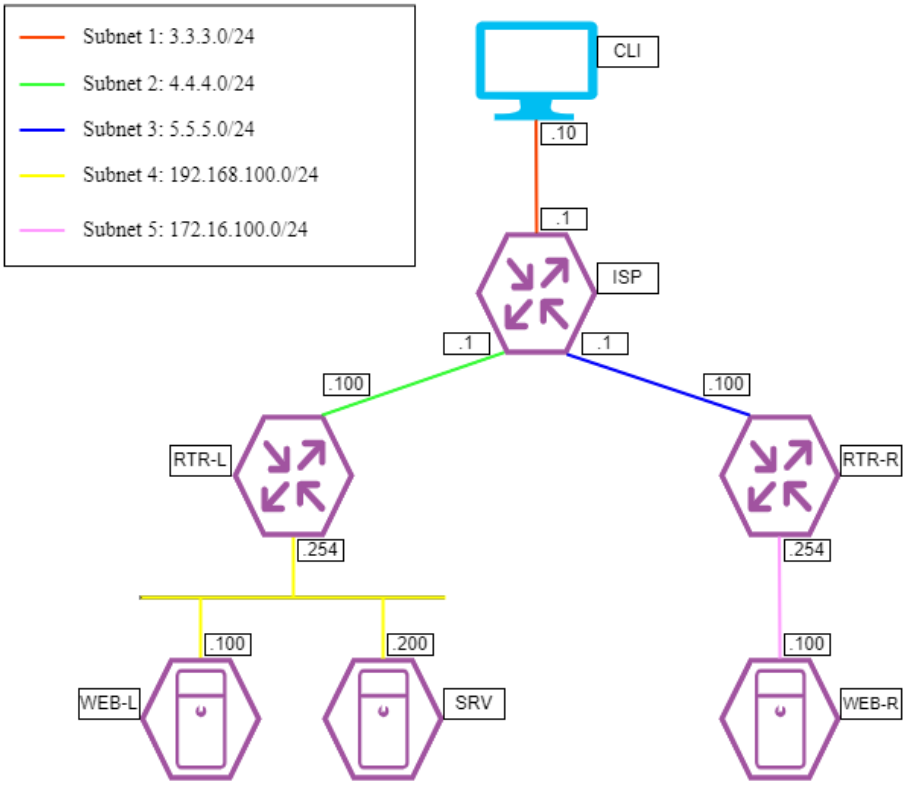
DEMO2022

Образец задания:

Образец задания для демонстрационного экзамена по комплекту оценочной документации.

Описание задания:

Топология сети



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.

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

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

Оглавление

Характеристики ВМ

Name VM	ОС	RAM	CPU	IP	Additionally
RTR-L	Debian 11/CSR	2 GB	2/4	4.4.4.100/24	
				192.168.200.254/24	
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	192.168.200.200/24	Доп диски 2 шт по 5 GB
WEB-L	Debian 11	2 GB	2	192.168.200.100/24	
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	

Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой. Настройку начинаем с RTR-L, RTR-R и ISP.

RTR-L (базовая настройка адресации)

```
en
conf t
hostname RTR-L
do wr
int gi 1
ip address 4.4.4.100 255.255.255.0
no sh
ip nat outside
int gi 2
ip address 192.168.200.254 255.255.255.0
no sh
ip nat inside
ip route 0.0.0.0 0.0.0.0 4.4.4.1
do wr
```

RTL-R (базовая настройка адресации)

```
en
conf t
hostname RTR-R
do wr
int gi 1
```

```
ip address 5.5.5.100 255.255.255.0
ip nat outside
no sh
int gi 2
ip address 172.16.100.254 255.255.255.0
ip nat inside
no sh
ip route 0.0.0.0 0.0.0.0 5.5.5.1
do wr
```

ISP

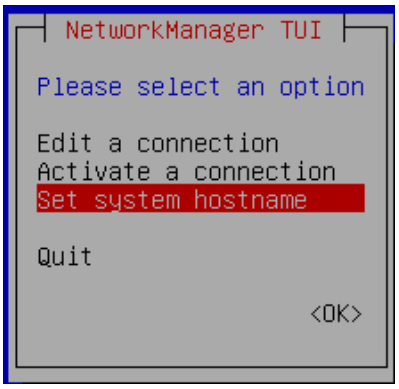
```
apt-cdrom add
apt install -y network-manager bind9 chrony
nano /etc/sysctl.conf
```

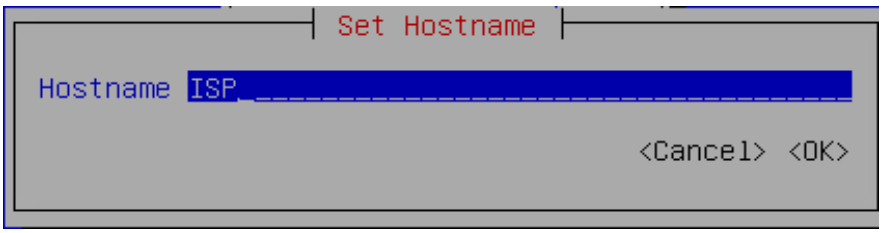
```
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

sysctl -p

nmtui

Wired Connection	Adapter	IP&Mask	Default Gateway
Wired Connection 1	Ens192	3.3.3.1/24	Null
Wired Connection 2	Ens224	4.4.4.1/24	4.4.4.100
Wired Connection 3	Ens256	5.5.5.1/24	Null






```
Reboot
mkdir /opt/dns
cp /etc/bind/db.local /opt/dns/demo.db
chown -R bind:bind /opt/dns
nano /etc/apparmor.d/usr.sbin.named
```

```
  # /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,
```

systemctl restart apparmor.service
nano /etc/bind/named.conf.options

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                4.4.4.100;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no;
        allow-query { any; };
        listen-on-v6 { any; };
};
```

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

```
// 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";
};
```

nano /opt/dns/demo.db

```
 GNU nano 5.4                                  /opt/dns/demo.db
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     demo.wsr. root.demo.wsr. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      isp.demo.wsr.
isp     IN      A       3.3.3.1
www     IN      A       4.4.4.100
www     IN      A       5.5.5.100
internet        CNAME   isp.demo.wsr.
int     IN      NS      rtr-1.demo.wsr.
rtr-1   IN      A       4.4.4.100
```

```
systemctl restart bind9
nano /etc/chrony/chrony.conf
```

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

local stratum 4
allow 3.3.3.0/24
allow 4.4.4.0/24
```

```
systemctl restart chronyd
```

RTR-L (проброс портов и настройка туннеля)

```
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
router eigrp 6500
network 192.168.200.0 0.0.0.255
network 172.16.1.0 0.0.0.255
crypto isakmp policy 1
encr aes
authentication pre-share
hash sha256
group 14
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
crypto ipsec profile VTI
set transform-set TSET
interface Tunnel1
tunnel mode ipsec ipv4
tunnel protection ipsec profile VTI
ip nat inside source static tcp 192.168.200.100 22 4.4.4.100 2222
ip nat inside source static tcp 192.168.200.200 53 4.4.4.100 53
ip nat inside source static udp 192.168.200.200 53 4.4.4.100 53
ip nat inside source static udp 192.168.200.200 123 4.4.4.100 123
no ip http secure-server
```

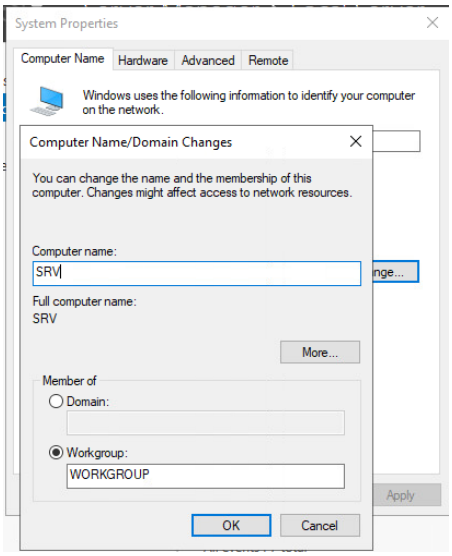
```
wr
reload
ip nat inside source static tcp 192.168.200.100 80 4.4.4.100 80
ip nat inside source static tcp 192.168.200.100 443 4.4.4.100 443
```

RTR-R(проброс портов и настройка туннеля)

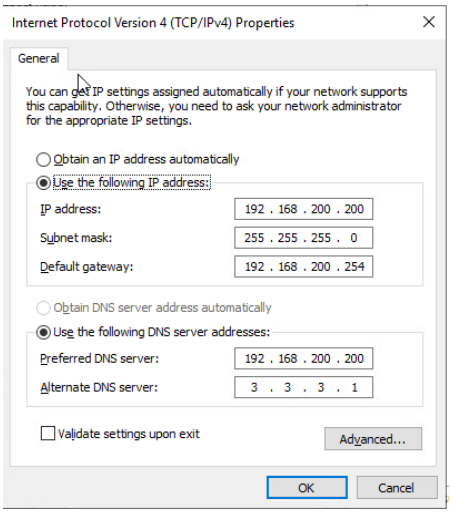
```
interface Tunne 1
ip address 172.16.1.2 255.255.255.0
tunnel mode gre ip
tunnel source 5.5.5.100
tunnel destination 4.4.4.100
router eigrp 6500
network 172.16.100.0 0.0.0.255
network 172.16.1.0 0.0.0.255
crypto isakmp policy 1
encr aes
authentication pre-share
hash sha256
group 14
crypto isakmp key 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
interface Tunnel1
tunnel mode ipsec ipv4
tunnel protection ipsec profile VTI
ip nat inside source static tcp 172.16.100.100 22 5.5.5.100 2244
ip nat inside source static tcp 172.16.100.100 53 5.5.5.100 53
ip nat inside source static udp 172.16.100.100 53 5.5.5.100 53
ip nat inside source static udp 172.16.100.100 123 5.5.5.100 123

no ip http secure-server
wr
reload
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
```

SRV

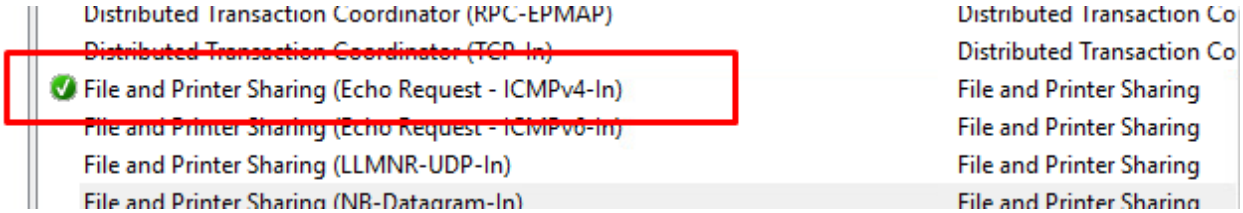
1. Присваиваем имя SRV

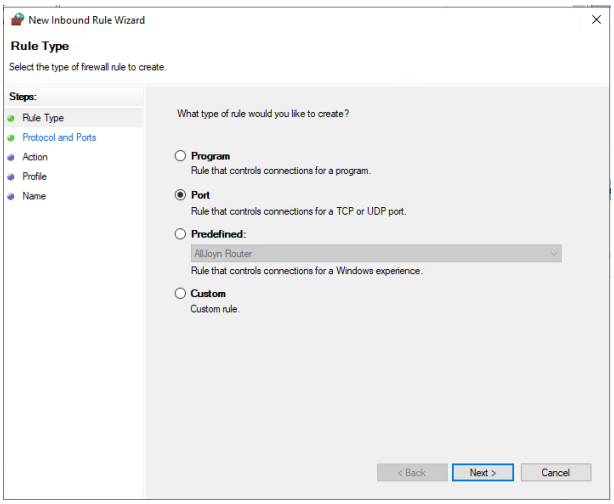


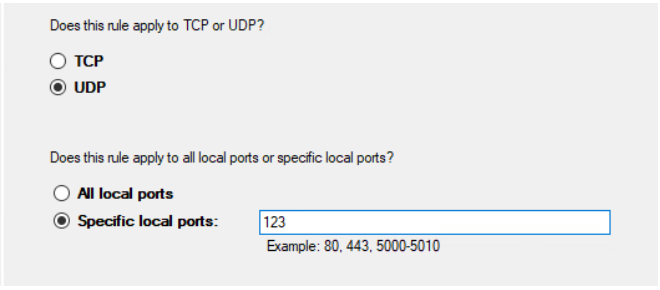
2. Устанавливаем IP-адрес.

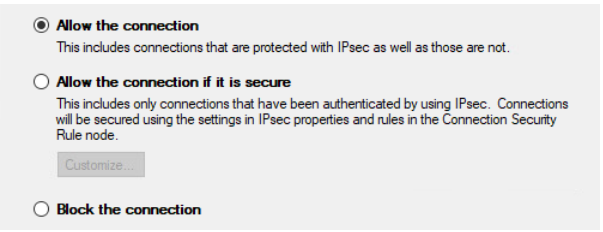


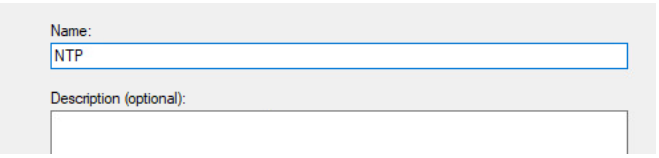
3. Включаем ICMP-запросы и создаем правило для NTP в Windows Firewall.



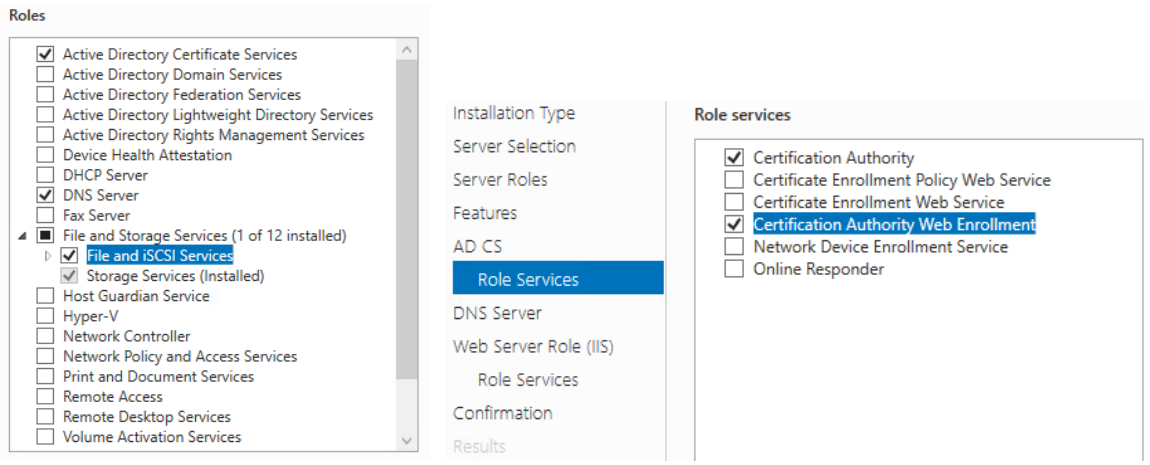


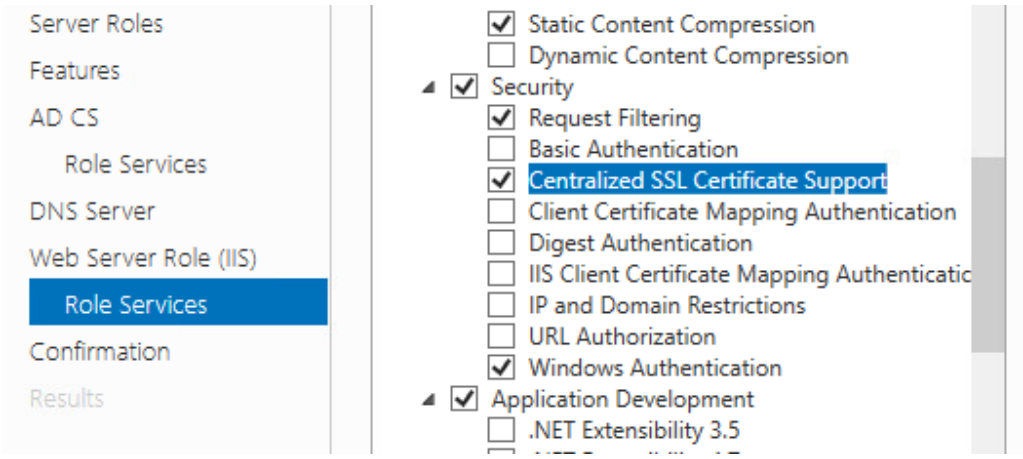






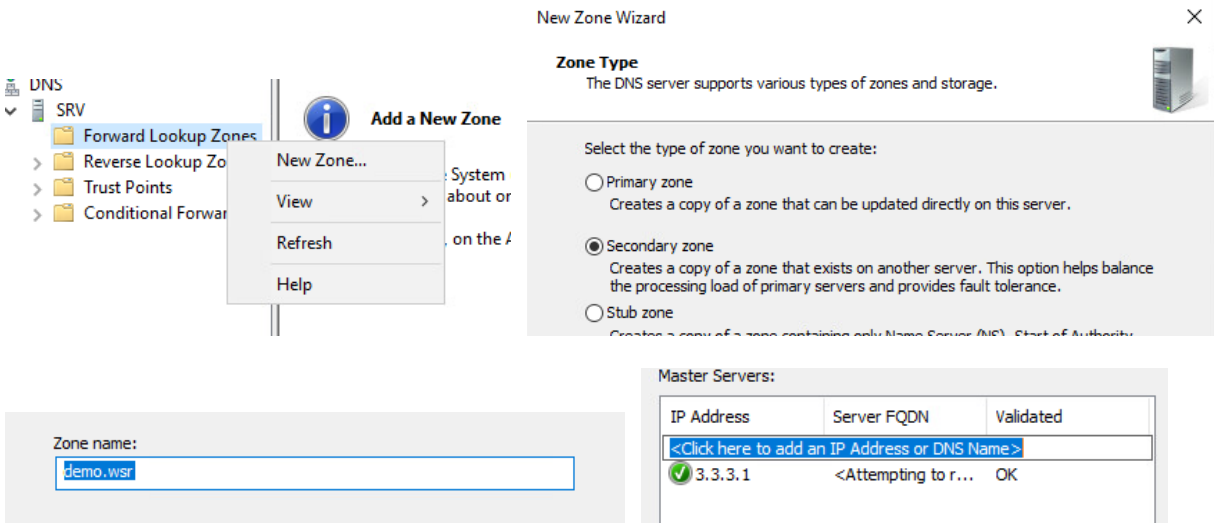
4. Устанавливаем компоненты



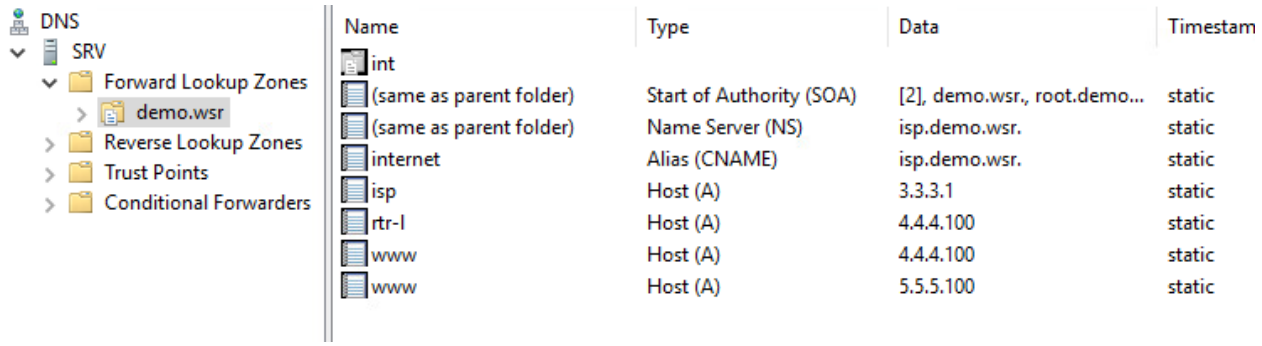


5. Настройка DNS

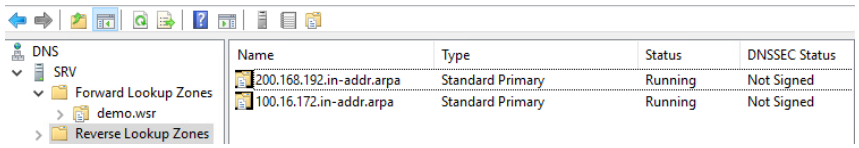
1.1. Создаем вторичную зону



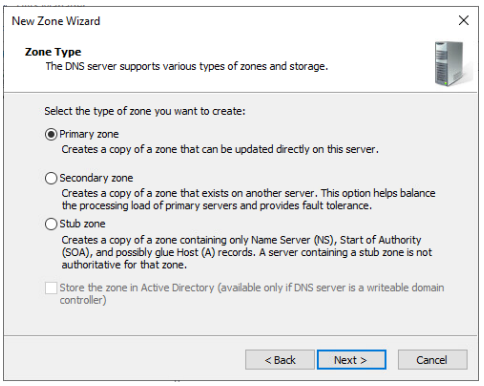
(Если с первого раза вторичная зона не определилась, удаляем ее и делаем снова)

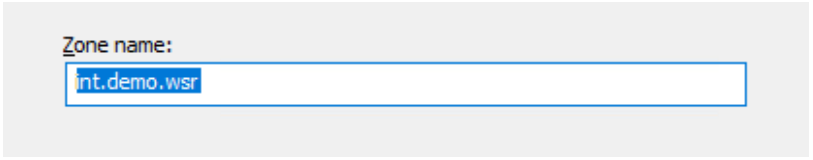


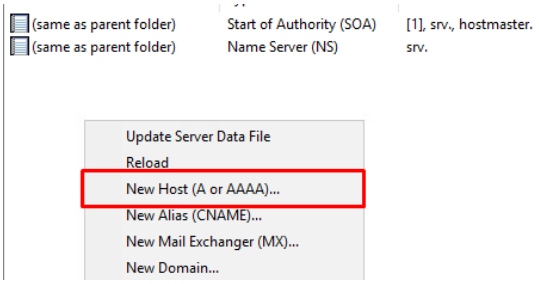
1.2. Создаем обратную зону

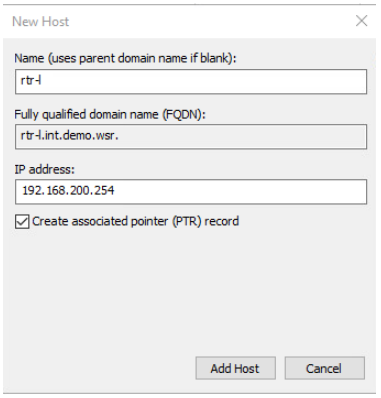


1.3. Создаем первичную зону

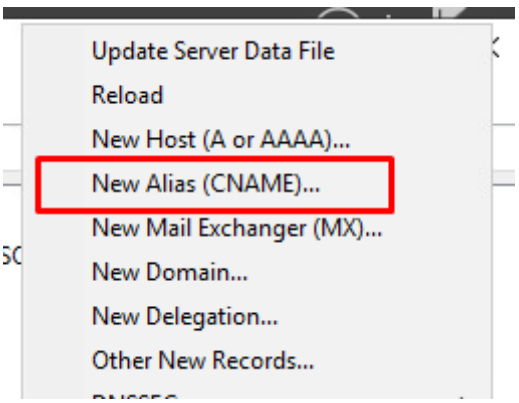

New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps 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

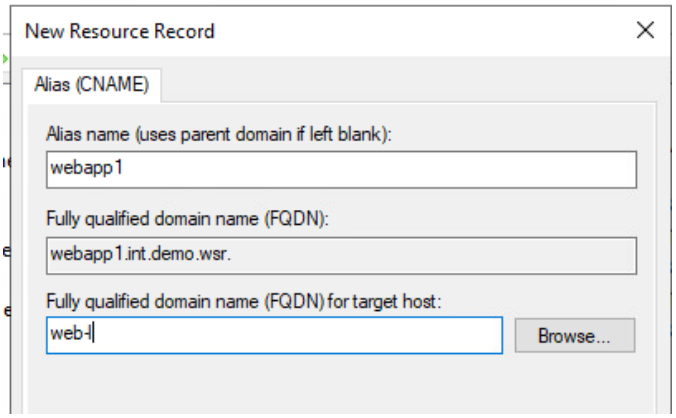

Zone name:
int.demo.wsr


(same as parent folder)
Start of Authority (SOA)
[1], srv., hostmaster.
(same as parent folder)
Name Server (NS)
srv.
Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...


New Host
Name (uses parent domain name if blank):
rtr-l
Fully qualified domain name (FQDN):
rtr-l.int.demo.wsr.
IP address:
192.168.200.254
Create associated pointer (PTR) record
Add Host
Cancel

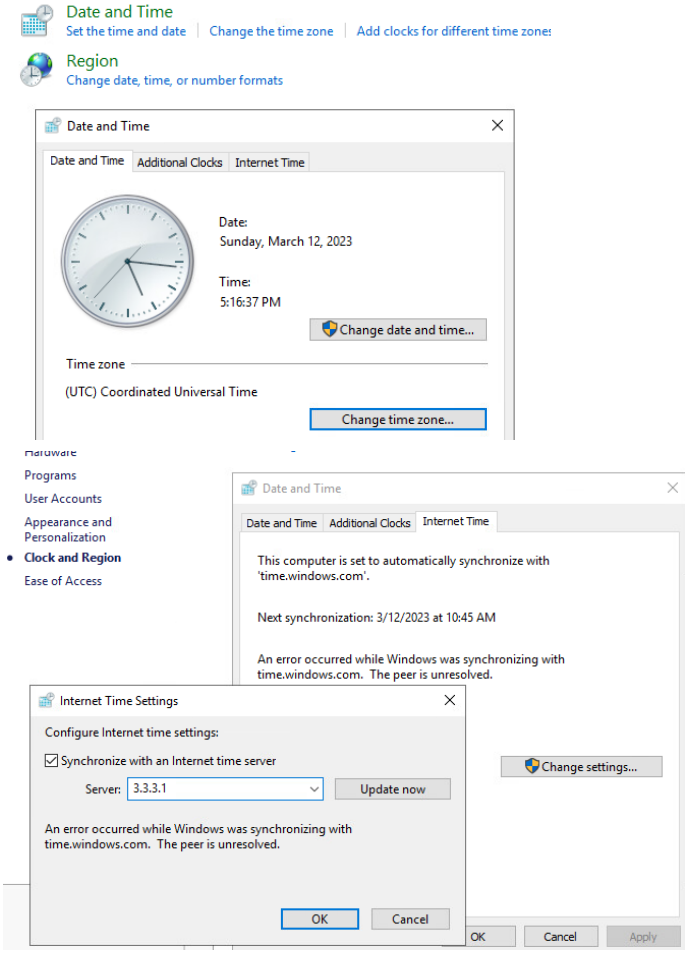

rtr-l Host (A) 192.168.200.254
rtr-r Host (A) 172.16.100.254
web-l Host (A) 192.168.200.100
web-r Host (A) 172.16.100.100
srv Host (A) 192.168.200.200


Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...
New Delegation...
Other New Records...

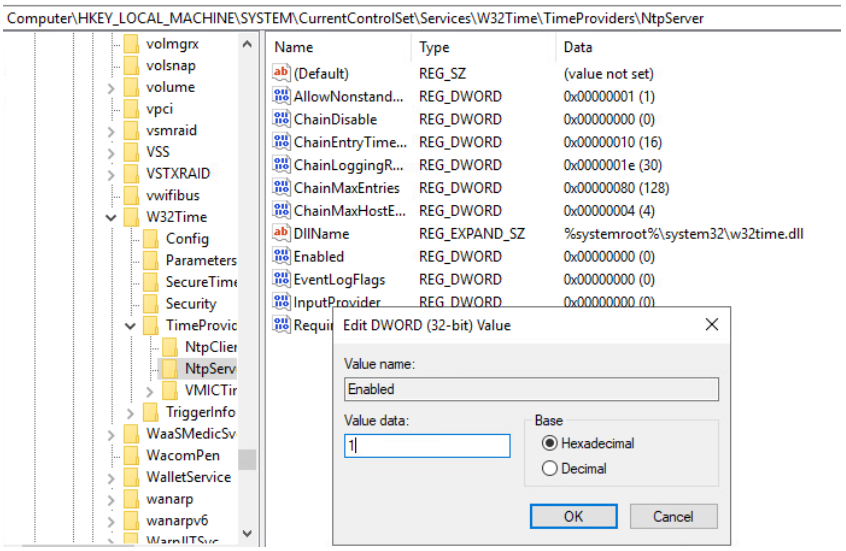

New Resource Record
Alias (CNAME)
Alias name (uses parent domain if left blank):
webapp1
Fully qualified domain name (FQDN):
webapp1.int.demo.wsr.
Fully qualified domain name (FQDN) for target host:
web-l
Browse...

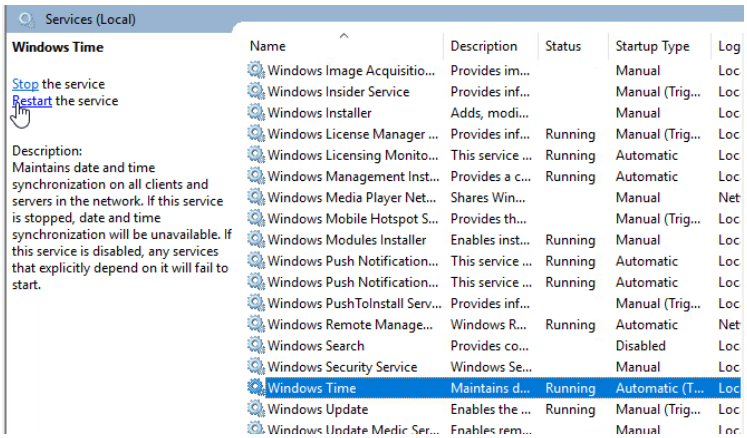

webapp1 Alias (CNAME) web-l
webapp2 Alias (CNAME) web-r
ntp Alias (CNAME) srv
dns Alias (CNAME) srv

6. Настройка NTP

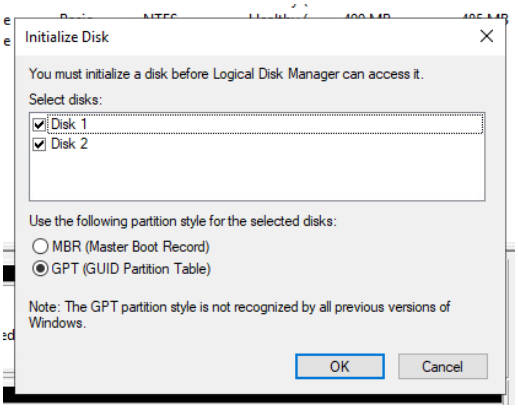


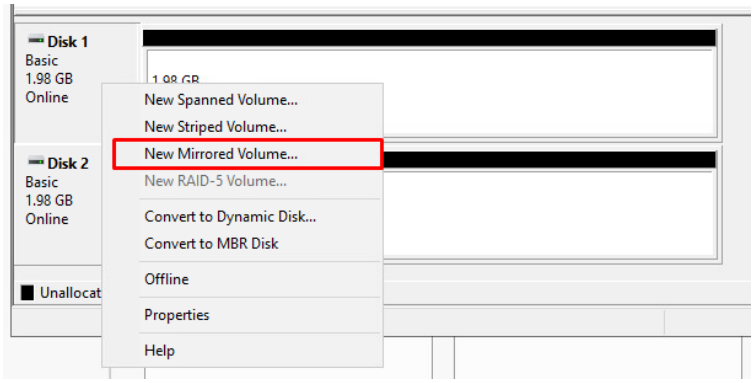
Заходим в regedit, по пути:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled`

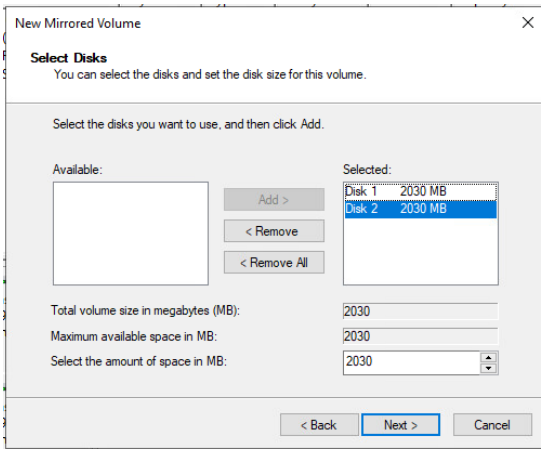


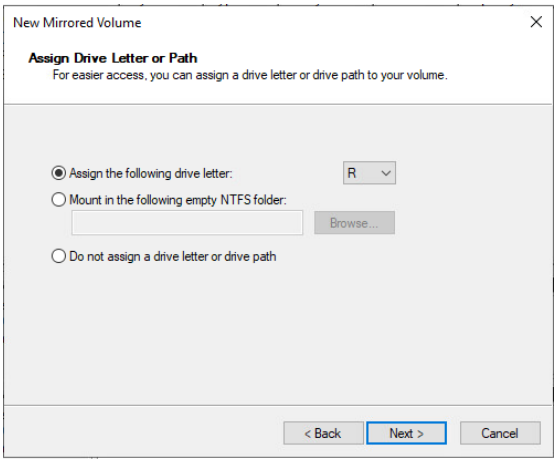


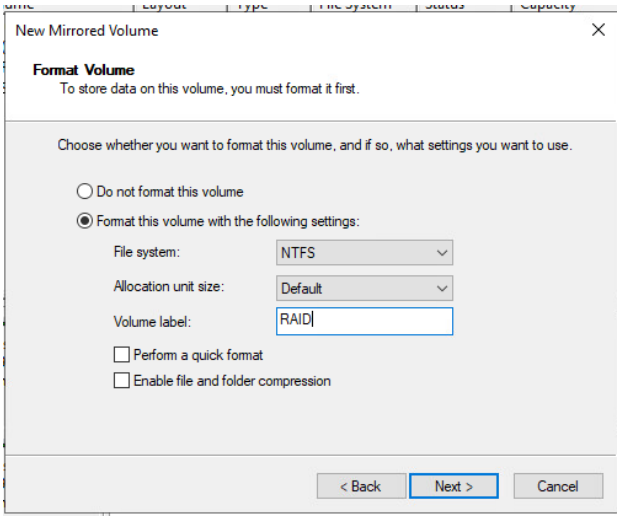
7. Создание RAID-массива



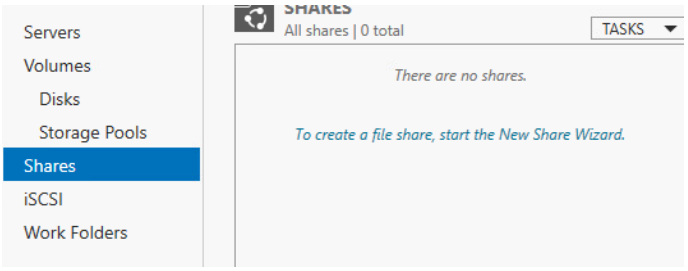


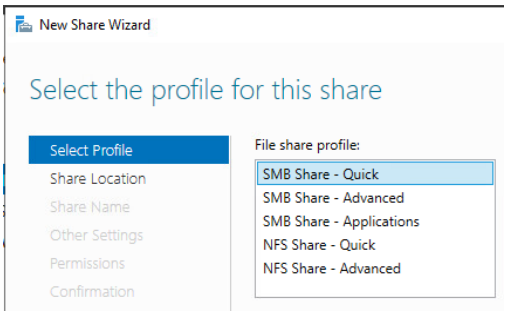


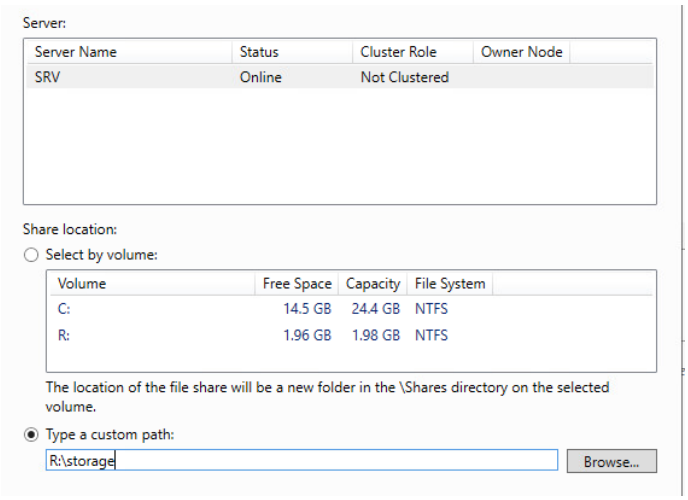


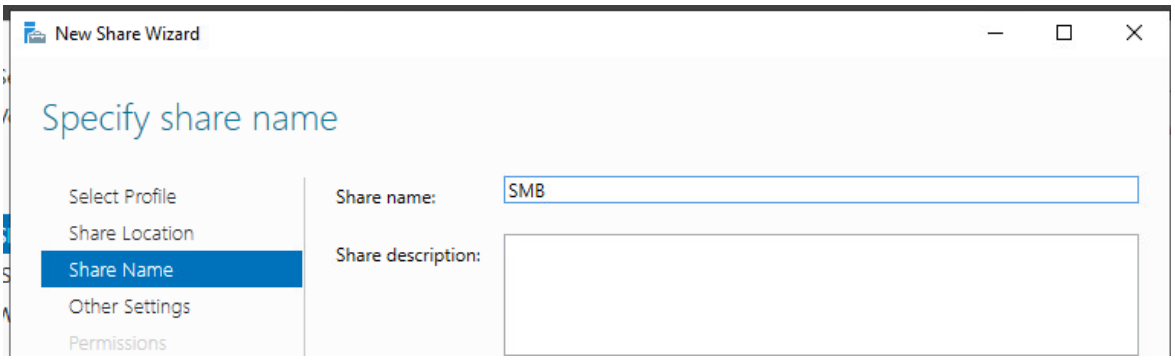


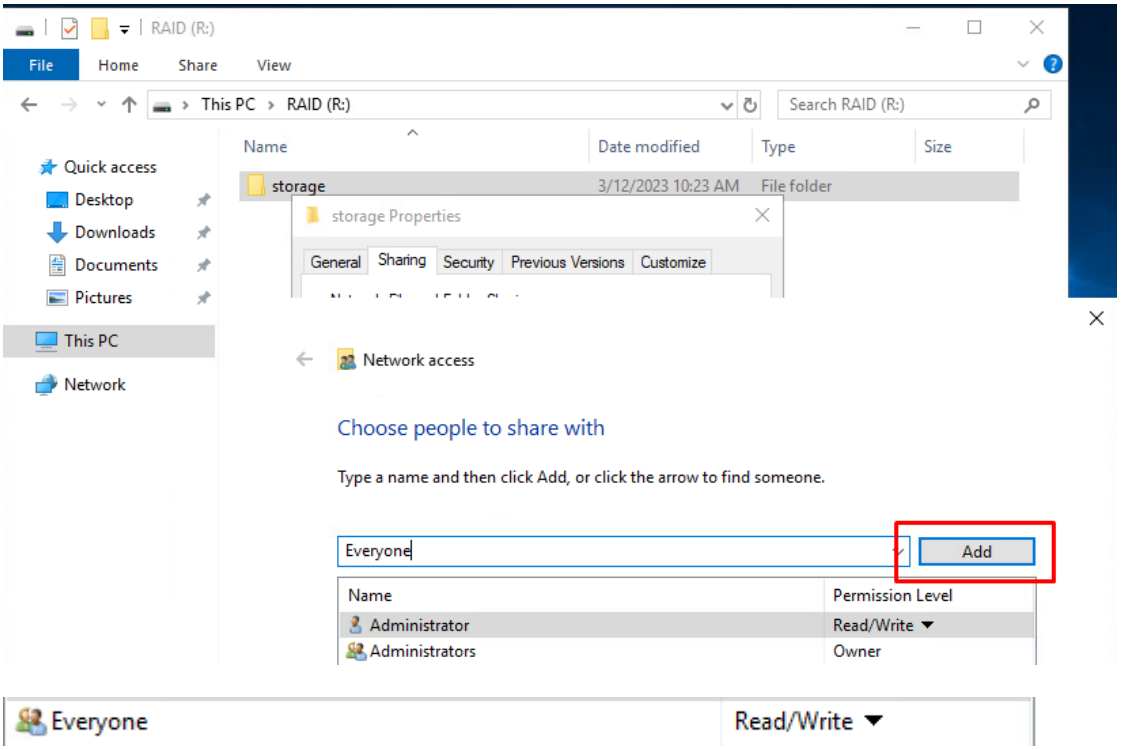
8. Настройка SMB



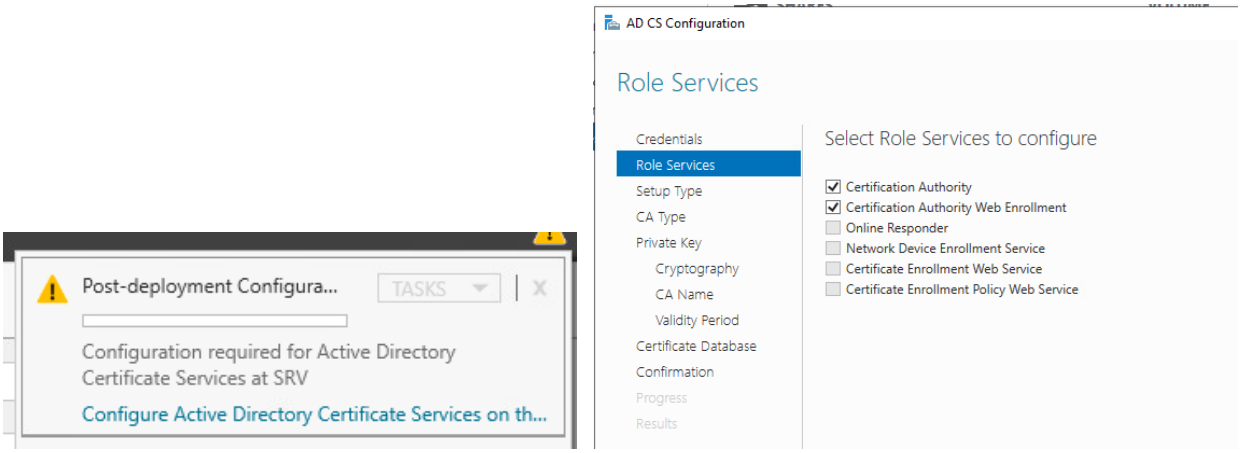


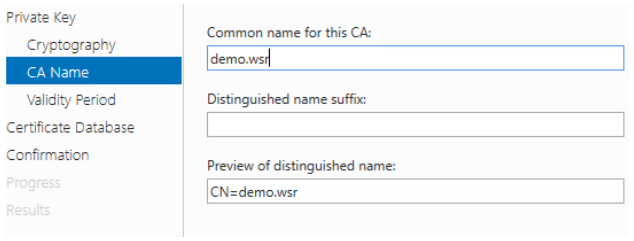


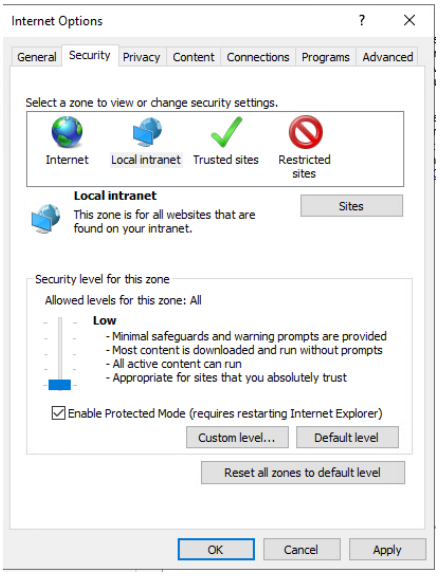


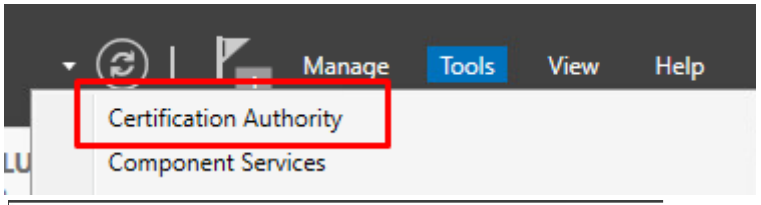


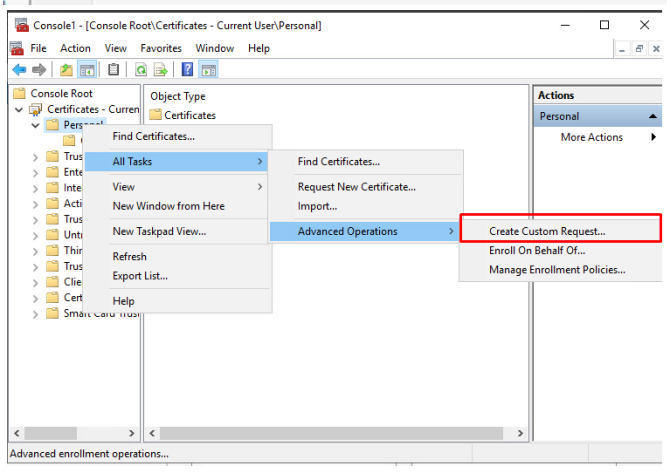
9. Создание сертификатов

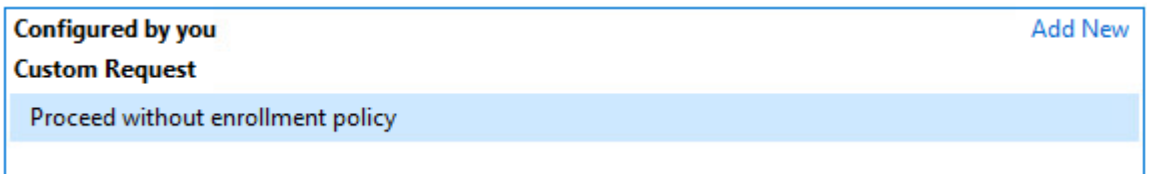


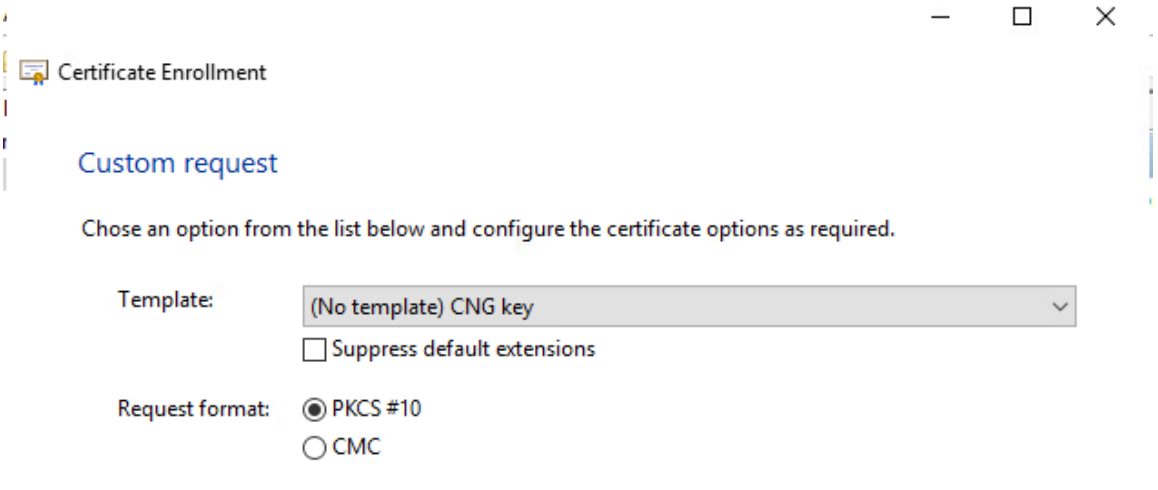

Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Common name for this CA:
demo.wsr
Distinguished name suffix:
Preview of distinguished name:
CN=demo.wsr

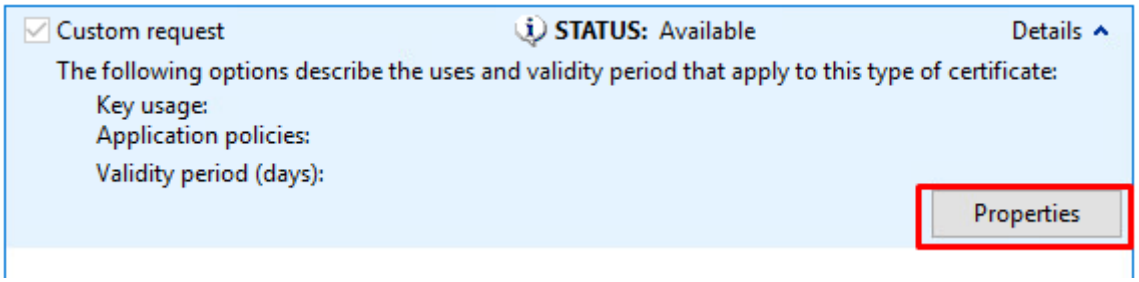

Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Select a zone to view or change security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Local intranet
This zone is for all websites that are found on your intranet.
Sites
Security level for this zone
Allowed levels for this zone: All
Low
- Minimal safeguards and warning prompts are provided
- Most content is downloaded and run without prompts
- All active content can run
- Appropriate for sites that you absolutely trust
Enable Protected Mode (requires restarting Internet Explorer)
Custom level...
Default level
Reset all zones to default level
OK
Cancel
Apply

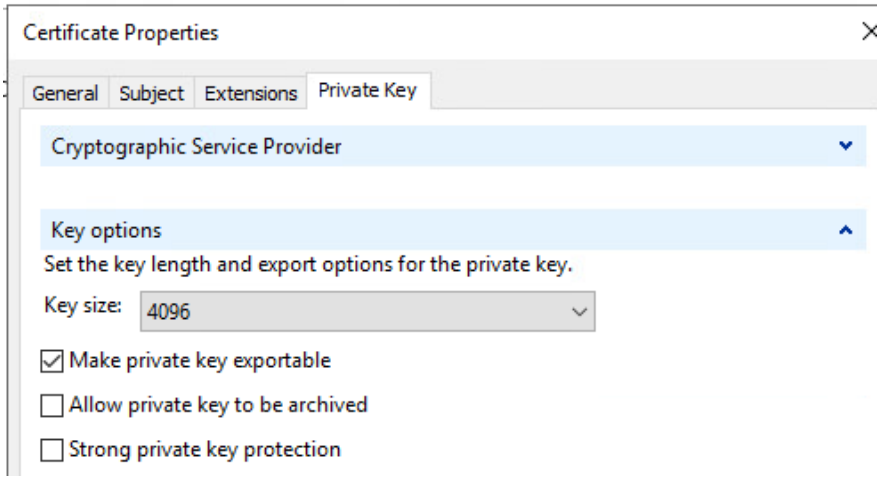

Manage
Tools
View
Help
Certification Authority
Component Services

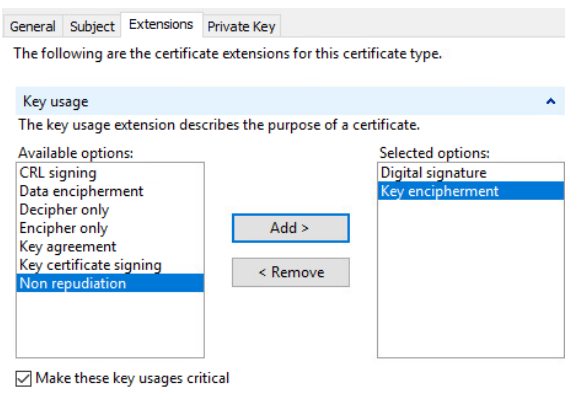

Console1 - [Console Root\Certificates - Current User\Personal]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Curren
Object Type
Certificates
Actions
Personal
More Actions
Find Certificates...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Find Certificates...
Request New Certificate...
Import...
Advanced Operations
Create Custom Request...
Enroll On Behalf Of...
Manage Enrollment Policies...
Advanced enrollment operations...

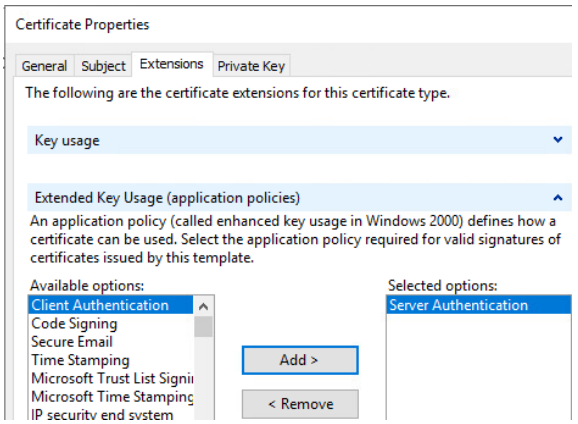

Configured by you
Add New
Custom Request
Proceed without enrollment policy

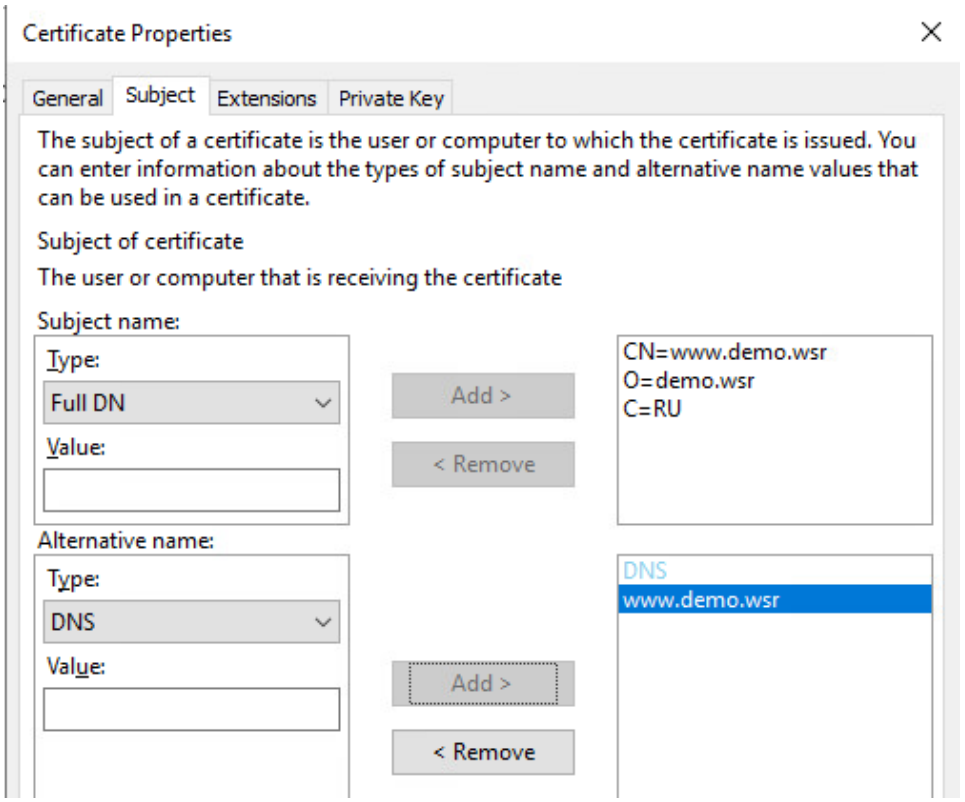

Certificate Enrollment
Custom request
Chose an option from the list below and configure the certificate options as required.
Template:
(No template) CNG key
Suppress default extensions
Request format:
PKCS #10
CMC

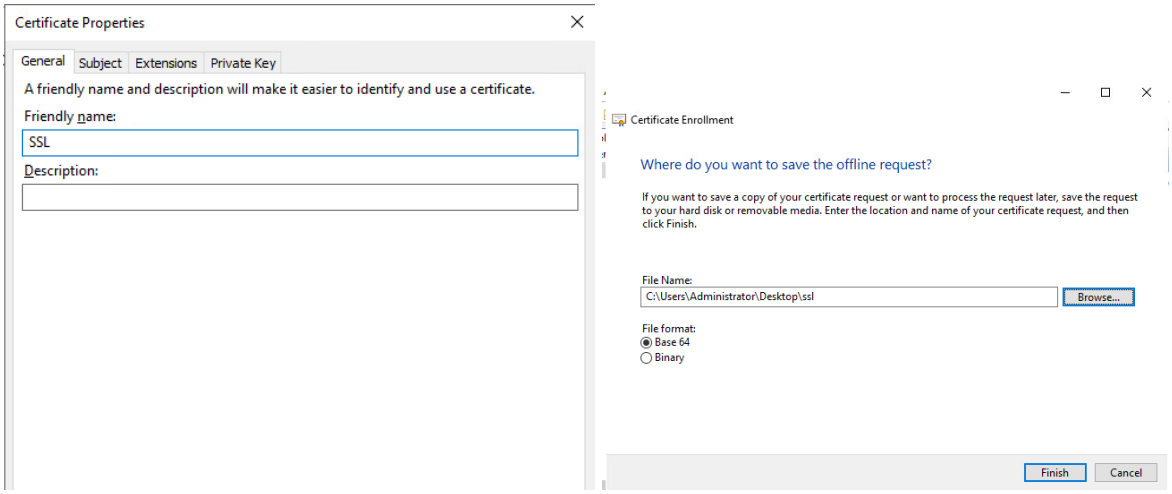

Custom request
STATUS: Available
Details
The following options describe the uses and validity period that apply to this type of certificate:
Key usage:
Application policies:
Validity period (days):
Properties

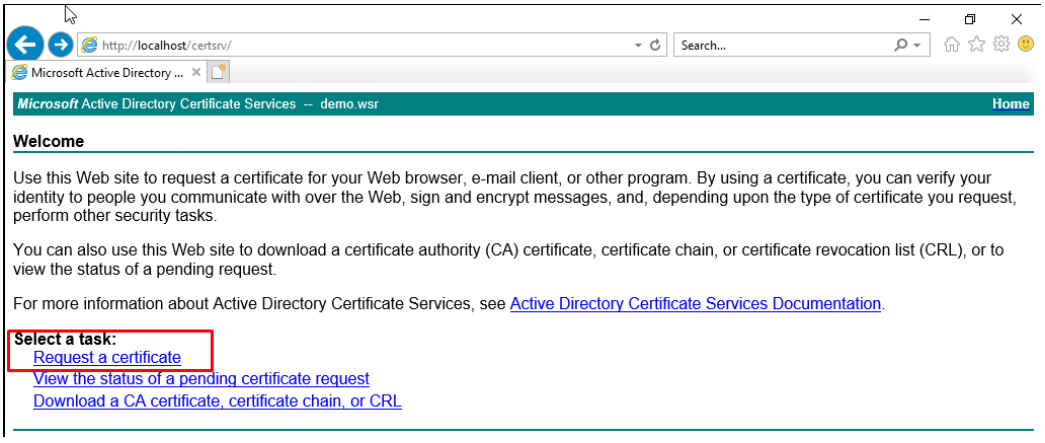

Certificate Properties
General
Subject
Extensions
Private Key
Cryptographic Service Provider
Key options
Set the key length and export options for the private key.
Key size:
4096
Make private key exportable
Allow private key to be archived
Strong private key protection

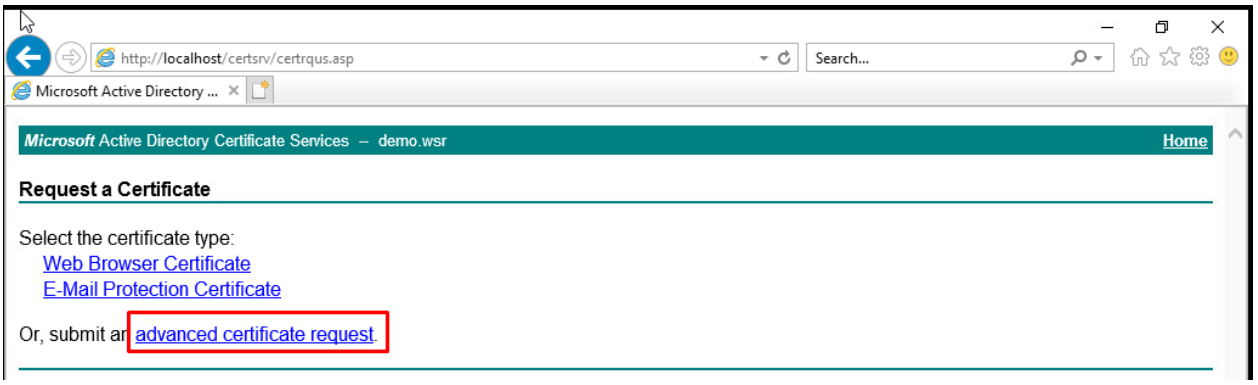

General
Subject
Extensions
Private Key
The following are the certificate extensions for this certificate type.
Key usage
The key usage extension describes the purpose of a certificate.
Available options:
CRL signing
Data encipherment
Decipher only
Encipher only
Key agreement
Key certificate signing
Non repudiation
Add >
< Remove
Selected options:
Digital signature
Key encipherment
Make these key usages critical

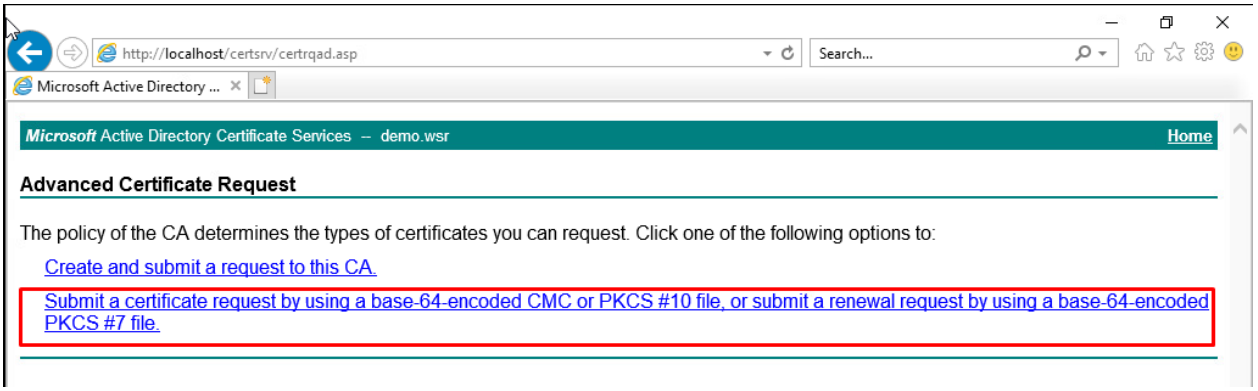

Certificate Properties
General
Subject
Extensions
Private Key
The following are the certificate extensions for this certificate type.
Key usage
Extended Key Usage (application policies)
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Available options:
Client Authentication
Code Signing
Secure Email
Time Stamping
Microsoft Trust List Signi
Microsoft Time Stamping
IP security end system
Add >
< Remove
Selected options:
Server Authentication

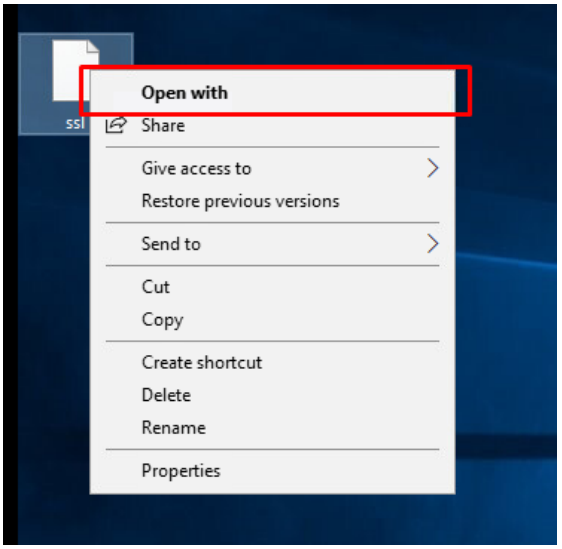

Certificate Properties
General
Subject
Extensions
Private Key
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.
Subject of certificate
The user or computer that is receiving the certificate
Subject name:
Type:
Full DN
Value:
Add >
< Remove
CN=www.demo.wsr
O=demo.wsr
C=RU
Alternative name:
Type:
DNS
Value:
Add >
< Remove
DNS
www.demo.wsr

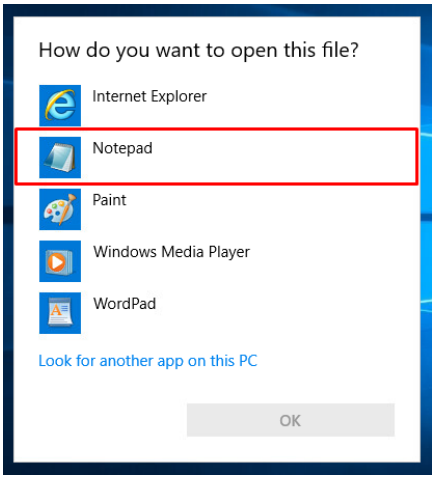

Certificate Properties
General
Subject
Extensions
Private Key
A friendly name and description will make it easier to identify and use a certificate.
Friendly name:
SSL
Description:
Certificate Enrollment
Where do you want to save the offline request?
If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.
File Name:
C:\Users\Administrator\Desktop\ssl
Browse...
File format:
Base 64
Binary
Finish
Cancel


http://localhost/certsrv/
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- demo.wsr
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

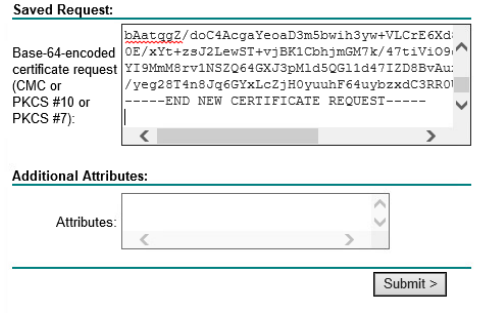

http://localhost/certsrv/certrqus.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- demo.wsr
Home
Request a Certificate
Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate
Or, submit an advanced certificate request.

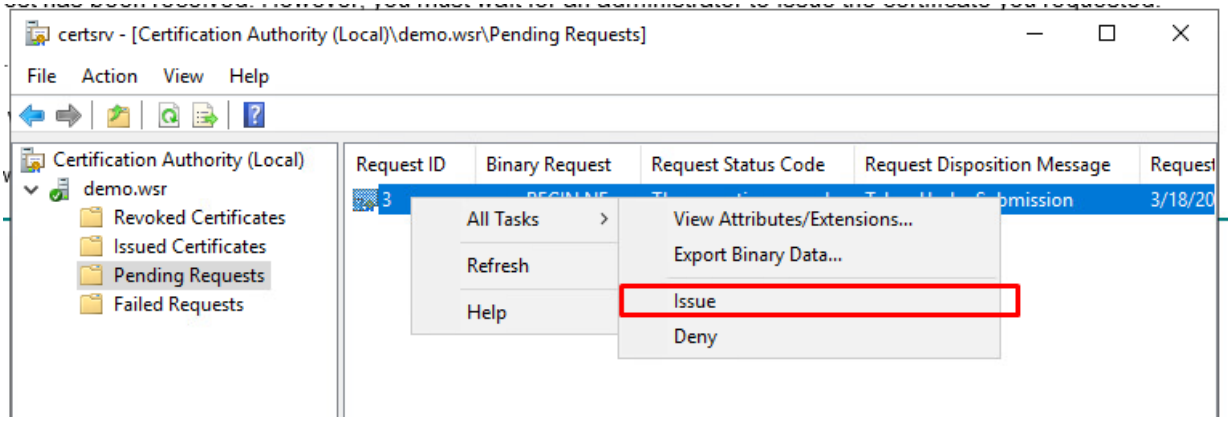

http://localhost/certsrv/certrqad.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- demo.wsr
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit 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.

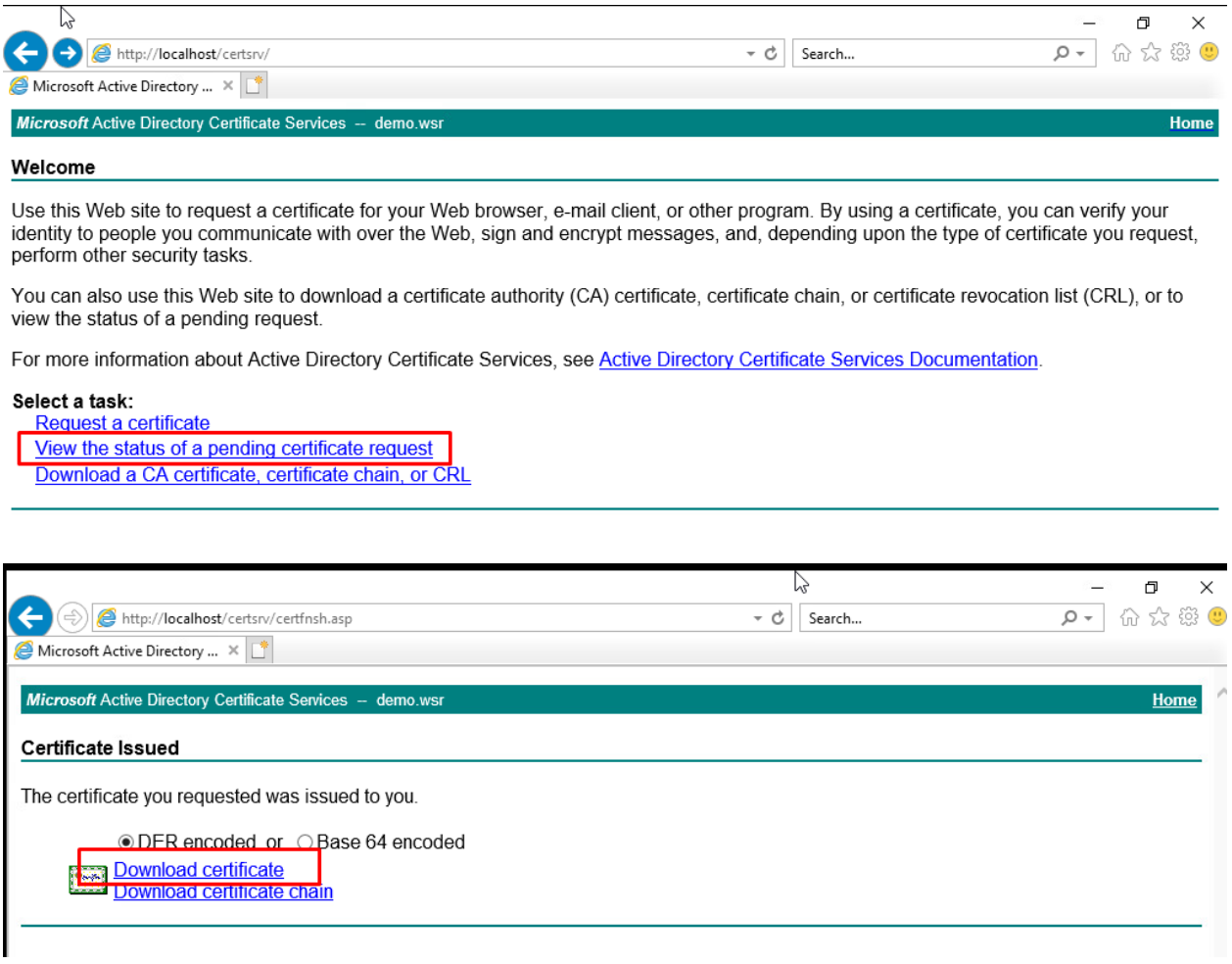

ssl
Open with
Share
Give access to
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties


How do you want to open this file?
Internet Explorer
Notepad
Paint
Windows Media Player
WordPad
Look for another app on this PC
OK

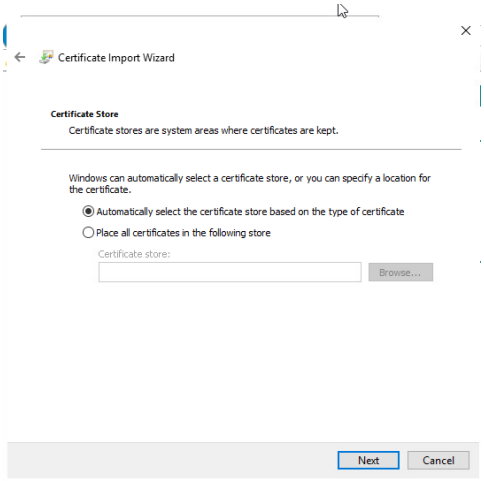

ssl - Notepad
File Edit Format View Help
gzanf9X+1g169EBsE06WRFJ3Qd1IIrxSDAxrmeTunDAWaZObpYfXSLAehe2AS2Jw
YOtbh6C+SiSPhBZLPI+1Ge950J9hbJ5uPGusTI/usguKvxMHnRivuRnrHMbNxbPP
s1Vl3tVlzB5/IylnZgIjigtIag3EwuHpfg6dmi9pO0nHy4QY5QIDAQABoIIBRzAc
BgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3NjMuMjAzBgkrBgEEAYI3FRQxJjAkAgEF
DANTU1YMEVNSVlxBZG1pbmlzdHJhdG9yDAdNTUMuRVhFMGYGCisGAQQBgjcNAgIx
WDBWAgEAHk4ATQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZg80AHcAYQByAGUAIABL
AGUAeQAgAFMAdABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZAB1AHIDAQAwgYkGCSqG
SIb3DQEJDjF8MHowFwYDVR0RBBAwDoIMd3d3LmR1bW8ud3NyMA4GA1UdDwEB/wQE
AwIFoDATBgNVHSUEDDAKBggrBgEFBQcDATAbBgkrBgEEAYI3FQoEDjAMMAoGCCsG
AQUFBwMBM80GA1UdDgQWBBTFd7CQUtHGehzhBq2154M/aqO9DzANBgkqhkiG9w0B
AQsFAAOCAgEALxiehVWdBBGwM+uQ82xaYruPsPKAOvuz7zw+5xKExdhBuJtiKBii
OdrarILm1WOi8N2xMEXN+AouI0KQOyKdljIsa6bpVdRxA92et6Li+/uJEBWIVdeC
iRmx/NF7dDjIH+1rV16Ul7IyCjyIDNR/y44+gfWdQD6rH4fvGRrYK2wb1LR9qmoj
evi5inTz7IFxvJNrhGRPaJi3dnBqeJPBHrKMZ4qZ5poenTPgjEdkh3lYWjpJElRT
Zzlgj8Pg3g70LSSWyePQ6RdjEbMSGoelgppoBmH8RBujLHKiEn+nEIJe3sWK+g/U
QshB8YO/h+ye4JfXKhHP17Nr1JcvFEQnPGtOnvwE72sflW4lf3BYwLw4GEIH+p31
su6pzhk+BKL1BvzoIt4V/oqSC7n+3hNWz3evm1MewTWNh5v+kJaByd2YnjKiE28A
bAatqgZ/doC4AcgaYeoaD3m5bwih3yw+VLCrE6Xd80T4DZXDLIV5BVpCiDK76zFM
0E/xYt+zsJ2LewST+vjBK1CbhjmGM7k/47tiViO9qxTlWOPo8SPOnLa431PssgQb
YI9MmM8rv1NSZQ64GXJ3pMld5QGl1d47IZD8BvAuxQNd19wJHn8nWhIHMMU/0tDg
/yeg28T4n8Jq6GYxLcZjH0yuuhF64uybzxdC3RR0UhAiPLqGAZM15R0=
-----END NEW CERTIFICATE REQUEST-----
CTRL-A + CTRL-C
Windows (CRLF)
Ln 34, Col 1
100%

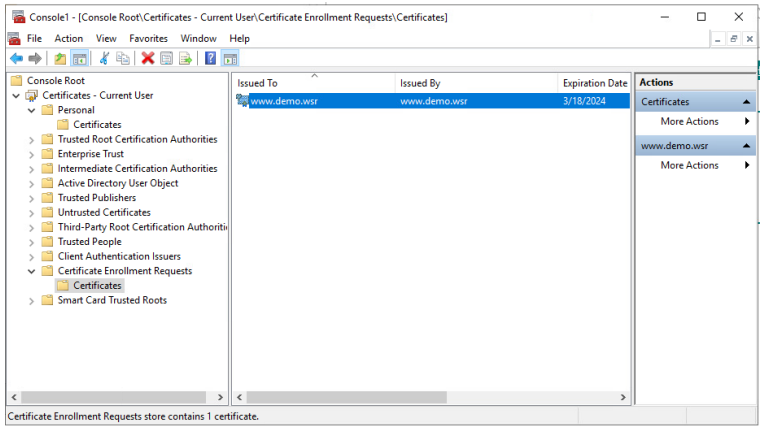

Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
bAatqgZ/doC4AcgaYeoaD3m5bwih3yw+VLCrE6Xd
0E/xYt+zsJ2LewST+vjBK1CbhjmGM7k/47tiViO9
YI9MmM8rv1NSZQ64GXJ3pMld5QGl1d47IZD8BvAu
/yeg28T4n8Jq6GYxLcZjH0yuuhF64uybzxdC3RR0
-----END NEW CERTIFICATE REQUEST-----
Additional Attributes:
Attributes:
Submit >

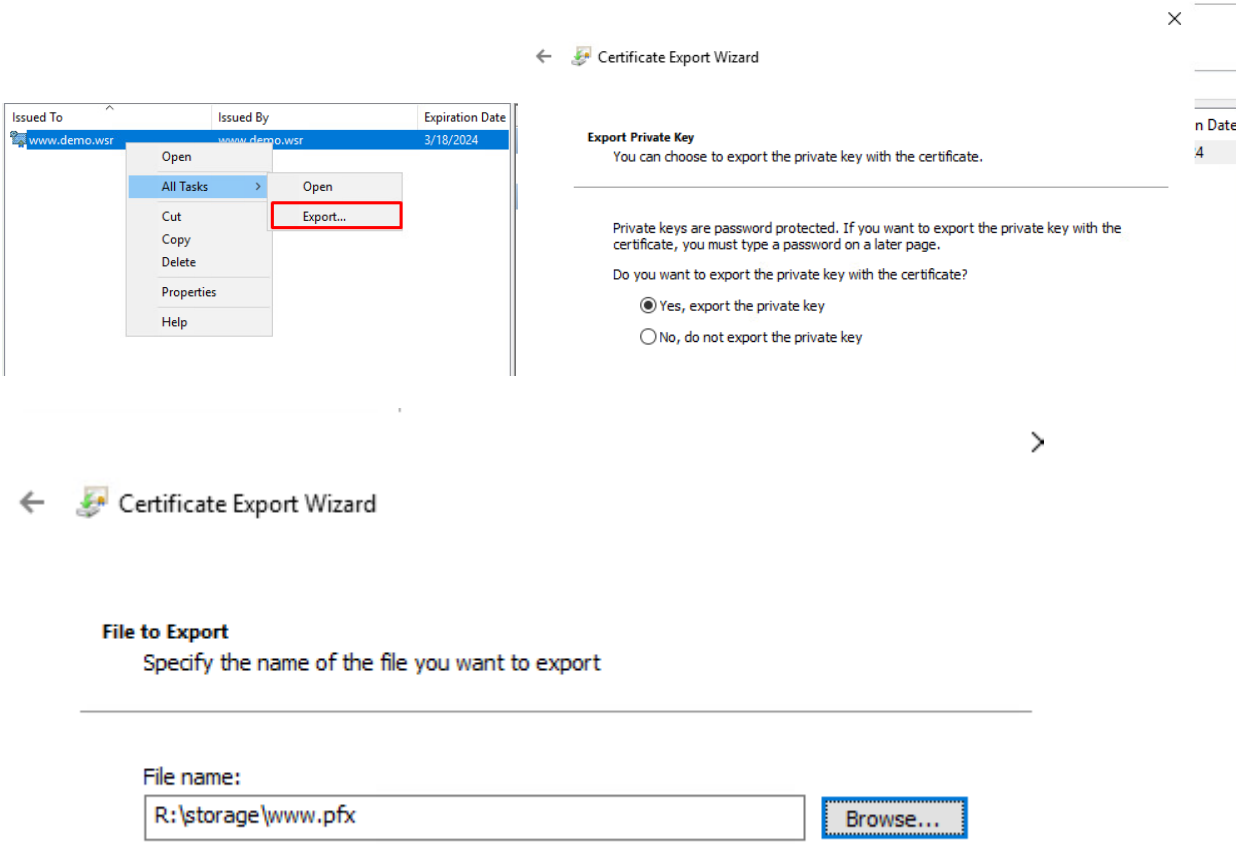

certsrv - [Certification Authority (Local)\demo.wsr\Pending Requests]
File Action View Help
Certification Authority (Local)
demo.wsr
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Request ID
Binary Request
Request Status Code
Request Disposition Message
All Tasks
Refresh
Help
View Attributes/Extensions...
Export Binary Data...
Issue
Deny


http://localhost/certsrv/
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- demo.wsr
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

http://localhost/certsrv/certfnsh.asp
Search...
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- demo.wsr
Home
Certificate Issued
The certificate you requested was issued to you.
DER encoded or Base 64 encoded
Download certificate
Download certificate chain


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Next
Cancel


Console1 - [Console Root\Certificates - Current User\Certificate Enrollment Requests\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Certificates
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
www.demo.wsr
www.demo.wsr
3/18/2024
Actions
Certificates
More Actions
www.demo.wsr
More Actions
Certificate Enrollment Requests store contains 1 certificate.



RTR-L (NTP)

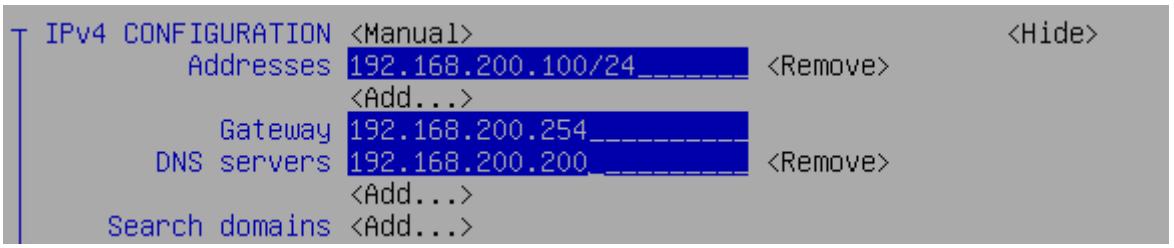
```
ip domain name int.demo.wsr
ip name-server 192.168.200.200
ntp server ntp.int.demo.wsr
```

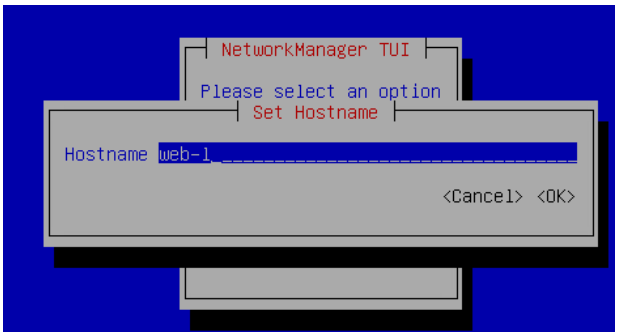
RTR-R (NTP)

```
ip domain name int.demo.wsr
ip name-server 192.168.200.200
ntp server ntp.int.demo.wsr
```

WEB-L

```
apt-cdrom add
apt install -y network-manager mc chrony openssh-server cifs-utils nginx
nmtui
```





Reboot

Nano /etc/ssh/sshd_config

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

systemctl restart sshd

systemctl enable ssh

nano /etc/chrony/chrony.conf

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

pool ntp.int.demo.wsr iburst
allow 192.168.200.0/24
```

```
# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0
maxdistance 16.0
```

timedatectl set-timezone UTC

systemctl restart chrony

nano /root/.smbclient

```
  GNU nano 5.4
username=Administrator
password=P@sswOrd_
```

mkdir /opt/share

nano /etc/fstab

```
# swap was on /dev/sda5 during installation
UUID=8c31b23a-608a-4166-a849-f7e213ce95c6 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

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

mount –a

apt install -y docker-ce

systemctl enable docker

mkdir /mnt/app

mount /dev/sr1 /mnt/app

docker load < /mnt/app/app.tar

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

docker ps

```
root@web-1:/mnt/app# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED         STATUS         PORTS
                  NAMES
a1bc6e466d2b   app       "/docker-entrypoint.…"   4 seconds ago   Up 3 seconds   0.0.0.0:8080
p, :::8080->80/tcp   app
```

```
cd /opt/share
openssl pkcs12 -nodes -nocerts -in www.pfx -out www.key
openssl pkcs12 -nodes -in www.pfx -out www.crt
cp /opt/share/www.key /etc/nginx/www.key
cp /opt/share/www.cer /etc/nginx/www.crt
nano /etc/nginx/snippets/snakeoil.conf
```

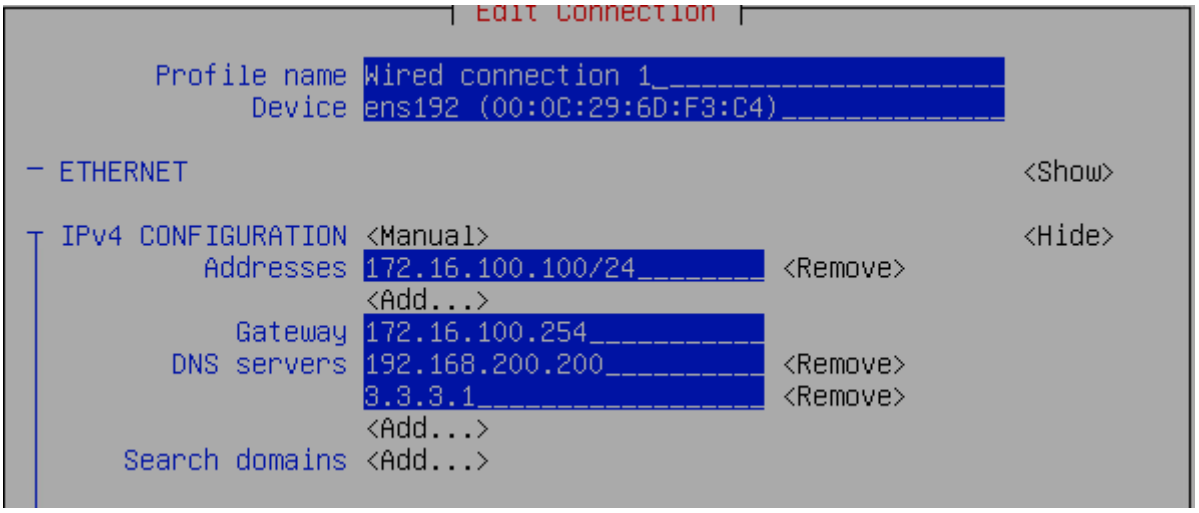
```
  GNU nano 5.4                          /etc/nginx/snippets/snakeoil.conf
# Self signed certificates generated by the ssl-cert package
# Don't use them in a production server!

ssl_certificate /etc/nginx/www.crt;
ssl_certificate_key /etc/nginx/www.key;
```

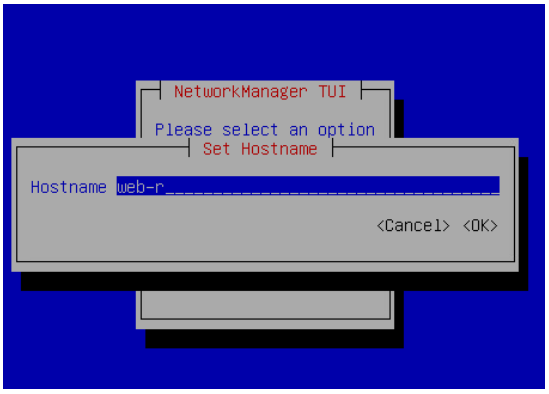
```
rm /etc/nginx/sites-available/default
nano /etc/nginx/sites-available/default
```

```
  GNU nano 5.4                        /etc/nginx/sites-available/default
upstream backend {
        server 192.168.200.100:8080 fail_timeout=25;
        server 172.16.100.100:8080 fail_timeout=25;
}

server {
        listen 443 ssl default_server;
        include snippets/snakeoil.conf;
        server_name www.demo.wsr;
        ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;
        location / {
                proxy_pass http://backend;
        }
}

server {
        listen 80 default_server;
        server_name _;
        return 302 https://www.demo.wsr;
}
```

WEB-R

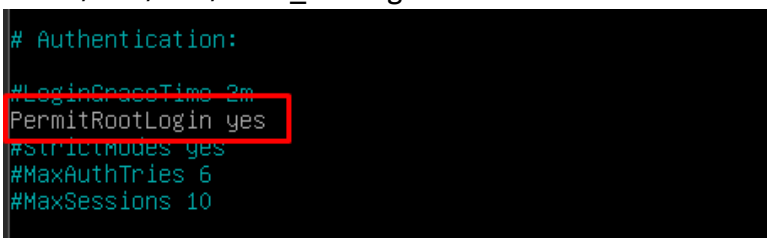
```
apt-cdrom add
apt install -y network-manager mc chrony openssh-server cifs-utils nginx
nmtui
```





Reboot

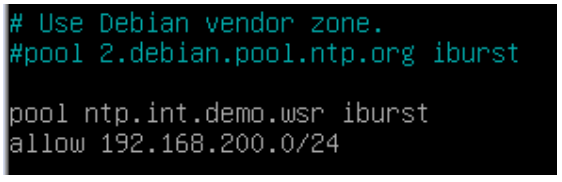
Nano /etc/ssh/sshd_config

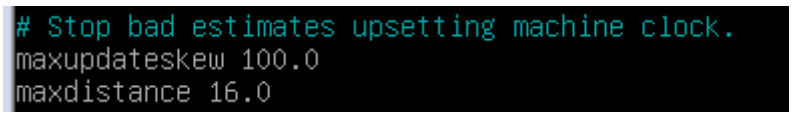


systemctl restart sshd

systemctl enable ssh

nano /etc/chrony/chrony.conf

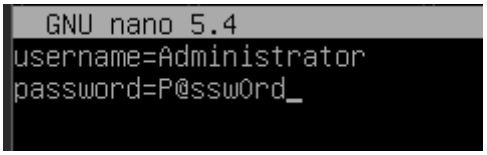




timedatectl set-timezone UTC

systemctl restart chrony

nano /root/.smbclient



mkdir /opt/share

nano /etc/fstab

```
# swap was on /dev/sda5 during installation
UUID=8c31b23a-608a-4166-a849-f7e213ce95c6 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

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

mount –a
apt install -y docker-ce
systemctl enable docker
mkdir /mnt/app
mount /dev/sr1 /mnt/app
docker load < /mnt/app/app.tar
docker run --name app -p 8080:80 -d app
docker ps

```
root@web-1:/mnt/app# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED         STATUS         PORTS
                    NAMES
a1bc6e466d2b   app       "/docker-entrypoint.…"   4 seconds ago   Up 3 seconds   0.0.0.0:8080
p, :::8080->80/tcp   app
```

cd /opt/share
cp /opt/share/www.key /etc/nginx/www.key
cp /opt/share/www.cer /etc/nginx/www.crt
nano /etc/nginx/snippets/snakeoil.conf

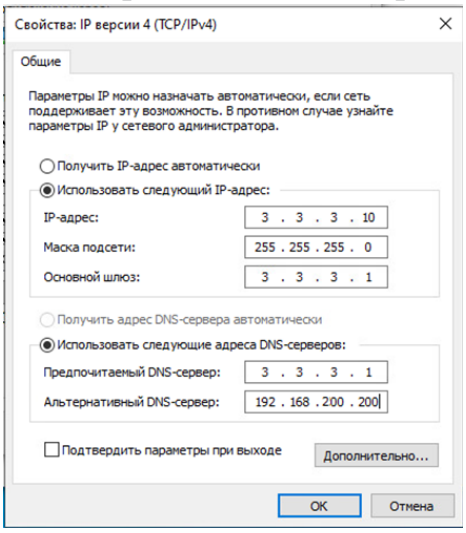
```
  GNU nano 5.4                          /etc/nginx/snippets/snakeoil.conf
# Self signed certificates generated by the ssl-cert package
# Don't use them in a production server!

ssl_certificate /etc/nginx/www.crt;
ssl_certificate_key /etc/nginx/www.key;
```

rm /etc/nginx/sites-available/default
nano /etc/nginx/sites-available/default

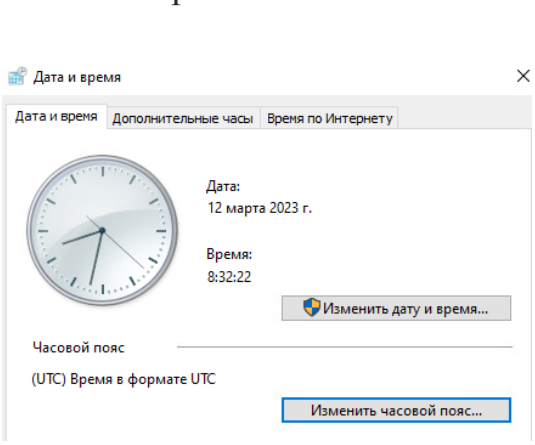
```
  GNU nano 5.4                        /etc/nginx/sites-available/default
upstream backend {
        server 192.168.200.100:8080 fail_timeout=25;
        server 172.16.100.100:8080 fail_timeout=25;
}

server {
        listen 443 ssl default_server;
        include snippets/snakeoil.conf;
        server_name www.demo.wsr;
        ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;
        location / {
                proxy_pass http://backend;
        }
}

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

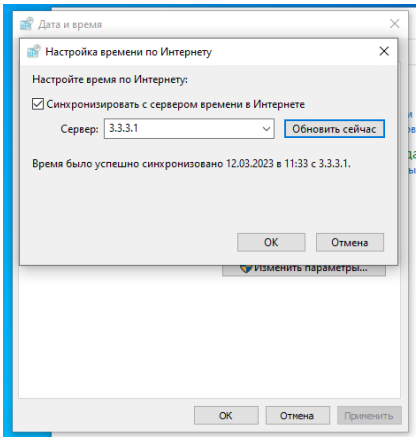
CLI

1. Присваиваем IP-адрес



2. Присваиваем имя
3. Настраиваем NTP



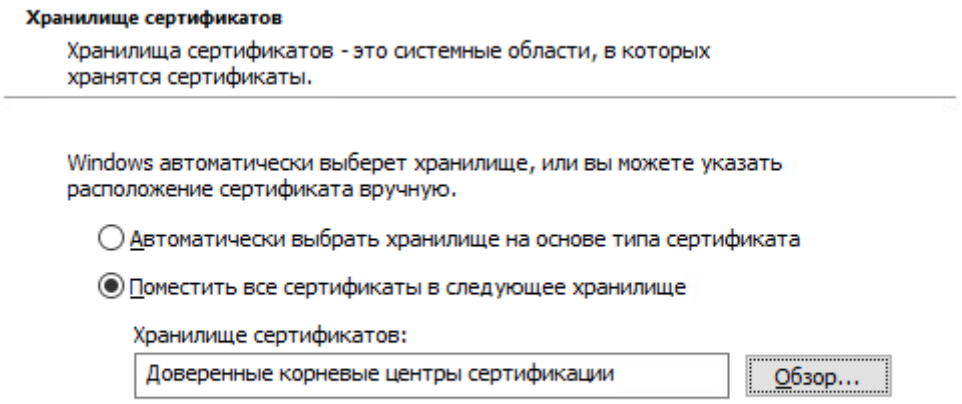


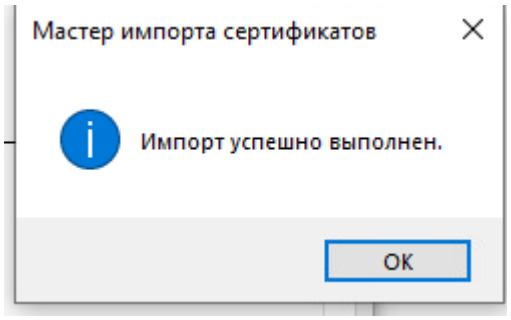
4. Устанавливаем сертификат

4.1. В CMD пишем:

```
Scp -P 2222 root@4.4.4.100:/opt/share/www.pfx C:\Users\User\Desktop
```

4.2. Открываем файл





RTR-L (ACL)

```
access-list 1 permit 192.168.200.0 0.0.0.255
ip nat inside source list 1 interface Gi1 overload
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
int gi 1
ip access-group Lnew in
```

RTR-R (ACL)

```
access-list 1 permit 172.16.100.0 0.0.0.255
ip nat inside source list 1 interface Gi1 overload
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
int gi 1
ip access-group Rnew in
```