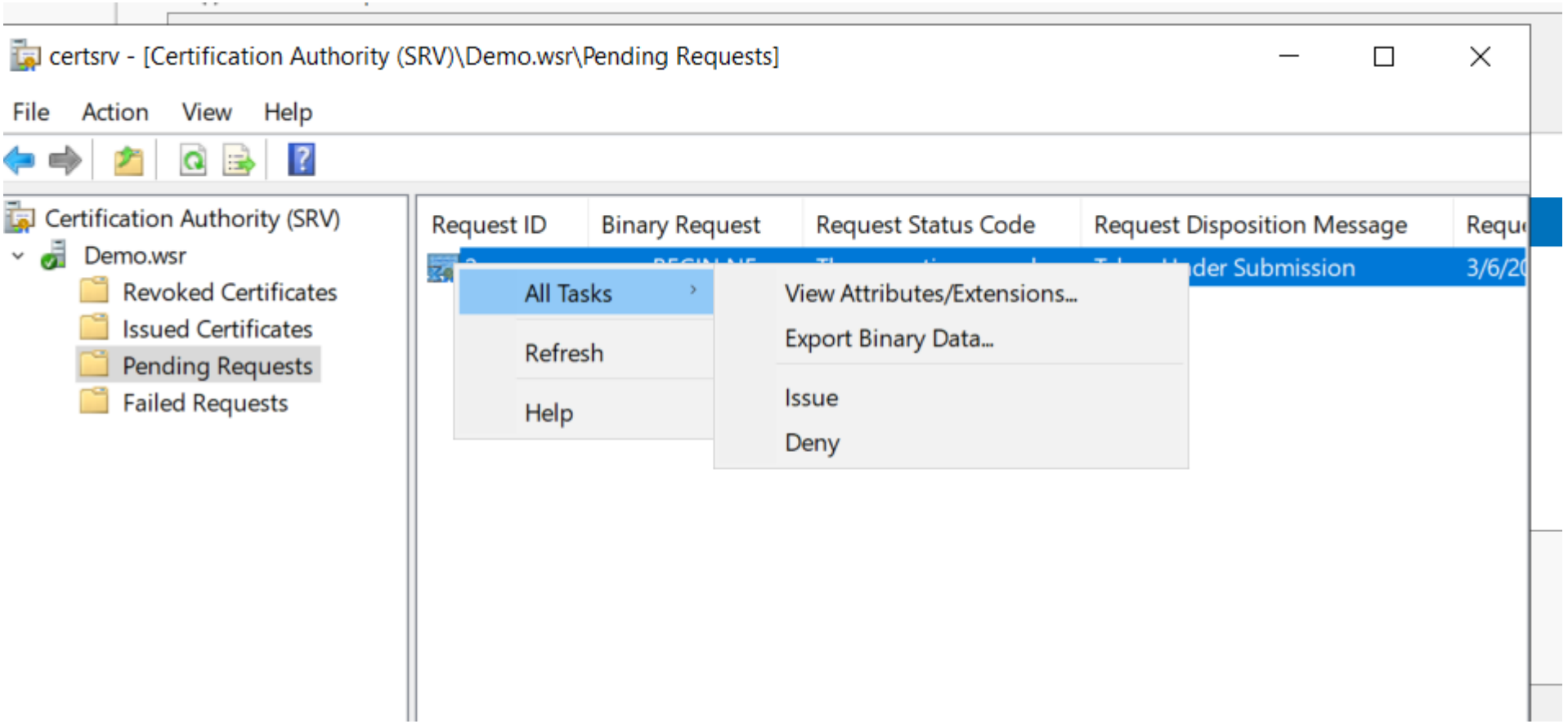

https://localhost/certsrv/certrqma.asp
Certific
Waiting for localhost
Type of Certificate Needed:
Server Authentication Certificate
Key Options:
Create new key set
Use existing key set
CSP:
Microsoft RSA SChannel Cryptographic Provider
Waiting for server response...
Key Usage:
Exchange
Key Size:
2048
Min: 384
Max:16384
(common key sizes: 512 1024 2048 4096 8192 16384)
Automatic key container name
User specified key container name
Mark keys as exportable
Enable strong private key protection
Additional Options:
Request Format:
CMC
PKCS10
Hash Algorithm:
sha1
Only used to sign request.
Save request
Attributes:
Friendly Name:
Submit >



В Server Manager выбрать AD CS => нажать правой клавишей на SRV и выбрать “Certification Authority”



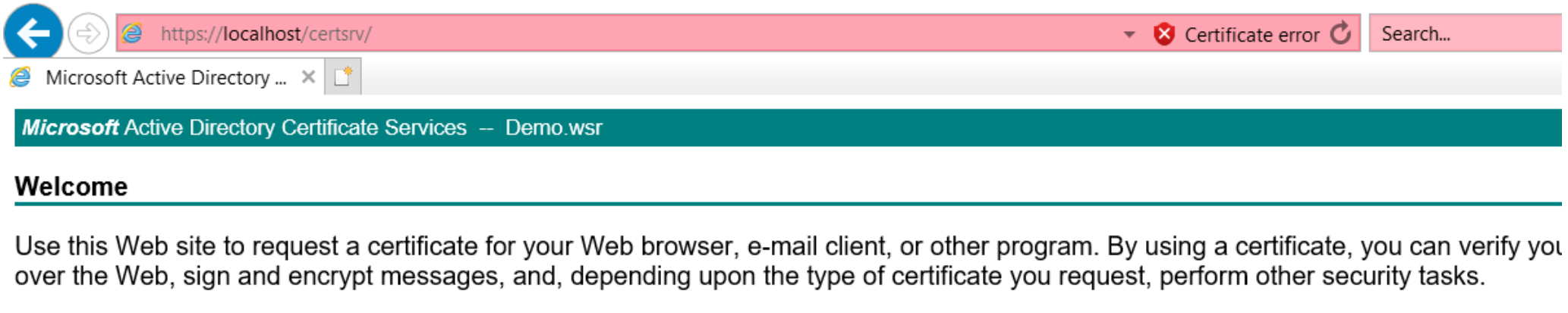
Нажать на “Pending Requests” далее правой клавишей на сертификате и выбрать All Tasks => Issue



Открыть Internet Explorer

Перейти по адресу:

https://localhost/certsrv



Выбрать “View the status of a pending certificate request”

Microsoft Active Directory Certificate Services -- Demo.wsr

View the Status of a Pending Certificate Request

Select the certificate request you want to view:

Server Authentication Certificate (Tuesday March 8 2022 5:22:13 PM)

Выбрать сертификат

Microsoft Active Directory Certificate Services -- Demo.wsr

Certificate Issued

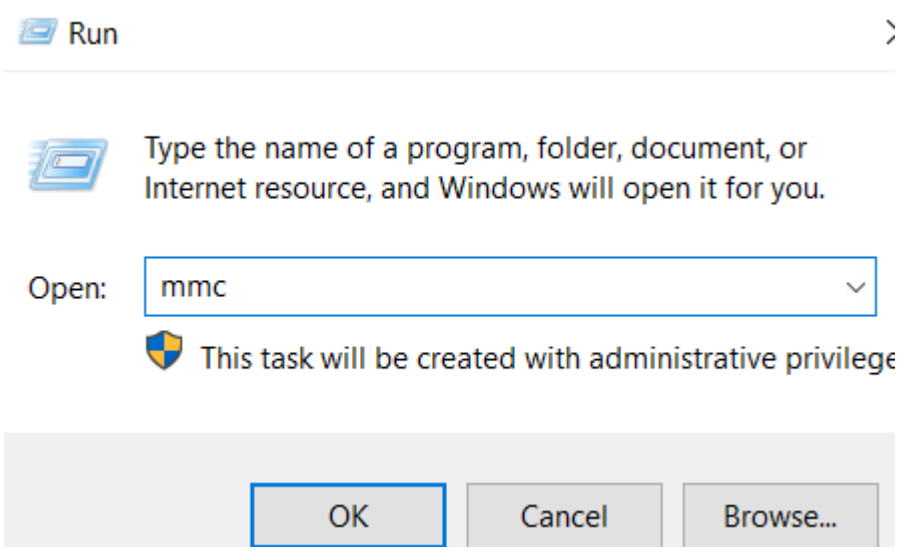
The certificate you requested was issued to you.

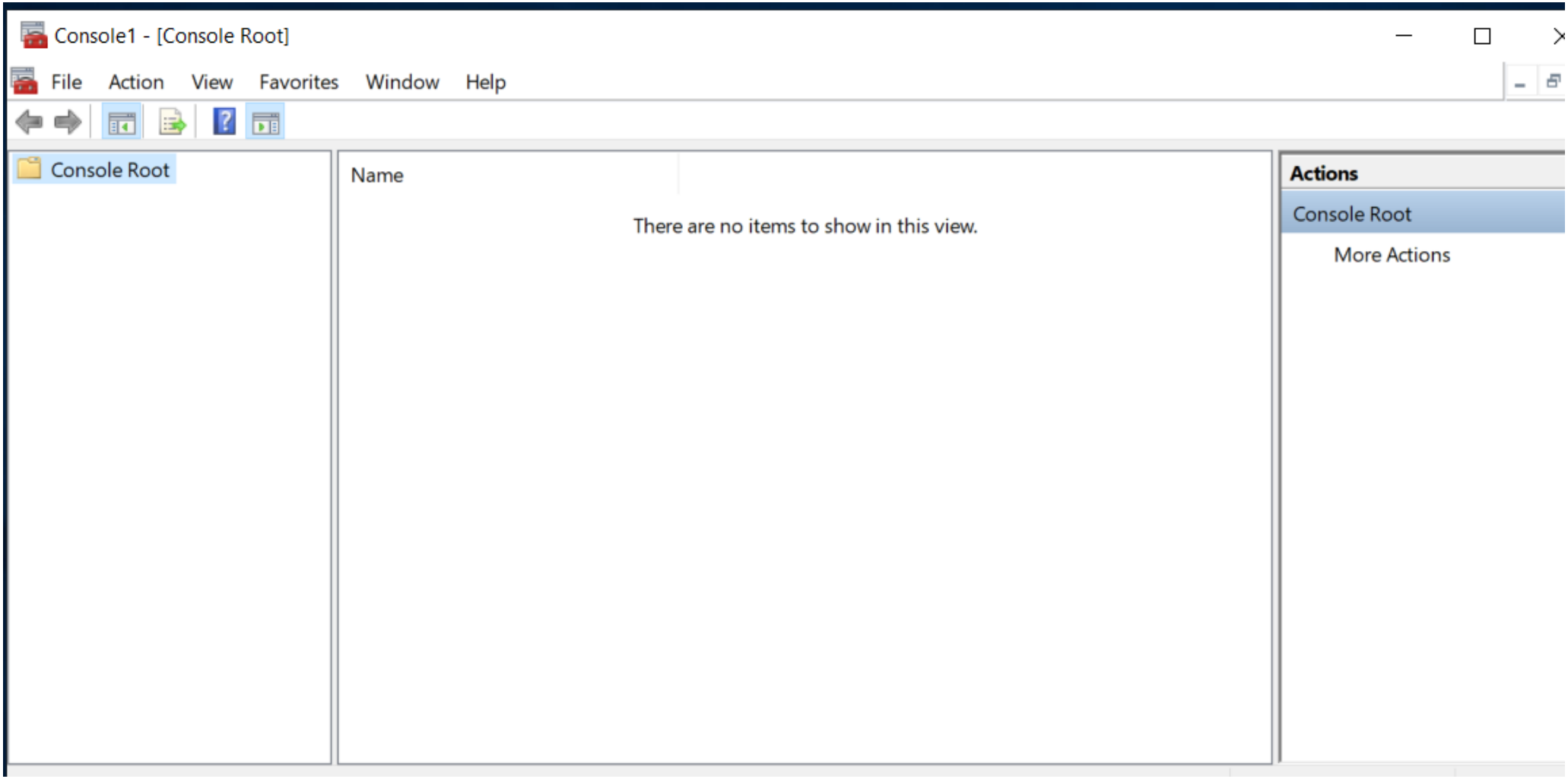
Install this certificate

☐ Save response

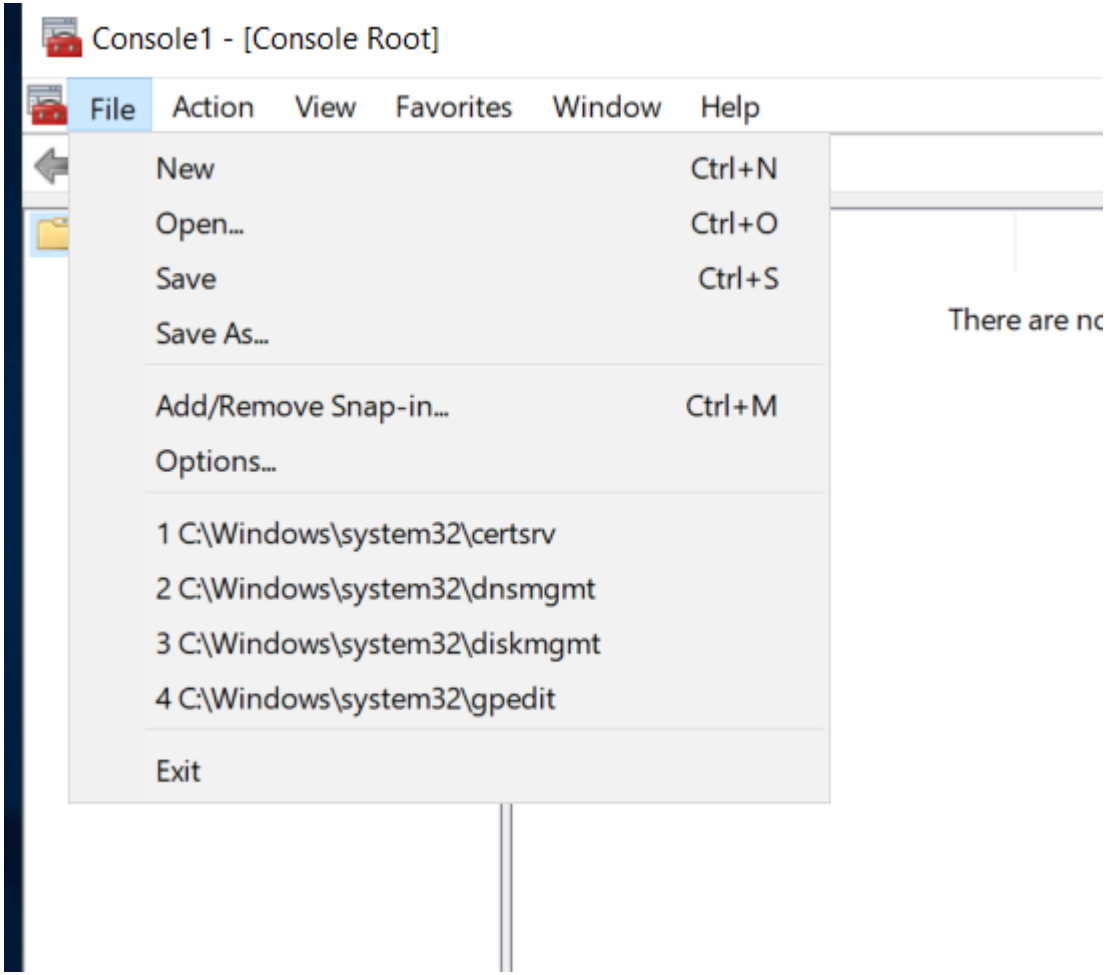
Кнопка пуск => Windows System =>Run

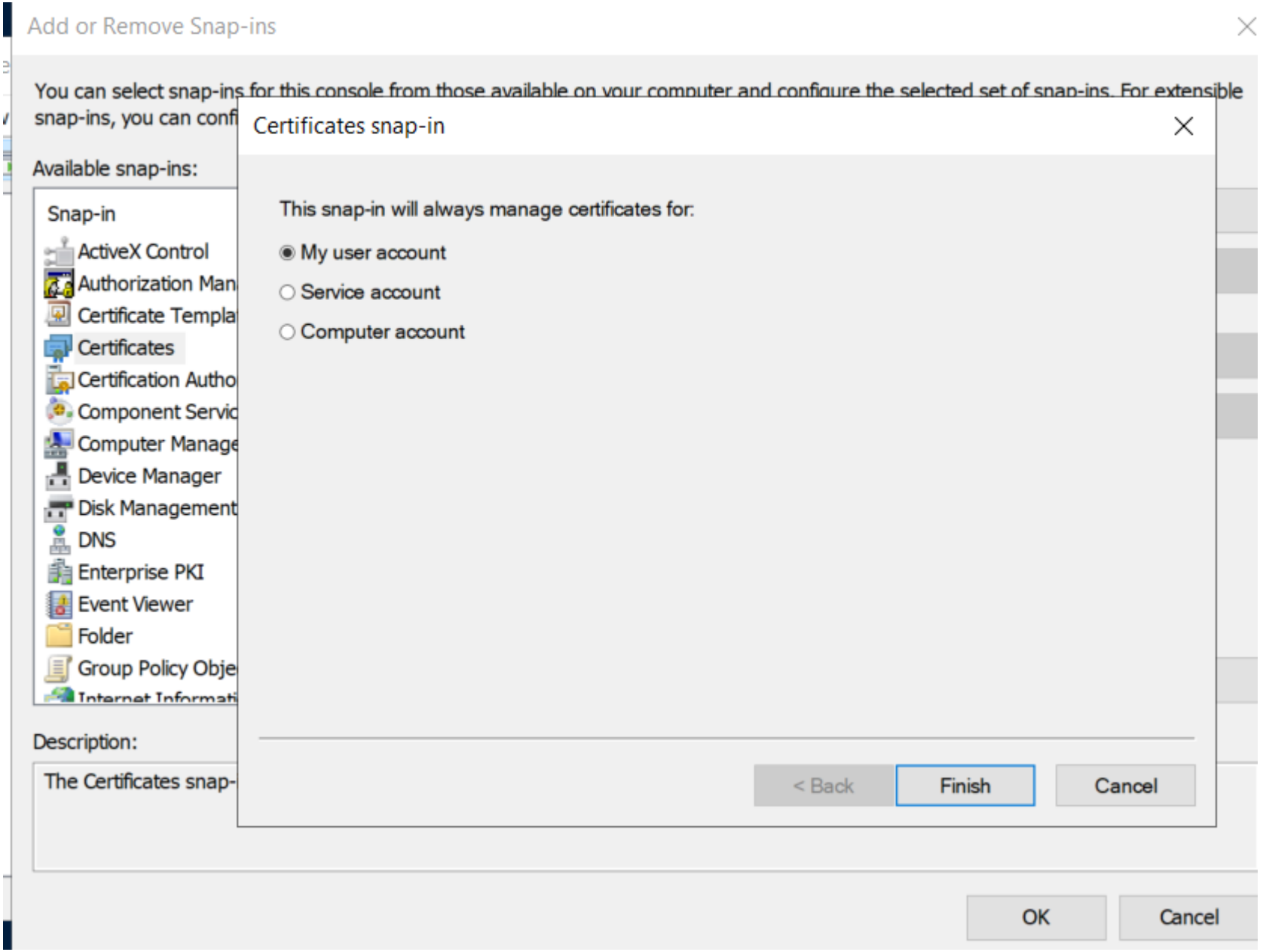
Ввести: mmc

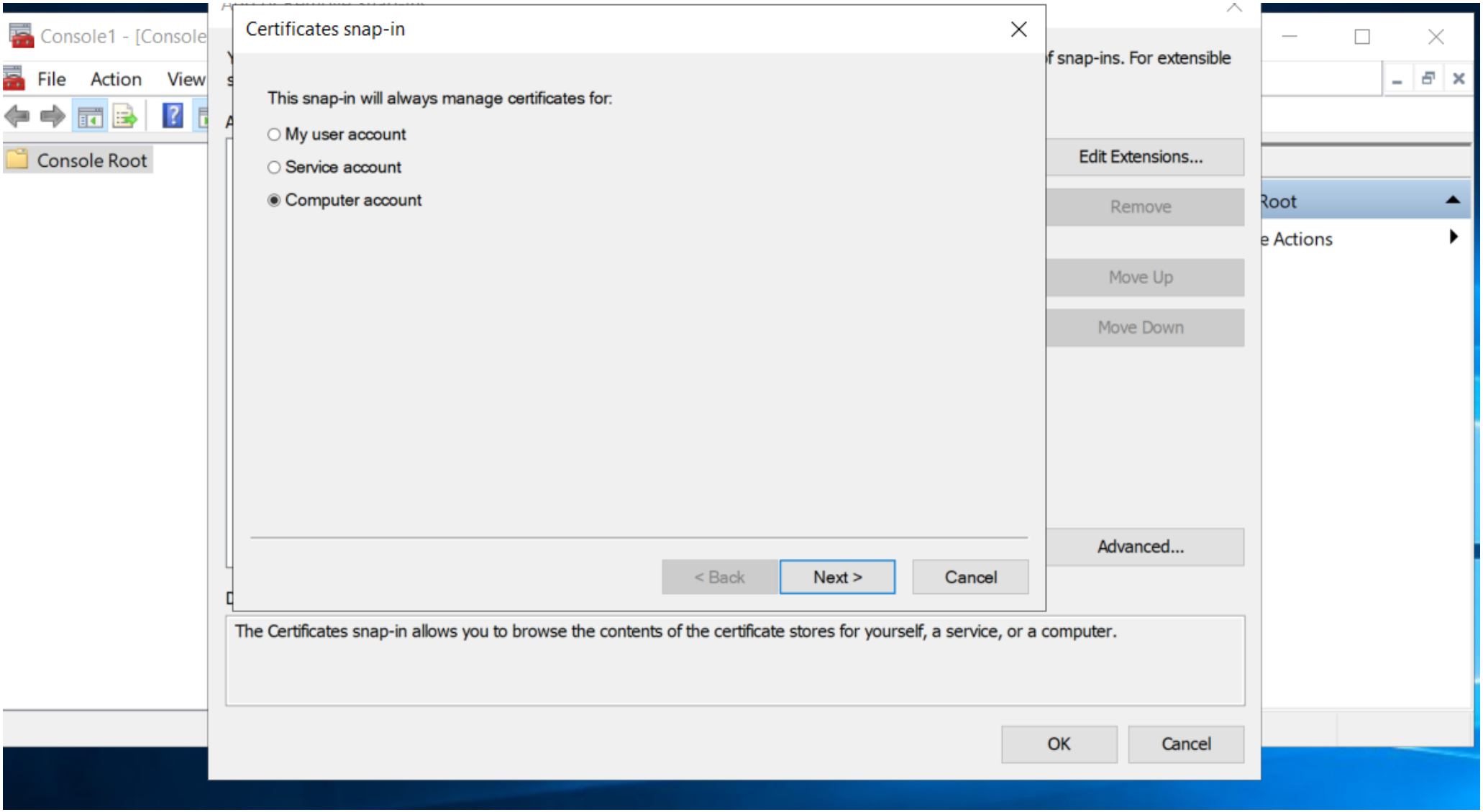


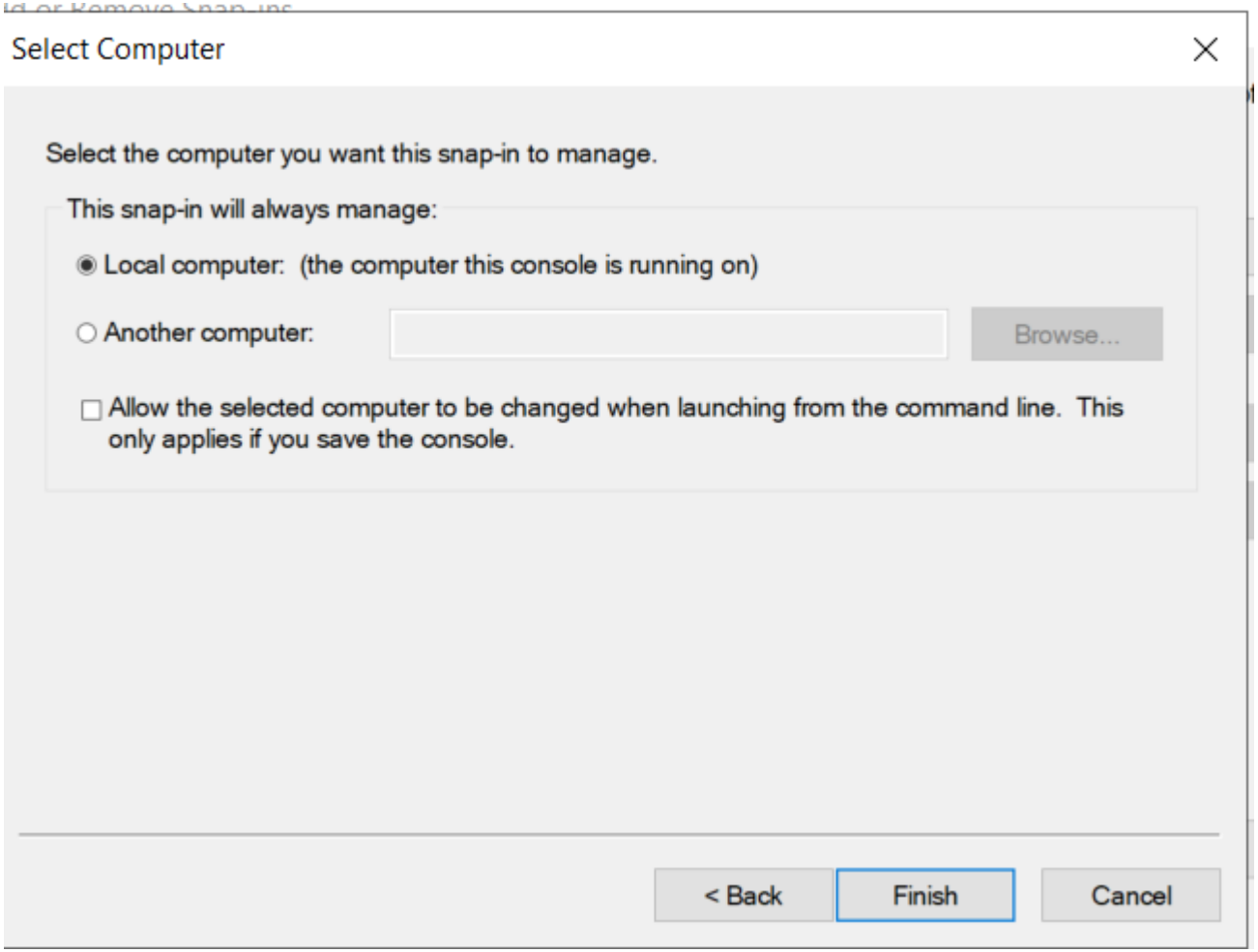


Выбрать Fail => Add/Remove Snap-in и добавть управление сертификатами для пользователя и ущё раз для компьютера

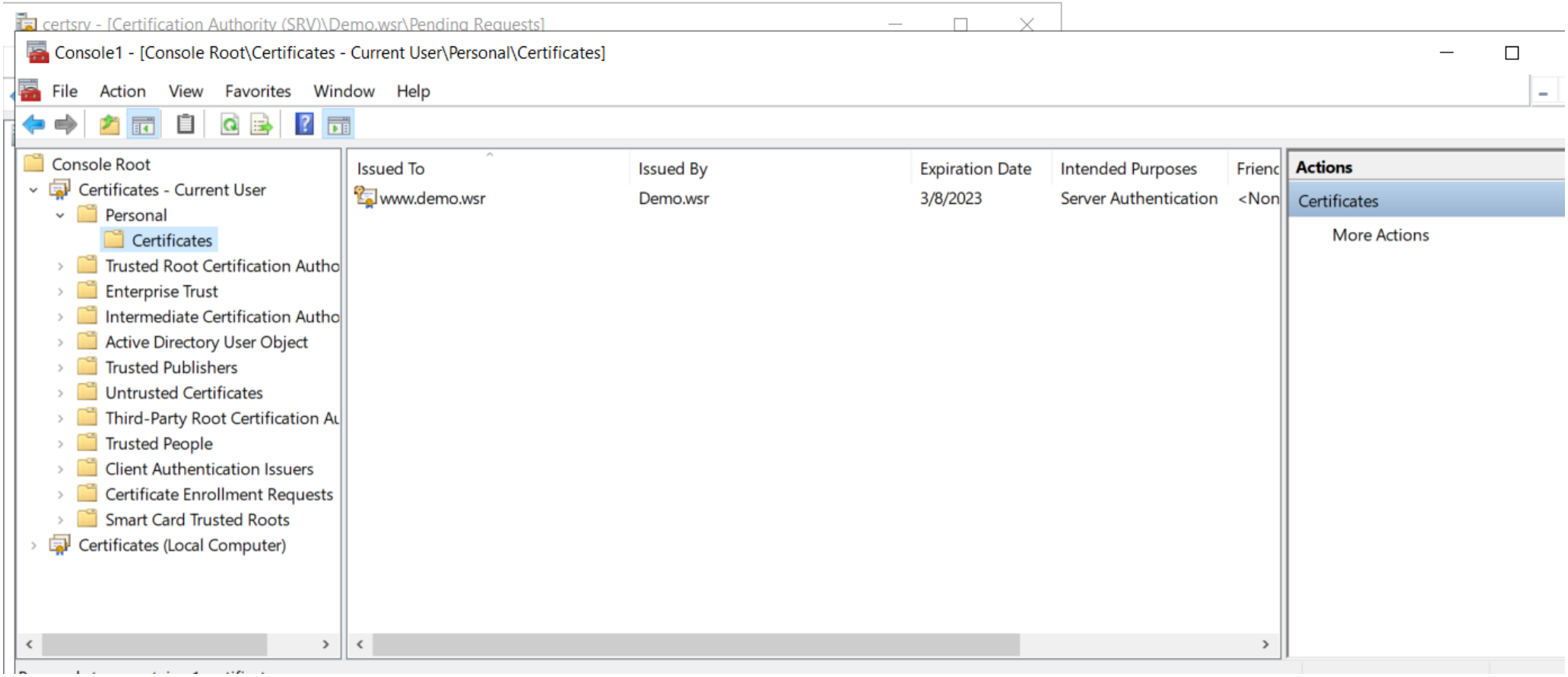

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\certsrv
2 C:\Windows\system32\dnsmgmt
3 C:\Windows\system32\diskmgmt
4 C:\Windows\system32\gpedit
Exit
There are nc

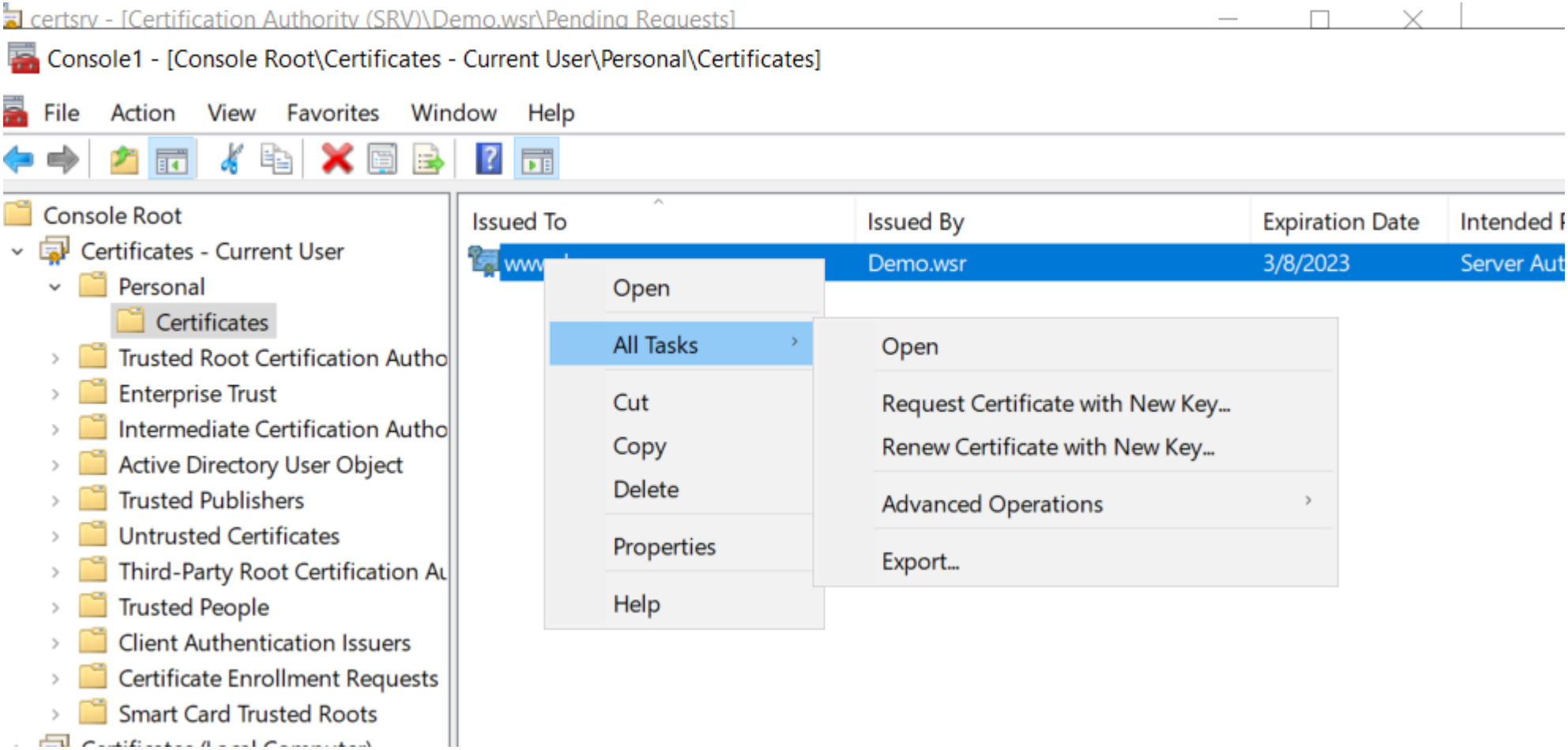

Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can confi
Available snap-ins:
Snap-in
ActiveX Control
Authorization Man
Certificate Templa
Certificates
Certification Autho
Component Servic
Computer Manage
Device Manager
Disk Management
DNS
Enterprise PKI
Event Viewer
Folder
Group Policy Obje
Description:
The Certificates snap-
OK
Cancel
Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Finish
Cancel


Console1 - [Console
File Action View
Console Root
Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel
f snap-ins. For extensible
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel
Root
e Actions

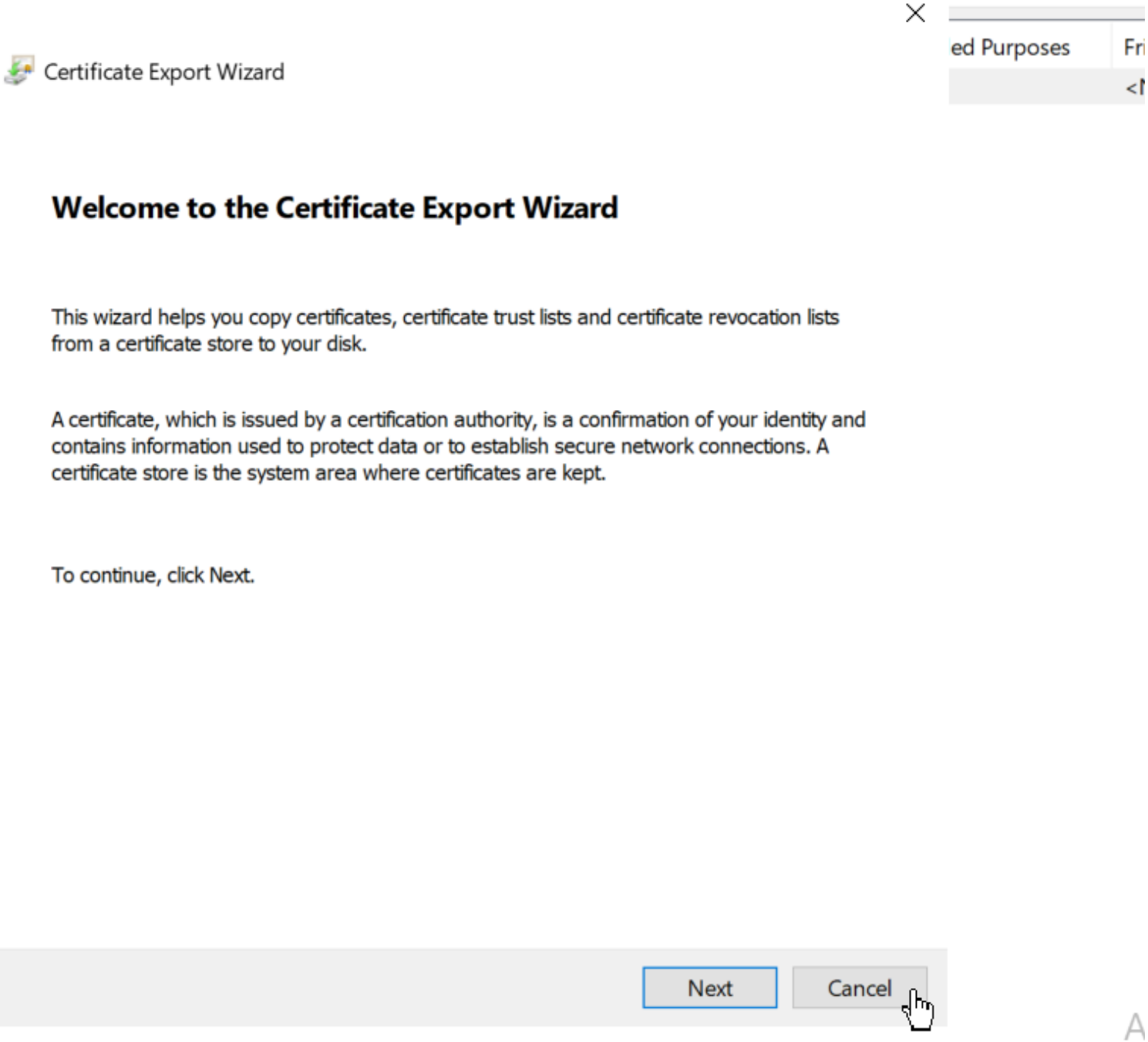


Открыть папку с сертификатами и выбрать наш сертификат

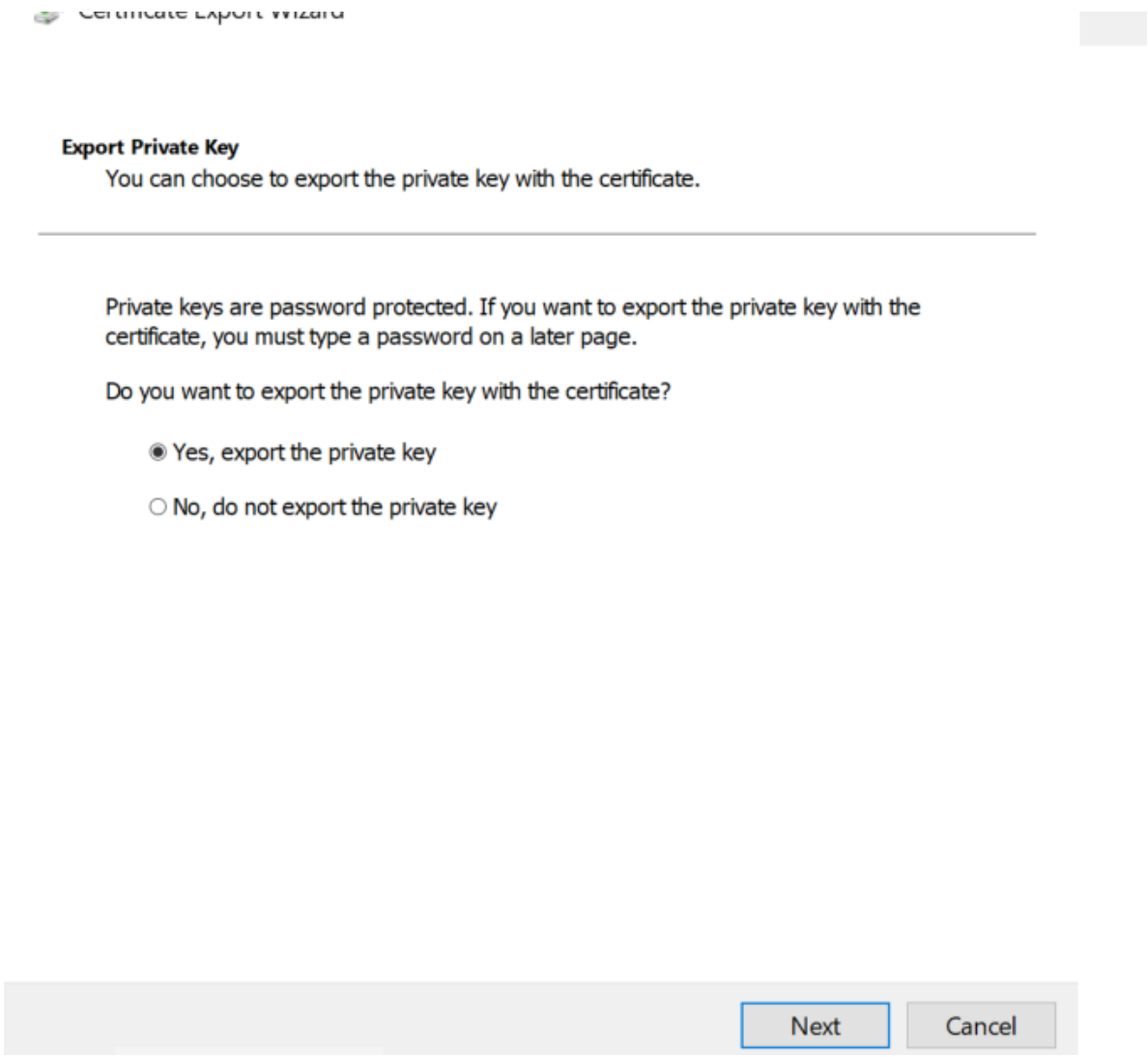

certsrv - [Certification Authority (SRV)\Demo.wsr\Pending Requests]
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Certificates (Local Computer)
Issued To
Issued By
Expiration Date
Intended Purposes
Frienc
www.demo.wsr
Demo.wsr
3/8/2023
Server Authentication
<Non
Actions
Certificates
More Actions

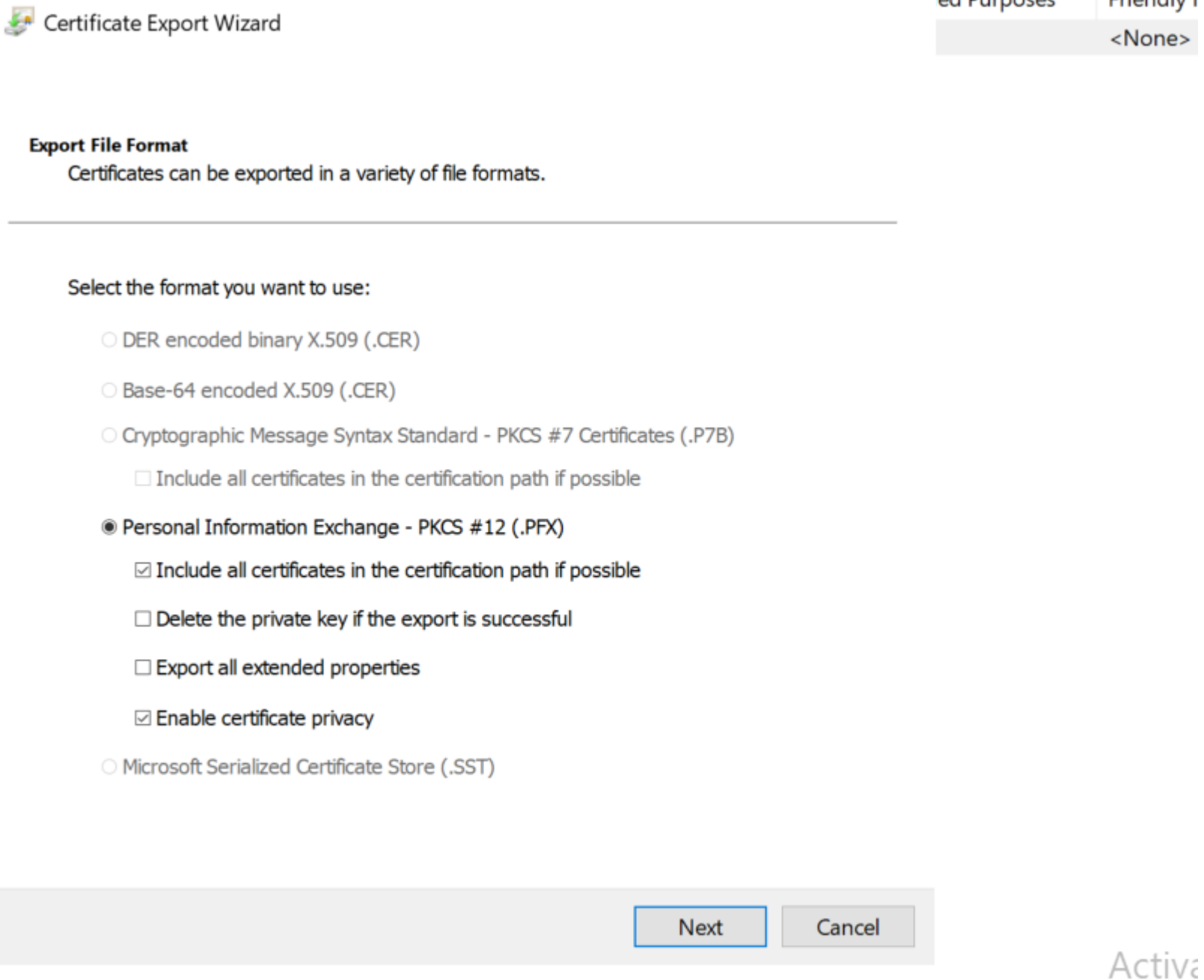


Выбрать export

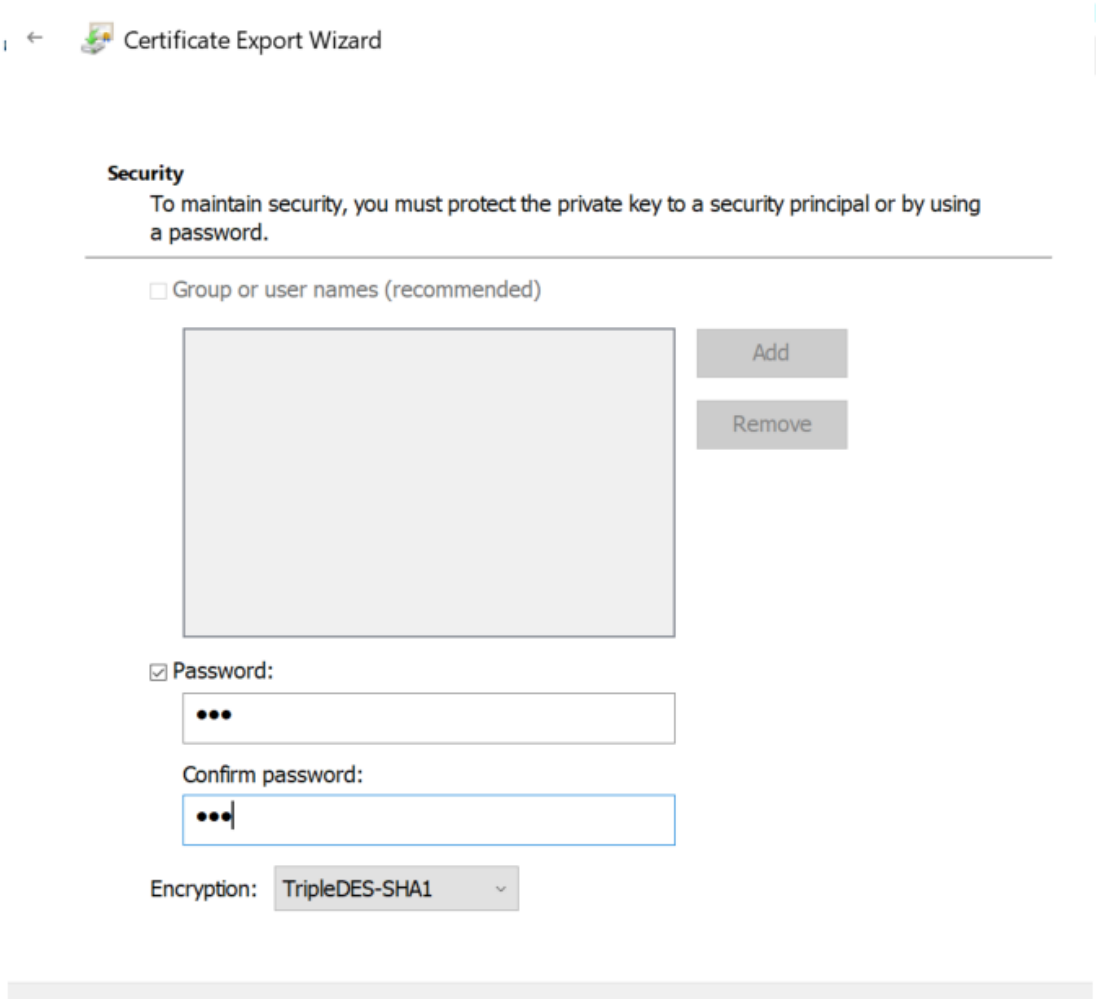

Certificate Export Wizard
ed Purposes
Fri
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel

Переключить на Yes

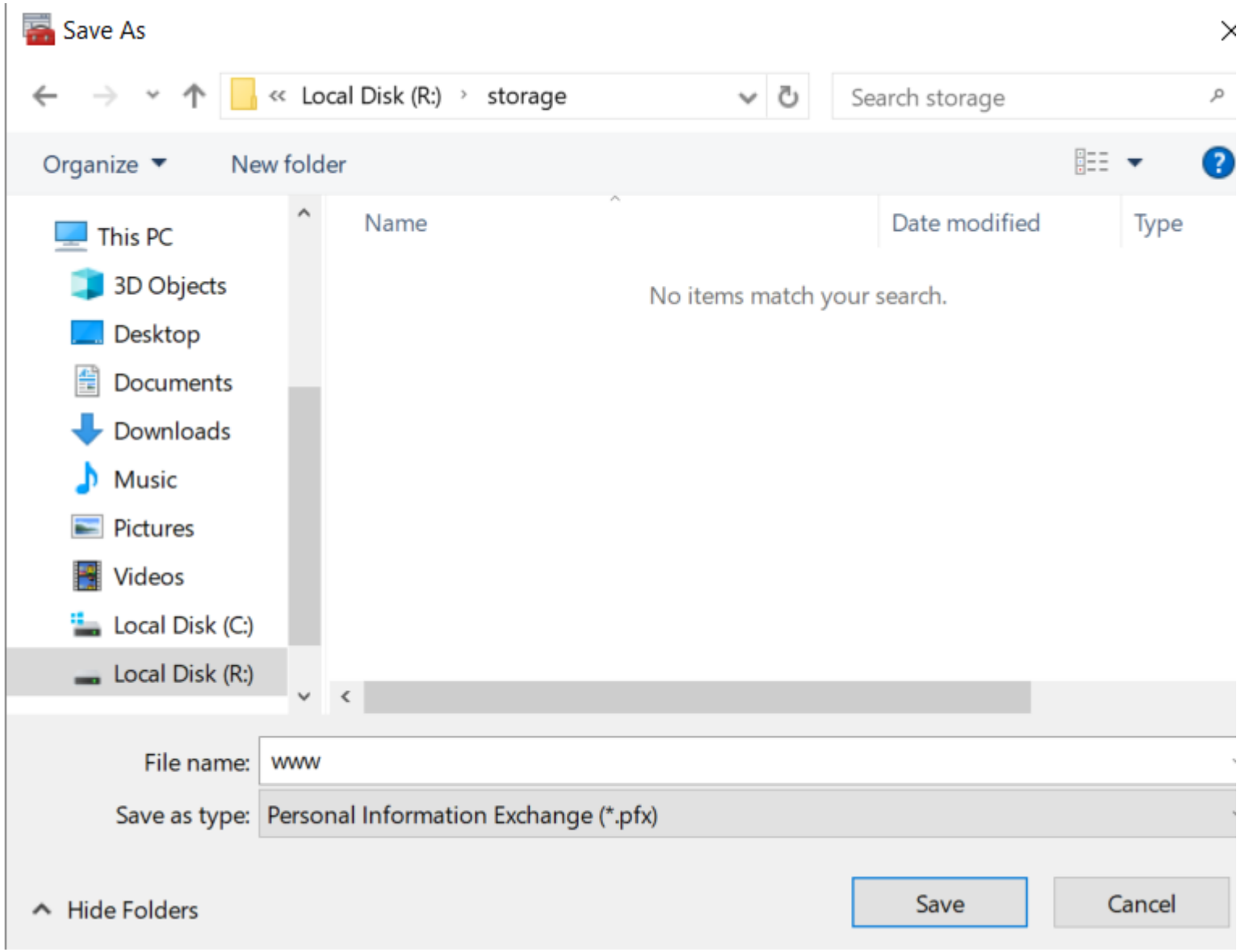



ed Purposes
Friendly
<None>
Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel
Activa

Установить пароль = 123



Выбрать нашу общую папку и сохранить туда сертификат



Certificate Export Wizard

ed Purpo

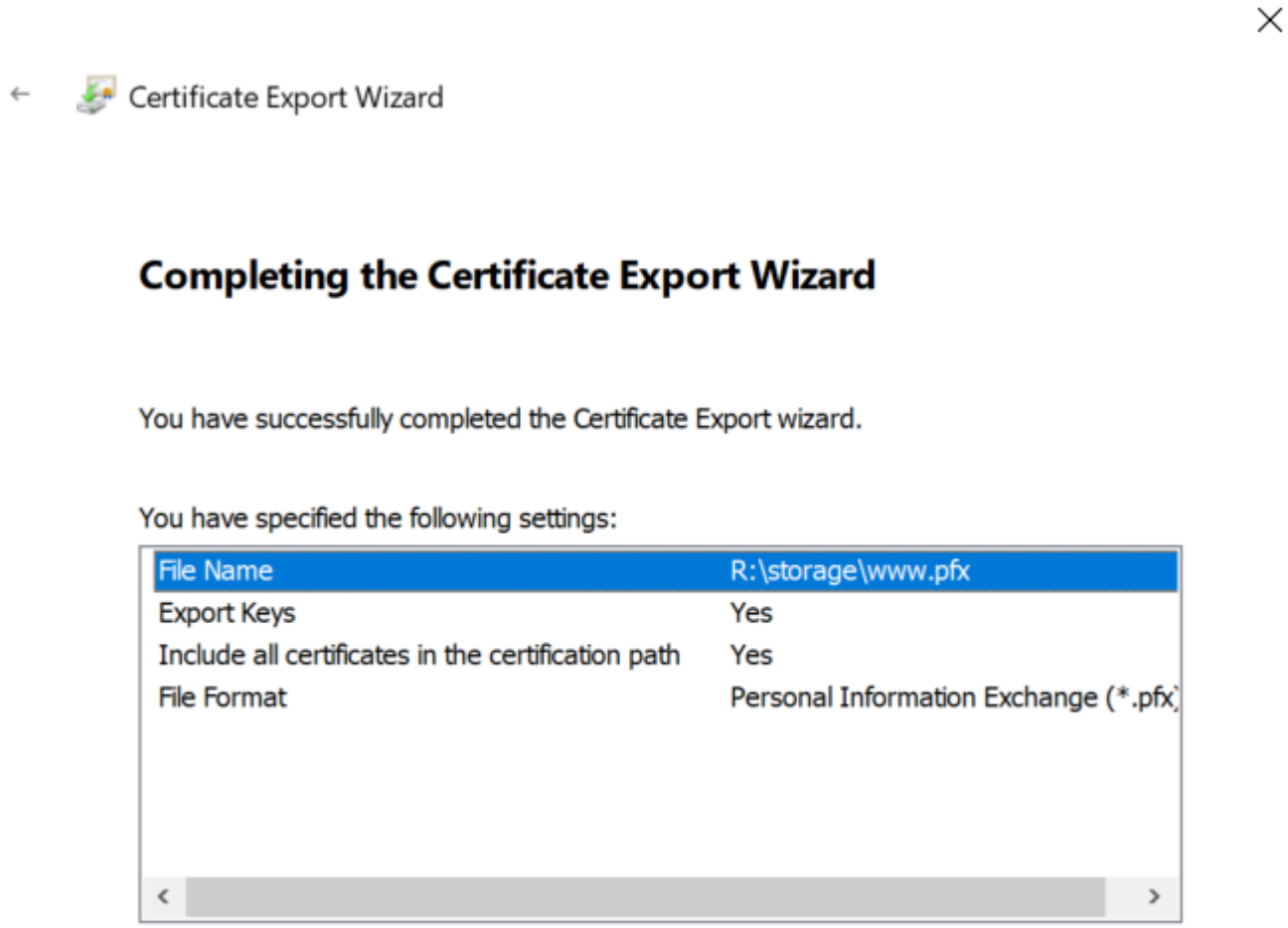
File to Export

Specify the name of the file you want to export

File name:

R:\storage\www.pfx

Browse...


Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name
R:\storage\www.pfx
Export Keys
Yes
Include all certificates in the certification path
Yes
File Format
Personal Information Exchange (*.pfx)

Выдача сертификата через PowerShell

```
Install-WindowsFeature -Name AD-Certificate, ADCS-Web-Enrollment -IncludeManagementTools

Install-AdcsCertificationAuthority -CAType StandaloneRootCa -CACommonName "Demo.wsr" -force

Install-AdcsWebEnrollment -Confirm -force

New-SelfSignedCertificate -subject "localhost"

Get-ChildItem cert:\LocalMachine\My

Move-item Cert:\LocalMachine\My\XFX2DX02779XFD1F6F4X8435A5X26ED2X8DEFX95 -destination
Cert:\LocalMachine\Webhosting\

New-IISSiteBinding -Name 'Default Web Site' -BindingInformation "*:443:" -Protocol htts -CertificateThumbPrint
XFX2DX02779XFD1F6F4X8435A5X26ED2X8DEFX95

Start-WebSite -Name "Default Web Site"

Get-CACrlDistributionPoint | Remove-CACrlDistributionPoint -force

Get-CAAuthorityInformationAccess |Remove-CAAuthorityInformationAccess -force

Get-CAAuthorityInformationAccess |Remove-CAAuthorityInformationAccess -force

Restart-Service CertSrv
```

Инфраструктура веб-приложения.

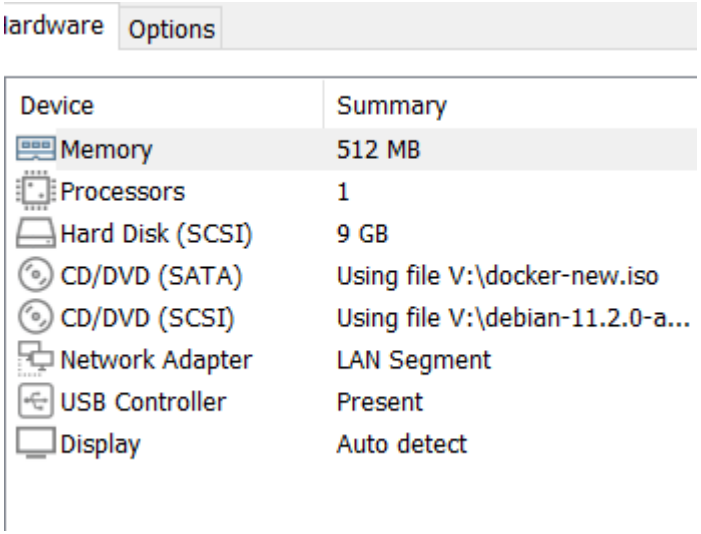
Данный блок подразумевает установку и настройку доступа к веб-приложению, выполненному в формате контейнера Docker

1. Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов;
    - Выполните установку приложения AppDocker0;
2. Пакеты для установки Docker расположены на дополнительном ISO-образе;
3. Инструкция по работе с приложением расположена на дополнительном ISO-образе;
4. Необходимо реализовать следующую инфраструктуру приложения.
    - Клиентом приложения является CLI (браузер Edge);
    - Хостинг приложения осуществляется на ВМ WEB-L и WEB-R;
    - Доступ к приложению осуществляется по DNS-имени www.demo.wsr;
        - Имя должно разрешаться во “внешние” адреса ВМ управления трафиком в обоих регионах;
        - При необходимости, для доступа к к приложению допускается реализовать реверс-прокси или трансляцию портов;
    - Доступ к приложению должен быть защищен с применением технологии TLS;
        - Необходимо обеспечить корректное доверие сертификату сайта, без применения “исключений” и подобных механизмов;
    - Незащищенное соединение должно переводится на защищенный канал автоматически;
5. Необходимо обеспечить отказоустойчивость приложения;
    - Сайт должен продолжать обслуживание (с задержкой не более 25 секунд) в следующих сценариях:
        - Отказ одной из ВМ Web
        - Отказ одной из ВМ управления трафиком.

WEB-L Doc

1. Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов;

Установить в виртуальную машину ещё один дисковод и загрузить в него docker.iso/ в первом у вас должен быть диск от Debian-BD-1



2. Пакеты для установки Docker расположены на дополнительном ISO-образе;

apt-cdrom add

apt install -y docker-ce

systemctl start docker
systemctl enable docker

mkdir /mnt/app

mount /dev/sr1 /mnt/app

```
root@WEB-L:/opt/share# mount /dev/sr1 /mnt/app
mount: /mnt/app: WARNING: source write-protected, mounted read-only.
root@WEB-L:/opt/share#
```

docker load < /mnt/app/app.tar

```
root@WEB-L:/mnt/app# docker load < /mnt/app/app.tar
2edcec3590a4: Loading layer  83.86MB/83.86MB
e379e8aedd4d: Loading layer    62MB/62MB
b8d6e692a25e: Loading layer  3.072kB/3.072kB
f1db227348d0: Loading layer  4.096kB/4.096kB
32ce5f6a5106: Loading layer  3.584kB/3.584kB
d874fd2bc83b: Loading layer  7.168kB/7.168kB
7aea6ab0ef13: Loading layer  4.096kB/4.096kB
Loaded image: app:latest
root@WEB-L:/mnt/app# _
```

docker images

```
root@WEB-L:/mnt/app# docker images
REPOSITORY   TAG         IMAGE ID       CREATED        SIZE
app          latest      85287aa0d79b   6 weeks ago    141MB
root@WEB-L:/mnt/app#
```

docker run --name app -p 8080:80 -d app

```
root@WEB-L:/mnt/app# docker run --name app -p 8080:80 -d app
3ae312fb5eb16d74055eb1de3c58e3614c66bc4036d6eb97822479ad36cc0ff0
root@WEB-L:/mnt/app#
```

docker ps

```
root@WEB-L:/mnt/app# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS
                    NAMES
3ae312fb5eb1   app       "/docker-entrypoint.…"   27 seconds ago   Up 25 seconds   0.0.0.0:8080->80/
tcp, :::8080->80/tcp   app
root@WEB-L:/mnt/app#
```

Если вы перезапустили виртуальную машину и docker не запустился то для перезапуска docker restart app

WEB-R

apt-cdrom add

```
root@WEB-R:/opt/share# apt-cdrom add
Using CD-ROM mount point /media/cdrom/
Identifying... [b0c1d2ffecd15e8a41d621f3e850b9db-2]
Scanning disc for index files...
Found 2 package indexes, 0 source indexes, 2 translation indexes and 0 signatures
This disc is called:
'Debian GNU/Linux 11.2.0 _Bullseye_ - Official amd64 BD Binary-1 20211218-11:13'
Reading Package Indexes... Done
Reading Translation Indexes... Done
Writing new source list
Source list entries for this disc are:
deb cdrom:[Debian GNU/Linux 11.2.0 _Bullseye_ - Official amd64 BD Binary-1 20211218-11:13]/ bullseye
 contrib main
Using CD-ROM mount point /media/cdrom/
Identifying... [cbfe69941a070ffcd49a671b9d29ce7d-2]
Scanning disc for index files...
Found 1 package indexes, 0 source indexes, 0 translation indexes and 0 signatures
This disc is called:
'Debian GNU/Linux 11.2.0 _Bullseye_ - Docker packages for WSR'
Reading Package Indexes... Done
Writing new source list
Source list entries for this disc are:
deb cdrom:[Debian GNU/Linux 11.2.0 _Bullseye_ - Docker packages for WSR]/ bullseye main
Repeat this process for the rest of the CDs in your set.
root@WEB-R:/opt/share#
```

apt install -y docker-ce

systemctl start docker
systemctl enable docker

```
root@WEB-R:/opt/share# systemctl enable docker
Synchronizing state of docker.service with SysV service script with /lib/systemd/systemd-sysv-instal
l.
Executing: /lib/systemd/systemd-sysv-install enable docker
root@WEB-R:/opt/share#
```

mkdir /mnt/app

mount /dev/sr1 /mnt/app

```
root@WEB-R:/opt/share# mount /dev/sr1 /mnt/app
mount: /mnt/app: WARNING: source write-protected, mounted read-only.
root@WEB-R:/opt/share# _
```

docker load < /mnt/app/app.tar

```
root@WEB-R:/opt/share# docker load < /mnt/app/app.tar
2edcec3590a4: Loading layer  83.86MB/83.86MB
e379e8aedd4d: Loading layer    62MB/62MB
b8d6e692a25e: Loading layer  3.072kB/3.072kB
f1db227348d0: Loading layer  4.096kB/4.096kB
32ce5f6a5106: Loading layer  3.584kB/3.584kB
d874fd2bc83b: Loading layer  7.168kB/7.168kB
7aea6ab0ef13: Loading layer  4.096kB/4.096kB
Loaded image: app:latest
root@WEB-R:/opt/share# _
```

docker images

```
root@WEB-R:/opt/share# docker images
REPOSITORY   TAG       IMAGE ID       CREATED        SIZE
app          latest    85287aa0d79b   6 weeks ago    141MB
root@WEB-R:/opt/share#
```

docker run --name app -p 8080:80 -d app

```
root@WEB-R:/opt/share# docker run --name app -p 8080:80 -d app
c849aff5740f17a2d6e599a79693be0320479cf498498c102423051f485b2be0
root@WEB-R:/opt/share# _
```

docker ps

```
root@WEB-R:/opt/share# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS
                    NAMES
c849aff5740f   app       "/docker-entrypoint.…"   24 seconds ago   Up 23 seconds   0.0.0.0:8080->80/
tcp, :::8080->80/tcp   app
root@WEB-R:/opt/share# _
```

RTR-L

en
conf t
no ip http secure-server
do wr
end
reload

```
Continue to reload? (yes/[no]): yes
Proceed with reload? [confirm]
```

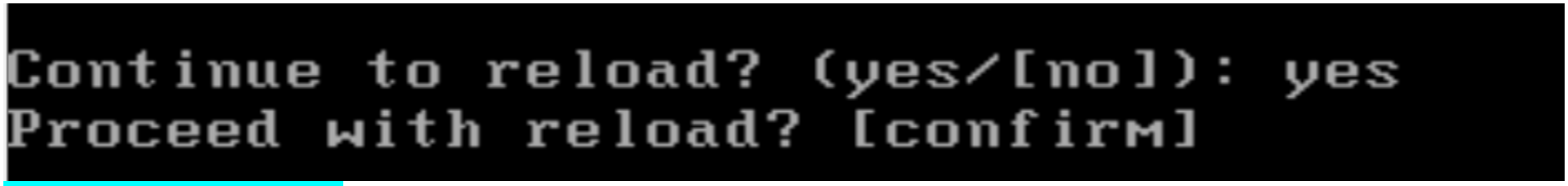
(ввести yes) Нажать Enter
Снова нажать Enter
ОН долго думает, и перезагрузка идёт долго

ip nat inside source static tcp 192.168.100.100 80 4.4.4.100 80
ip nat inside source static tcp 192.168.100.100 443 4.4.4.100 443

do wr

RTR-R

en
conf t
no ip http secure-server
do wr
end
reload



(ввести yes) Нажать Enter
Снова нажать Enter
ОН долго думает, и перезагрузка идёт долго

ip nat inside source static tcp 172.16.100.100 80 5.5.5.100 80
ip nat inside source static tcp 172.16.100.100 443 5.5.5.100 443

do wr

5. Необходимо обеспечить отказоустойчивость приложения;

WEB-L ssl

Установить nginx

apt install -y nginx

Перейти в перемонтированную папку

cd /opt/share

Преобразовать сертификат
Запросит пароль, который мы ставили при выпуске (123)

openssl pkcs12 -nodes -nocerts -in www.pfx -out www.key
openssl pkcs12 -nodes -nokeys -in www.pfx -out www.cer

Скопировать в нужную папку

cp /opt/share/www.key /etc/nginx/www.key
cp /opt/share/www.cer /etc/nginx/www.cer

Открыть файл и изменить пути до ключа
nano /etc/nginx/snippets/snakeoil.conf

Открыть файл

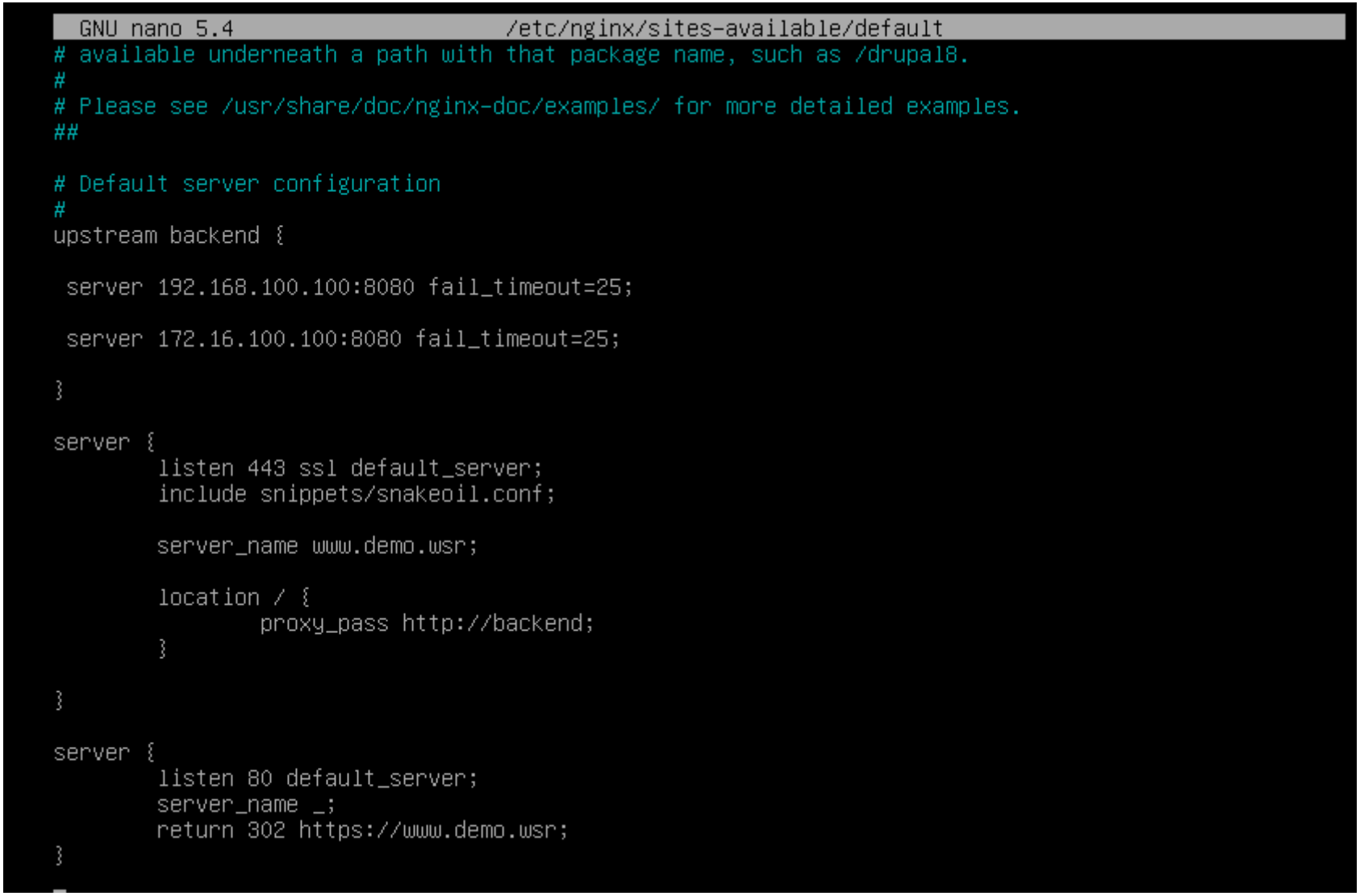
nano /etc/nginx/sites-available/default

Всё что есть в файле закомментировать, добавить следующие строчки

```
upstream backend {
 server 192.168.100.100:8080 fail_timeout=25;
 server 172.16.100.100:8080 fail_timeout=25;
}

server {
    listen 443 ssl default_server;
    include snippers/snakeoil.conf;

    server_name www.demo.wsr;

 location / {
  proxy_pass http://backend ;
 }
}

server {
```

listen 80 default_server;
server_name _;
return 301 https://www.demo.wsr;

}



Перезапустить

systemctl reload nginx

Зайти на SRV и убрать созданный (с помощью WEB-l) сертификат и ключ, оставить только тот который был создан в SRV

WEB-R ssl

Аналогично WEB-L

apt install -y nginx

cd /opt/share

openssl pkcs12 -nodes -nocerts -in www.pfx -out www.key
openssl pkcs12 -nodes -nokeys -in www.pfx -out www.cer

cp /opt/share/www.key /etc/nginx/www.key
cp /opt/share/www.cer /etc/nginx/www.cer

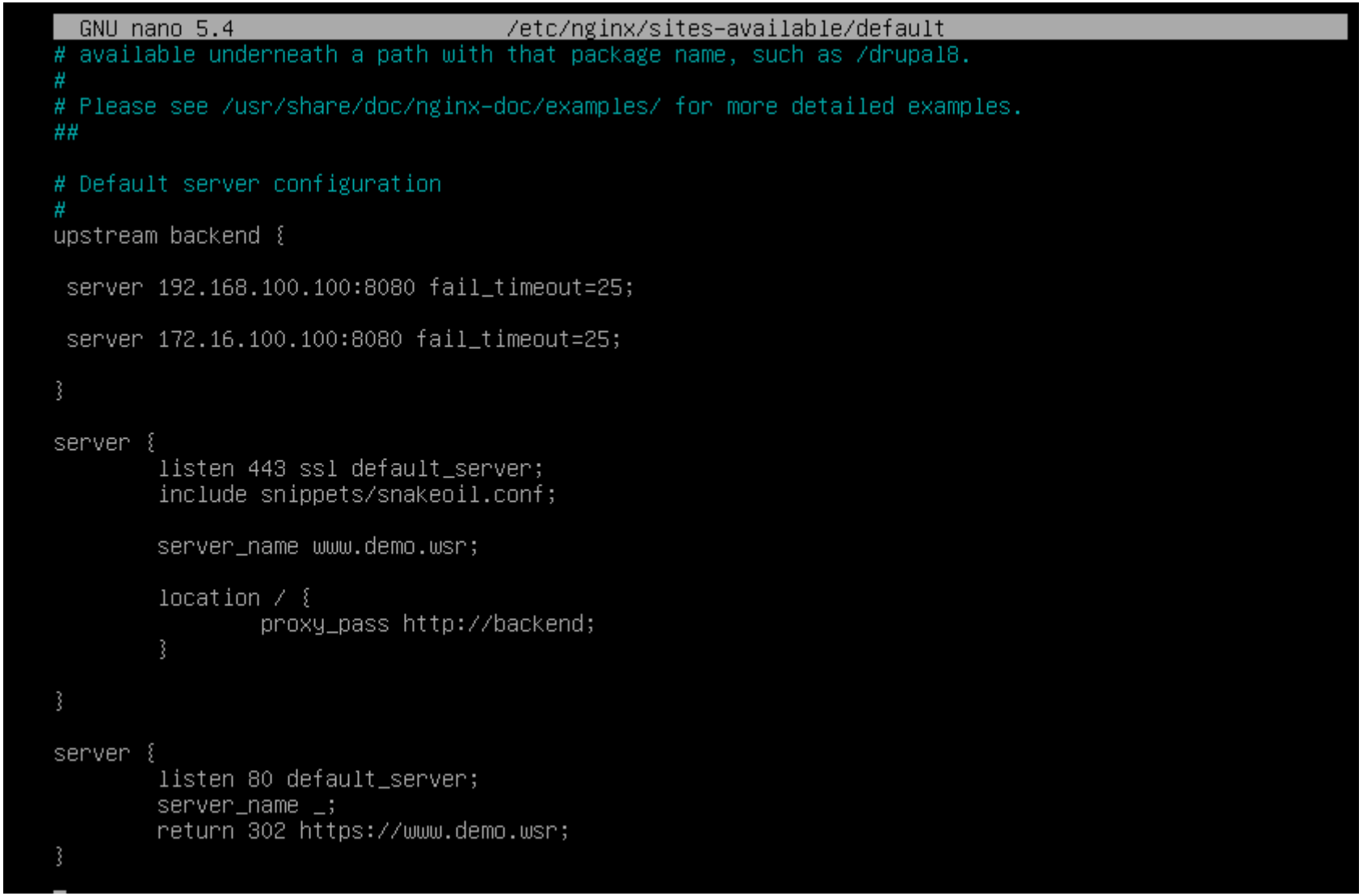
nano /etc/nginx/snippets/snakeoil.conf

Открываем файл

nano /etc/nginx/sites-available/default

Всё что есть в файле закомментировать, добавить следующие строчки

```
upstream backend {
 server 192.168.100.100:8080 fail_timeout=25;
 server 172.16.100.100:8080 fail_timeout=25;
}

server {
    listen 443 ssl default_server;
    include snippers/snakeoil.conf;

    server_name www.demo.wsr;

 location / {
  proxy_pass http://backend ;
 }
}

server {
   listen 80  default_server;
  server_name _;
  return 301 https://www.demo.wsr;

}
```

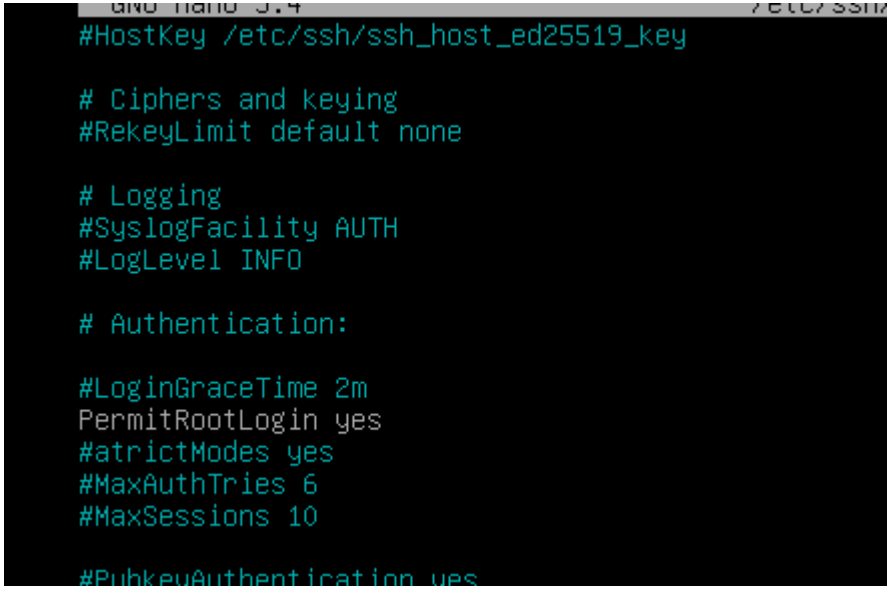


systemctl reload nginx

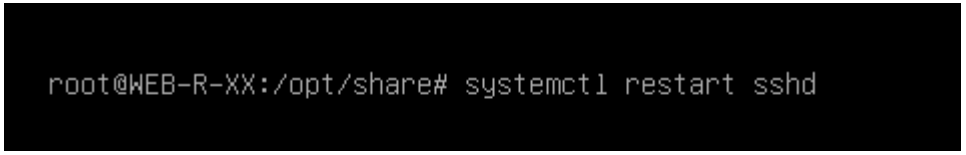
WEB-R ssh

Отредактировать конфиг ssh

nano /etc/ssh/sshd_config



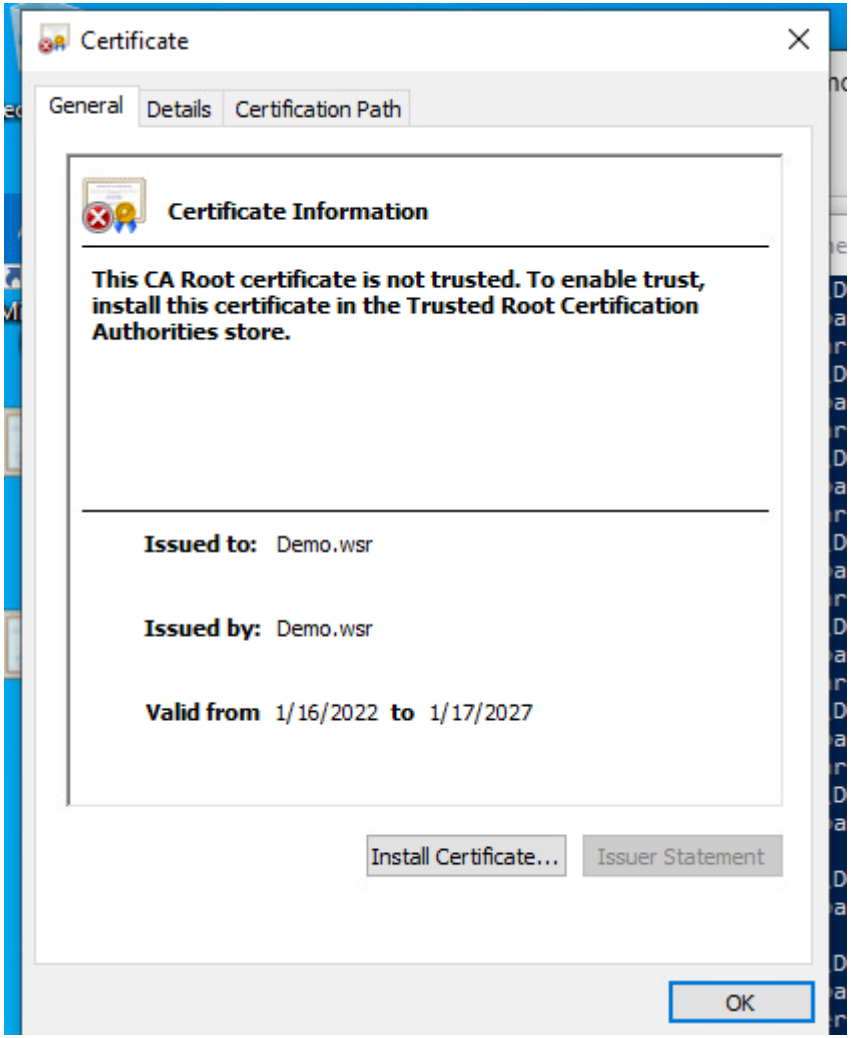
systemctl restart sshd



CLI ssl

Открыть PowerShell и скопировать сертификат с WEB-R, далее установить.

scp -P 2244 'root@5.5.5.100:/opt/share/www.cer' C:\Users\user\Desktop\



Проверку осуществлять в IE