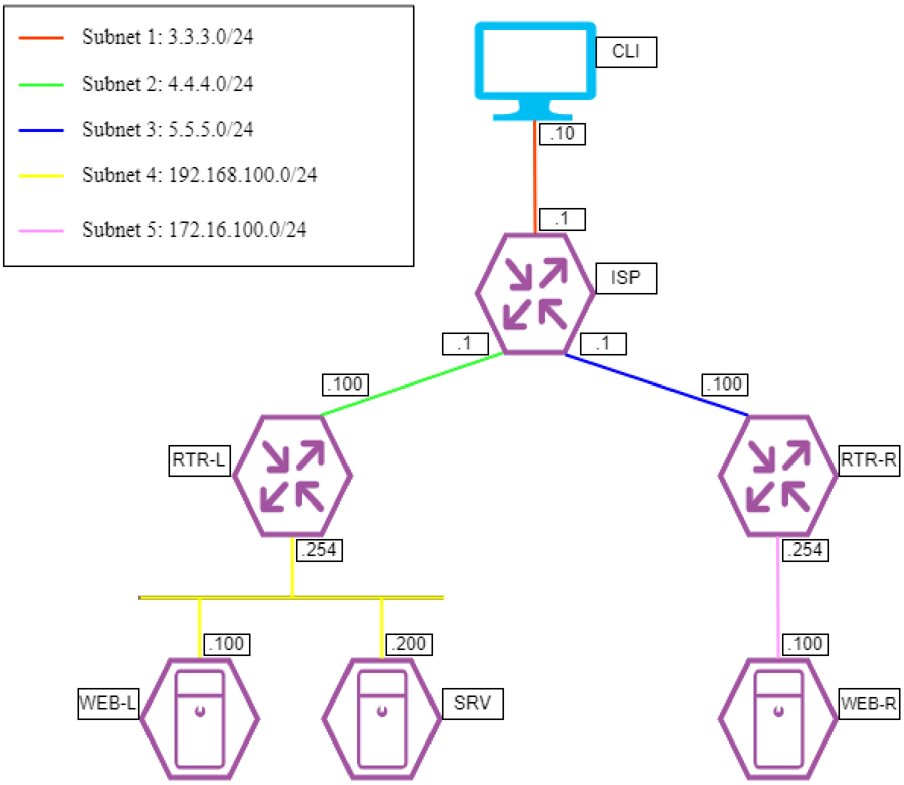
DEMO2022

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	OC	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
```

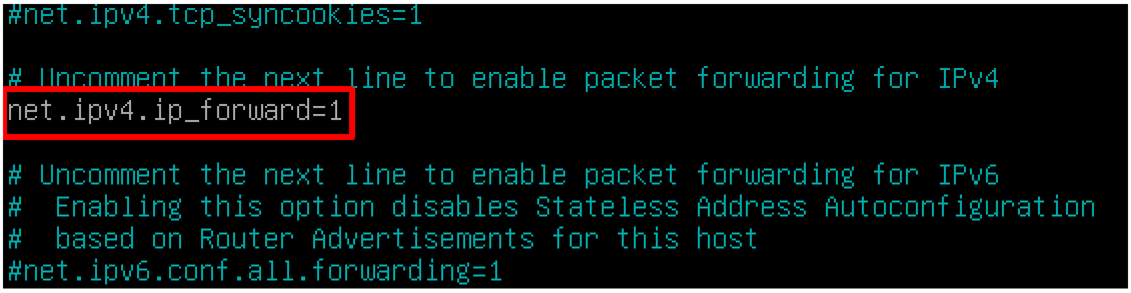
RTL-R (базовая настройка адресации)

```
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
```

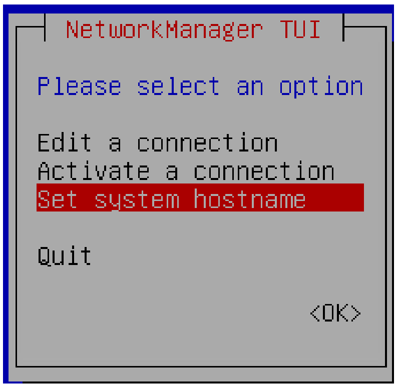


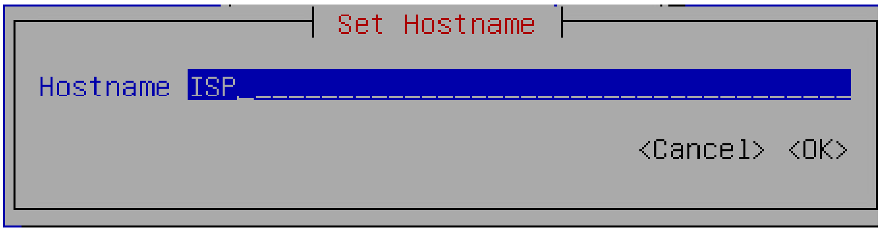
```
#net.ipv4.tcp_syncookies=1

# 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

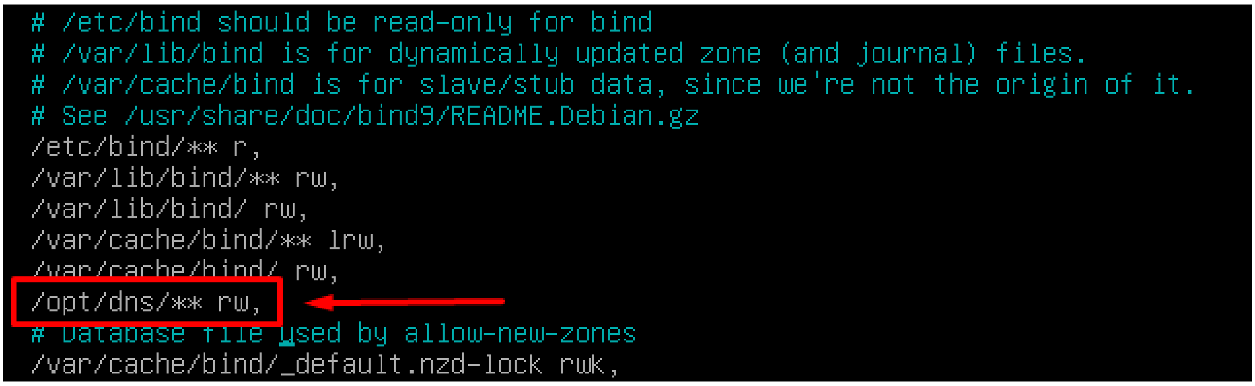
Wired Connection	Adapter	IP&Mask	Default Gateway
Wired Connection 1	Ens192	3.3.3.1/24	Null
Wired Connection 2	Ens224	4.4.4.1/24	4.4.4.100
Wired Connection 3	Ens256	5.5.5.1/24	Null





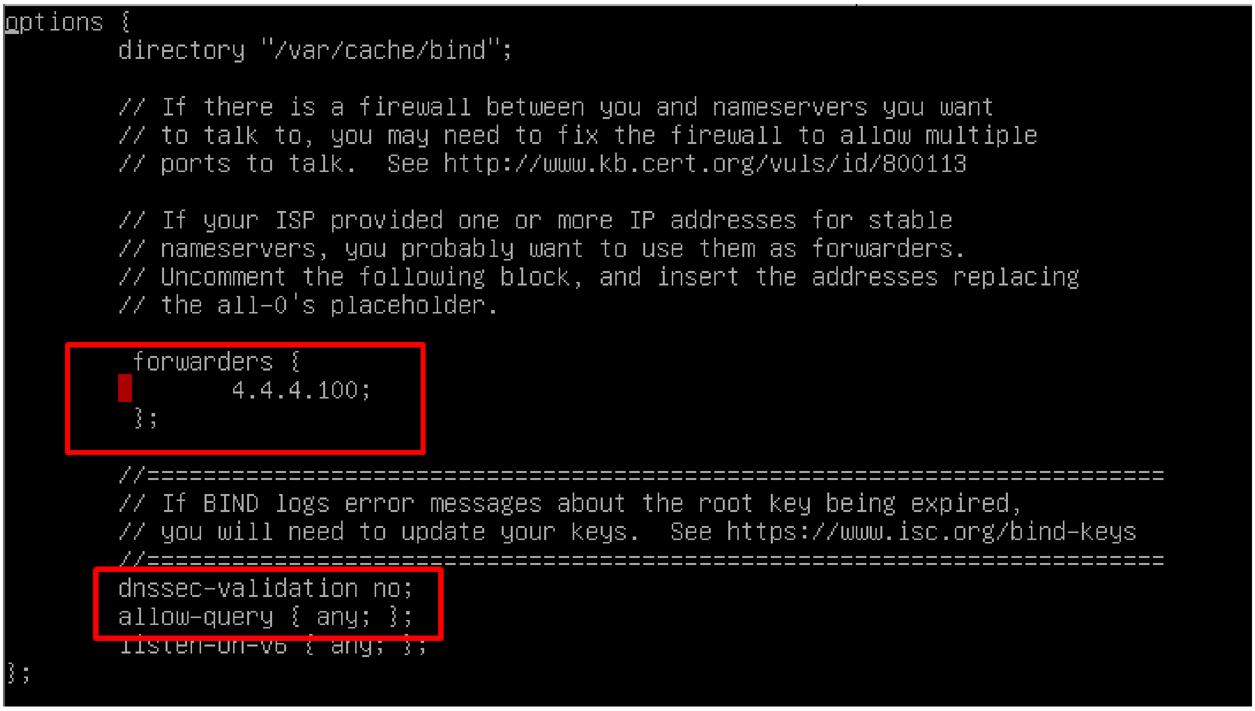
Hostname ISP

```
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
```



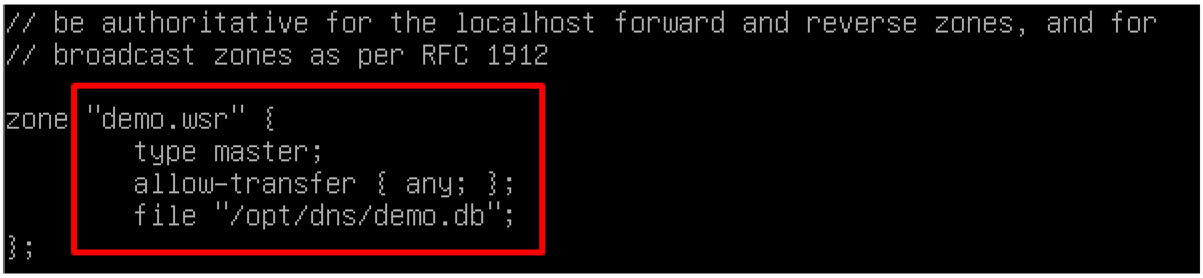
```
# /etc/bind should be read-only for bind
# /var/lib/bind is for dynamically updated zone (and journal) files.
# /var/cache/bind is for slave/stub data, since we're not the origin of it.
# See /usr/share/doc/bind9/README.Debian.gz
/etc/bind/** r,
/var/lib/bind/** rw,
/var/lib/bind/ rw,
/var/cache/bind/** 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
```



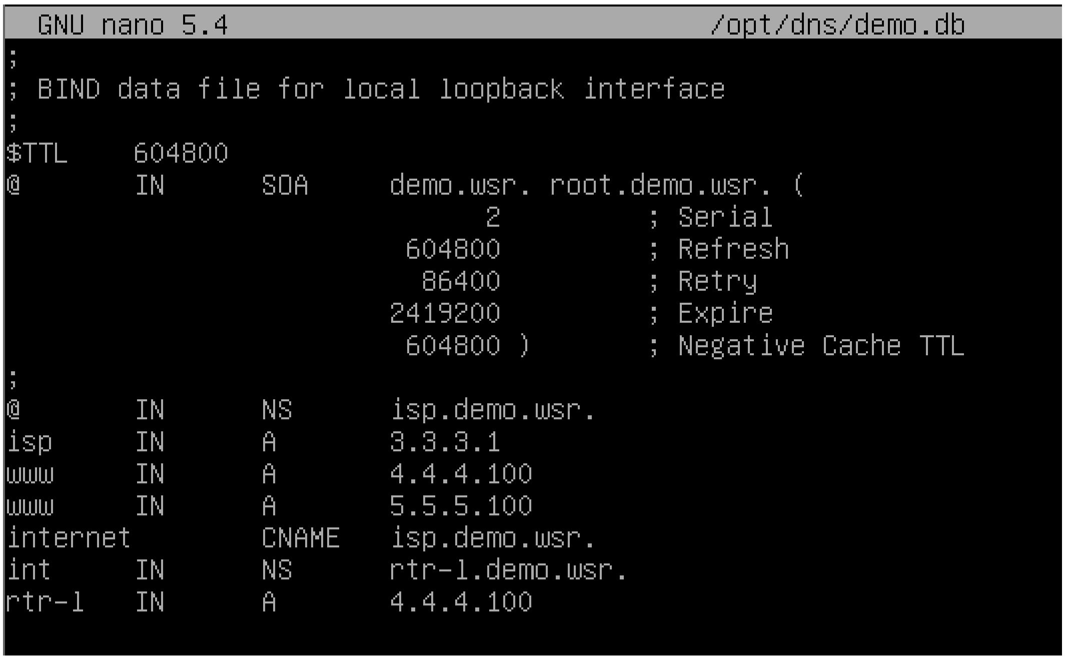
```
options {
        directory "/var/cache/bind";

        // 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
```



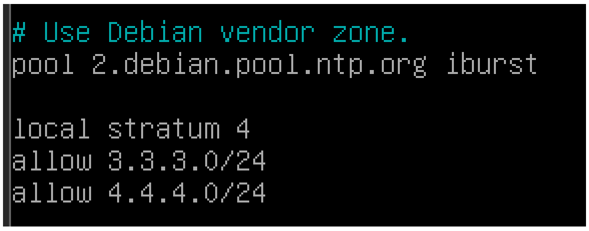
```
// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

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-l.demo.wsr.
rtr-l   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 tcp 192.168.200.200 123 4.4.4.100 123
no ip http secure-server
```

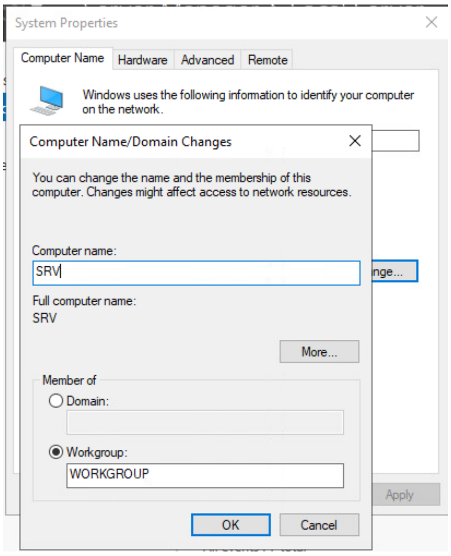
```
wr
reload
ip nat inside source static tcp 192.168.200.100 80 4.4.4.100 80
ip nat inside source static tcp 192.168.200.100 443 4.4.4.100 443
```

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 tcp 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



System Properties

Computer Name | Hardware | Advanced | Remote

Windows uses the following information to identify your computer on the network.

Computer Name/Domain Changes

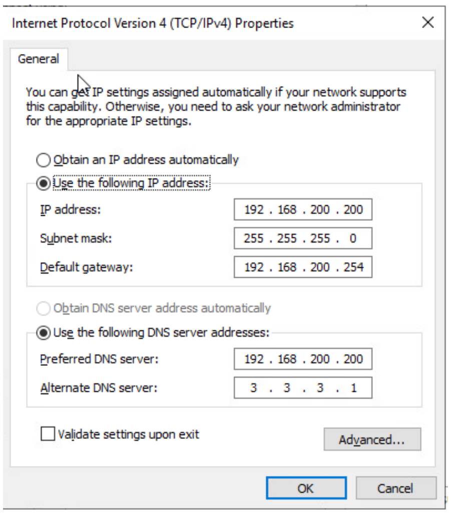
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
SRV

Full computer name:
SRV

Member of
○ Domain:
● Workgroup:
WORKGROUP

2. Устанавливаем IP-адрес.



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:

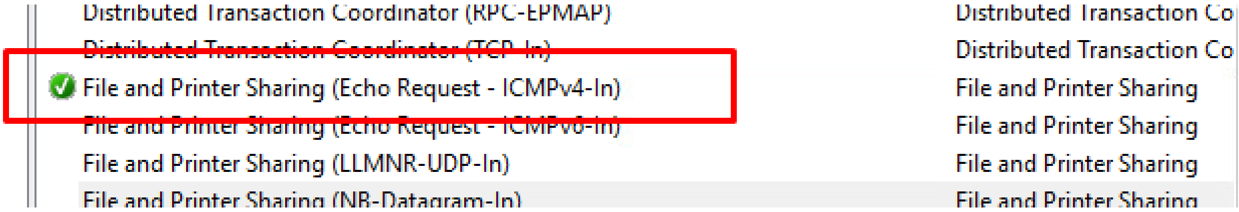
IP address: 192 . 168 . 200 . 200
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 200 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

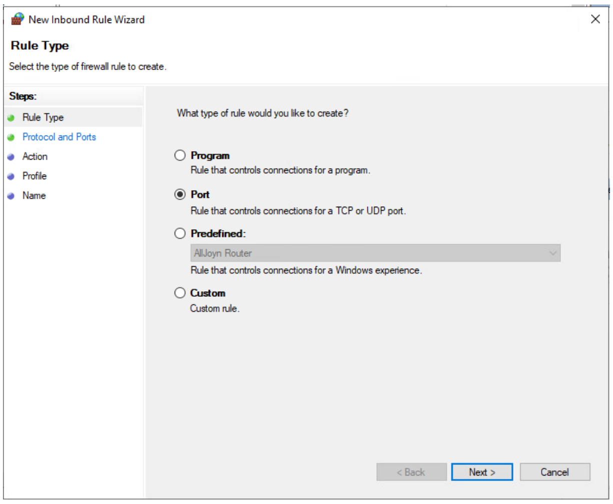
Preferred DNS server: 192 . 168 . 200 . 200
Alternate DNS server: 3 . 3 . 3 . 1

□ Validate settings upon exit

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



Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Co
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Co
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

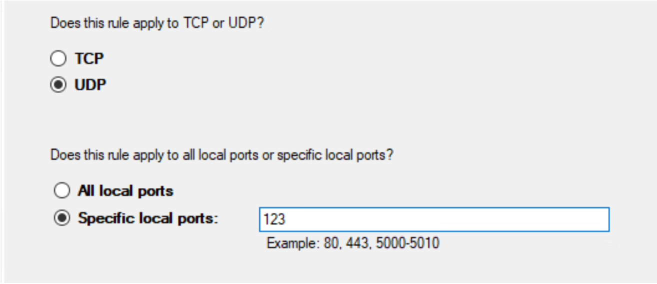
What type of rule would you like to create?

○ **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.

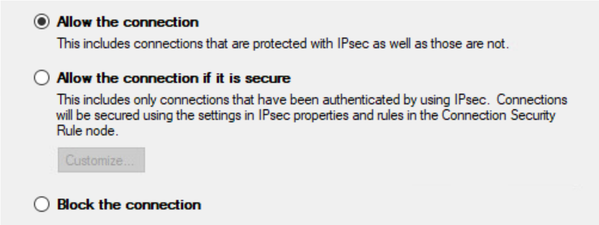


Does this rule apply to TCP or UDP?

○ **TCP**
● **UDP**

Does this rule apply to all local ports or specific local ports?

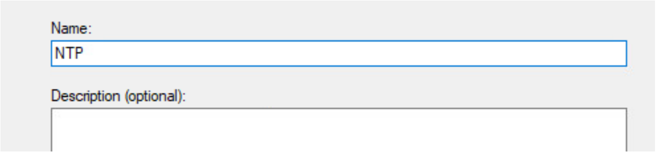
○ **All local ports**
● **Specific local ports:** 123
Example: 80, 443, 5000-5010



● **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.

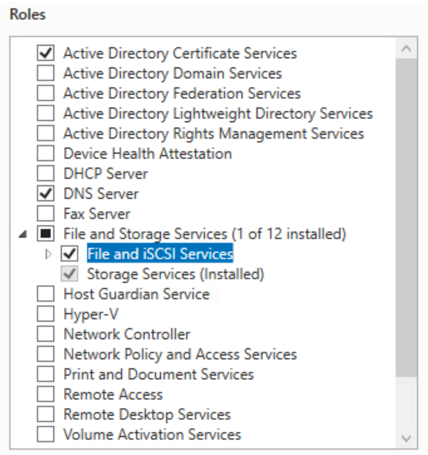
○ **Block the connection**



Name: NTP

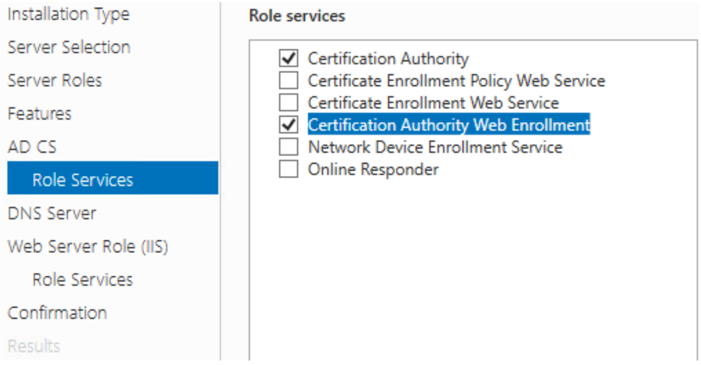
Description (optional):

4. Устанавливаем компоненты



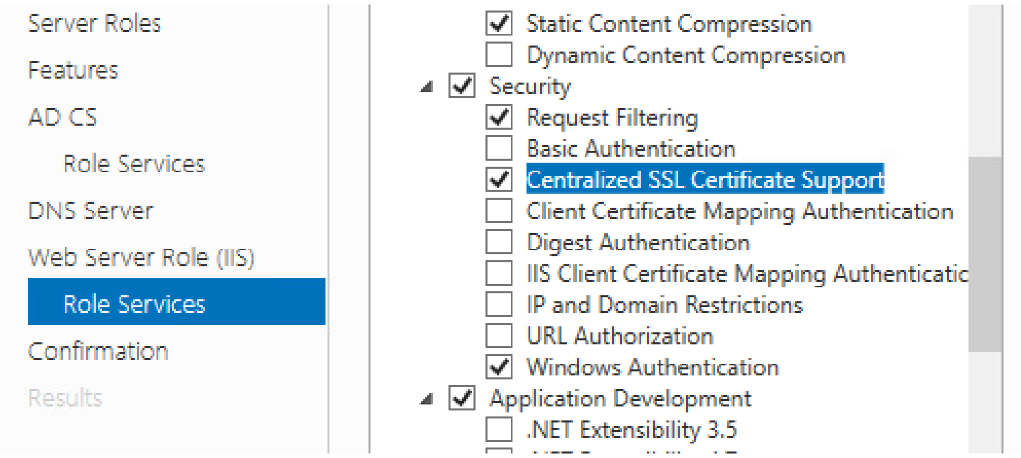
Roles

- ☑ 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
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
  - ☑ File and iSCSI Services
  - ☑ Storage Services (Installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services



Role services

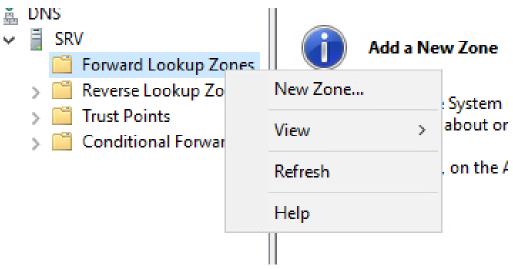
- ☑ Certification Authority
- □ Certificate Enrollment Policy Web Service
- □ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- □ Online Responder

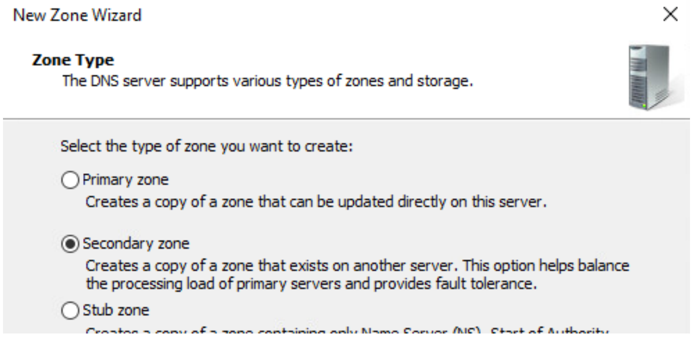


☑ Static Content Compression
□ Dynamic Content Compression
☑ Security
☑ Request Filtering
□ Basic Authentication
☑ Centralized SSL Certificate Support
□ Client Certificate Mapping Authentication
□ Digest Authentication
□ IIS Client Certificate Mapping Authenticatic
□ IP and Domain Restrictions
□ URL Authorization
☑ Windows Authentication
☑ Application Development
□ .NET Extensibility 3.5

5. Настройка DNS

1.1. Создаем вторичную зону





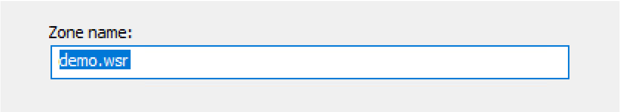
Zone Type
The DNS server supports various types of zones and storage.

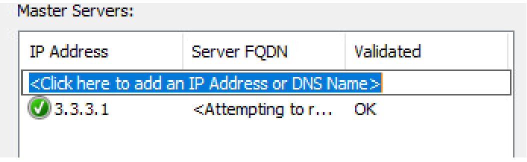
Select the type of zone you want to create:

○ 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.

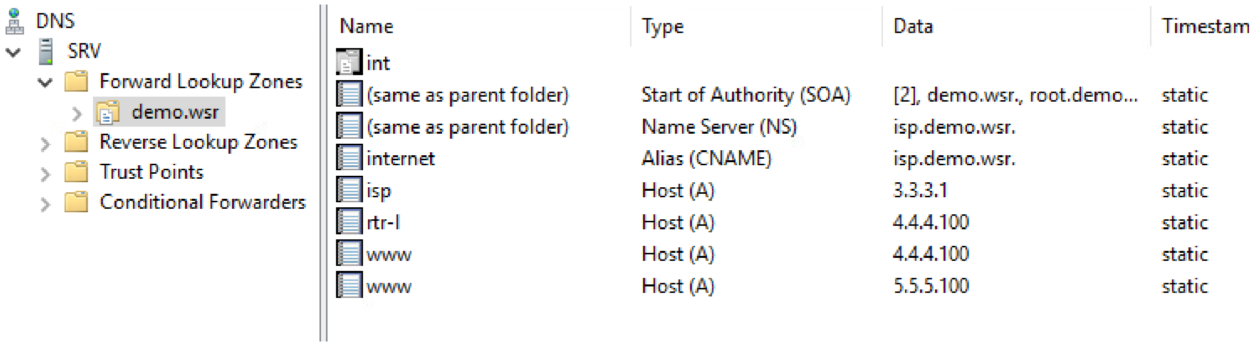
○ Stub zone


Zone name: demo.wsr


Master Servers:

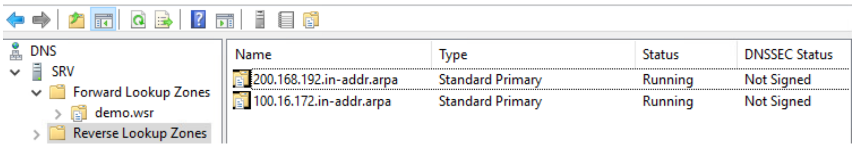
IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
✓ 3.3.3.1	<Attempting to r...	OK

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



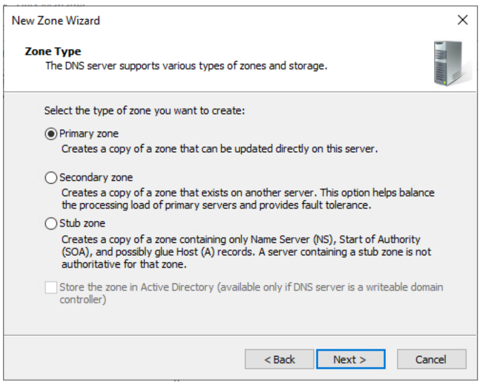
Name	Type	Data	Timestam
int			
(same as parent folder)	Start of Authority (SOA)	[2], demo.wsr., root.demo...	static
(same as parent folder)	Name Server (NS)	isp.demo.wsr.	static
internet	Alias (CNAME)	isp.demo.wsr.	static
isp	Host (A)	3.3.3.1	static
rtr-l	Host (A)	4.4.4.100	static
www	Host (A)	4.4.4.100	static
www	Host (A)	5.5.5.100	static

1.2. Создаем обратную зону



Name	Type	Status	DNSSEC Status
200.168.192.in-addr.arpa	Standard Primary	Running	Not Signed
100.16.172.in-addr.arpa	Standard Primary	Running	Not Signed

1.3. Создаем первичную зону



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

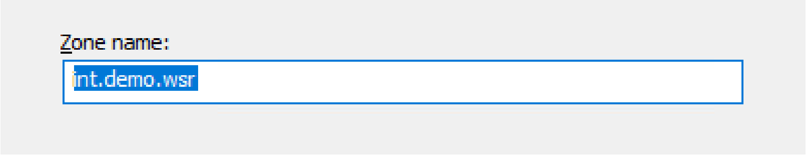
Select the type of zone you want to create:

● Primary zone
Creates a copy of a zone that can be updated directly on this server.

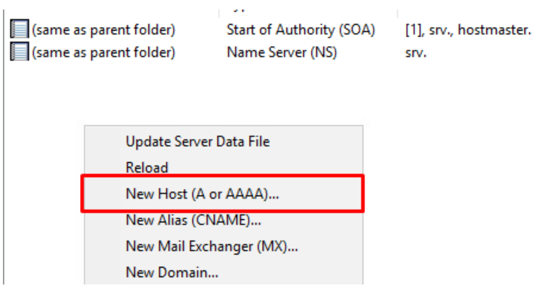
○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ 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.

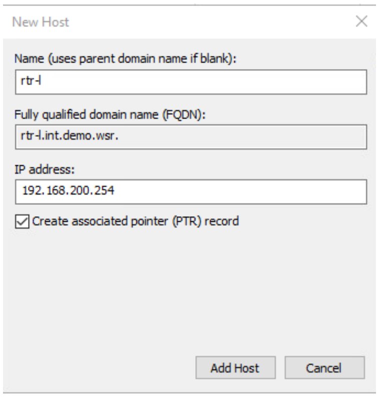
□ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)



Zone name: int.demo.wsr



(same as parent folder)	Start of Authority (SOA)	[1], srv., hostmaster.
(same as parent folder)	Name Server (NS)	srv.



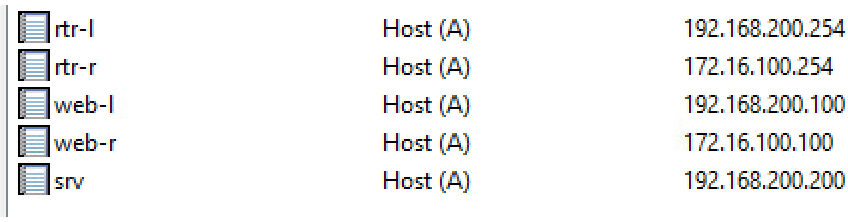
New Host

Name (uses parent domain name if blank): rtr-l

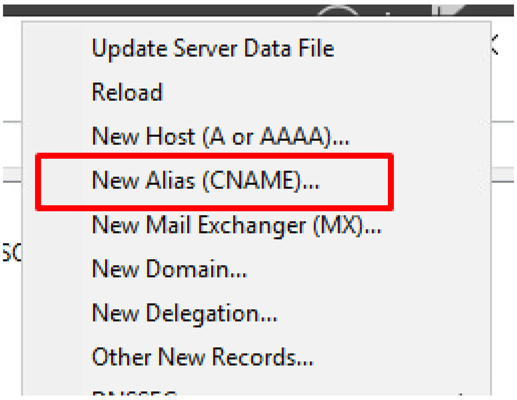
Fully qualified domain name (FQDN): rtr-l.int.demo.wsr.

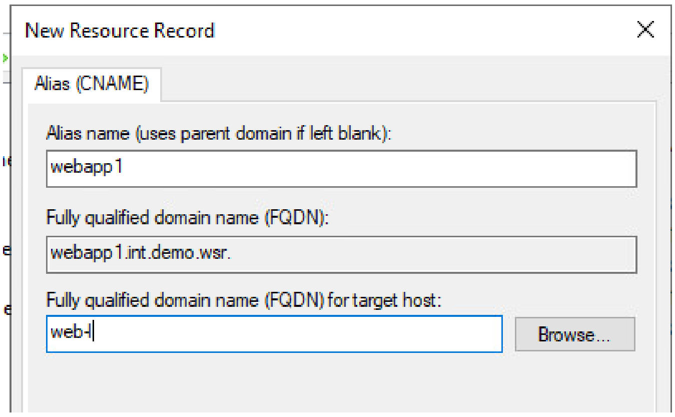
IP address: 192.168.200.254

☑ Create associated pointer (PTR) record



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





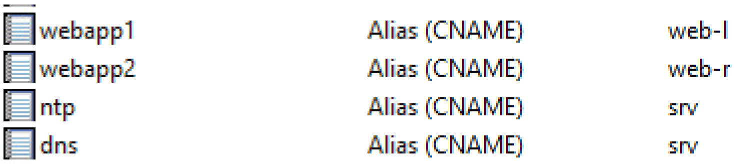
New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank): webapp1

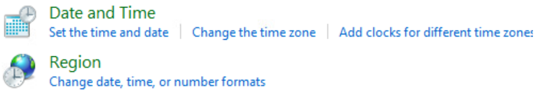
Fully qualified domain name (FQDN): webapp1.int.demo.wsr.

Fully qualified domain name (FQDN) for target host: web-l



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

6. Настройка NTP

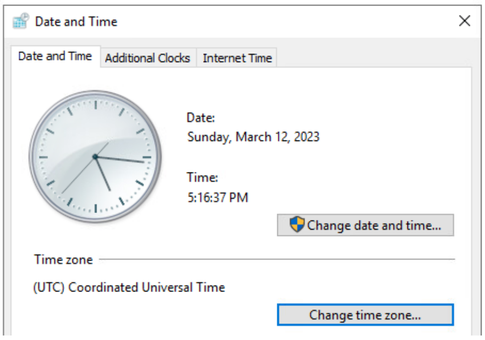


Date and Time

Set the time and date | Change the time zone | Add clocks for different time zones

Region

Change date, time, or number formats

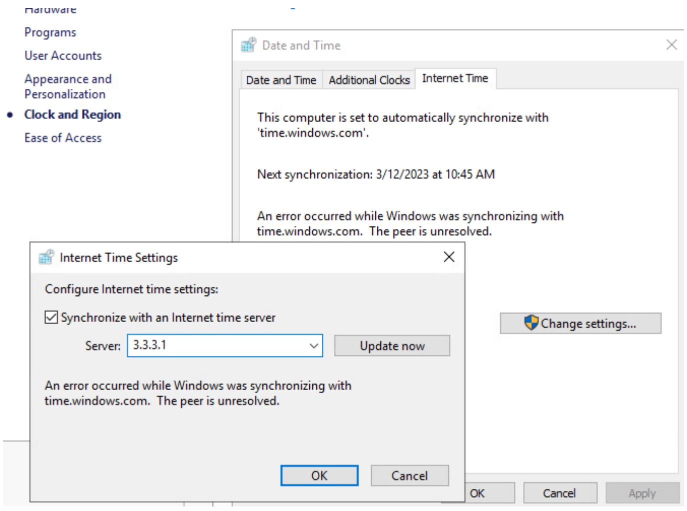


Date:
Sunday, March 12, 2023

Time:
5:16:37 PM

Time zone

(UTC) Coordinated Universal Time



This computer is set to automatically synchronize with 'time.windows.com'.

Next synchronization: 3/12/2023 at 10:45 AM

An error occurred while Windows was synchronizing with time.windows.com. The peer is unresolved.

Configure Internet time settings:

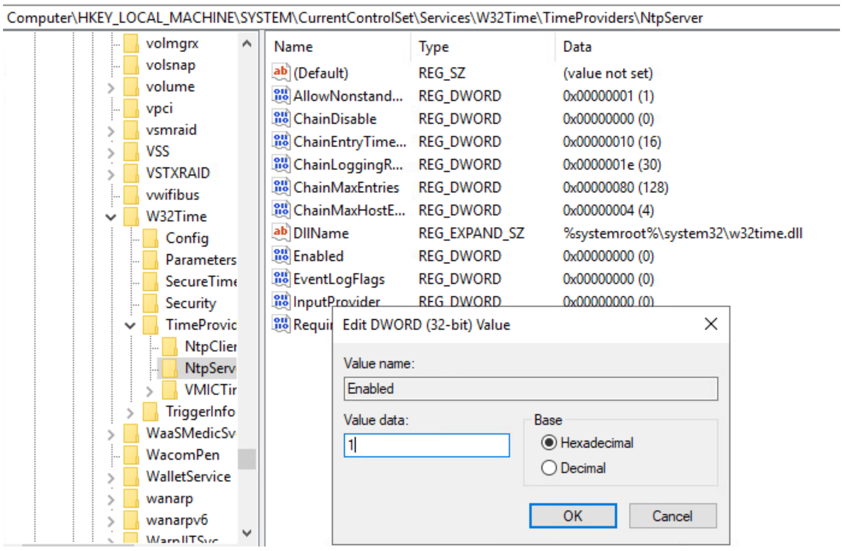
☑ Synchronize with an Internet time server

Server: 3.3.3.1

An error occurred while Windows was synchronizing with time.windows.com. The peer is unresolved.

Заходим в regedit, по пути:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled
```



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer

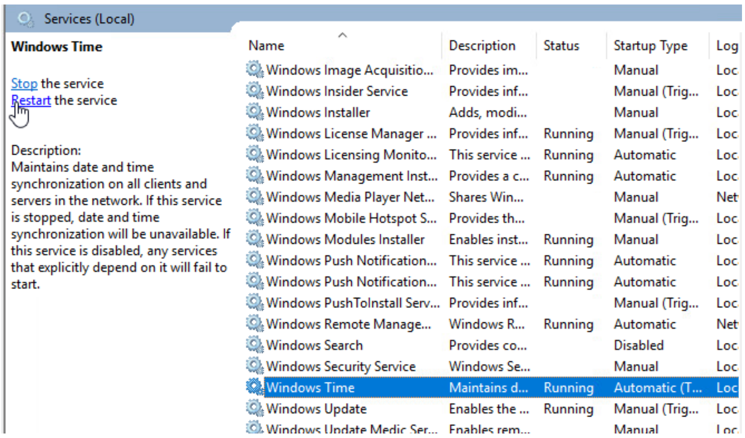
Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowNonstand...	REG_DWORD	0x00000001 (1)
ChainDisable	REG_DWORD	0x00000000 (0)
ChainEntryTime...	REG_DWORD	0x00000010 (16)
ChainLoggingR...	REG_DWORD	0x0000001e (30)
ChainMaxEntries	REG_DWORD	0x00000080 (128)
ChainMaxHostE...	REG_DWORD	0x00000004 (4)
DllName	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
Enabled	REG_DWORD	0x00000000 (0)
EventLogFlags	REG_DWORD	0x00000000 (0)
InputProvider	REG_DWORD	0x00000000 (0)
Requi		

Edit DWORD (32-bit) Value

Value name: Enabled

Value data: 1

Base
● Hexadecimal
○ Decimal



Services (Local)

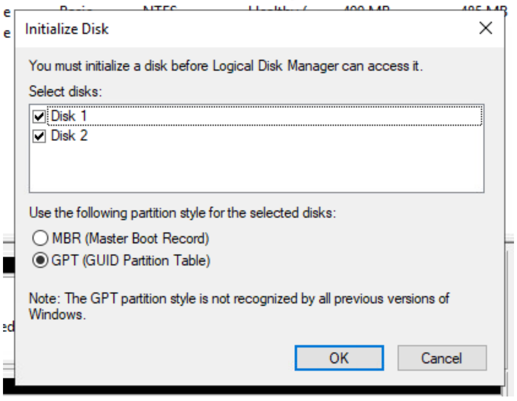
Windows Time

Stop the service
Restart the service

Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log
Windows Image Acquisitio...	Provides im...		Manual	Loc
Windows Insider Service	Provides inf...		Manual (Trig...	Loc
Windows Installer	Adds, modi...		Manual	Loc
Windows License Manager ...	Provides inf...	Running	Manual (Trig...	Loc
Windows Licensing Monito...	This service ...	Running	Automatic	Loc
Windows Management Inst...	Provides a c...	Running	Automatic	Loc
Windows Media Player Net...	Shares Win...		Manual	Net
Windows Mobile Hotspot S...	Provides th...		Manual (Trig...	Loc
Windows Modules Installer	Enables inst...	Running	Manual	Loc
Windows Push Notification...	This service ...	Running	Automatic	Loc
Windows Push Notification...	This service ...	Running	Automatic	Loc
Windows PushToInstall Serv...	Provides inf...		Manual (Trig...	Loc
Windows Remote Manage...	Windows R...	Running	Automatic	Net
Windows Search	Provides co...		Disabled	Loc
Windows Security Service	Windows Se...		Manual	Loc
Windows Time	Maintains d...	Running	Automatic (T...	Loc
Windows Update	Enables the ...	Running	Manual (Trig...	Loc
Windows Update Medic Ser...	Enables rem...		Manual	Loc

7. Создание RAID-массива



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

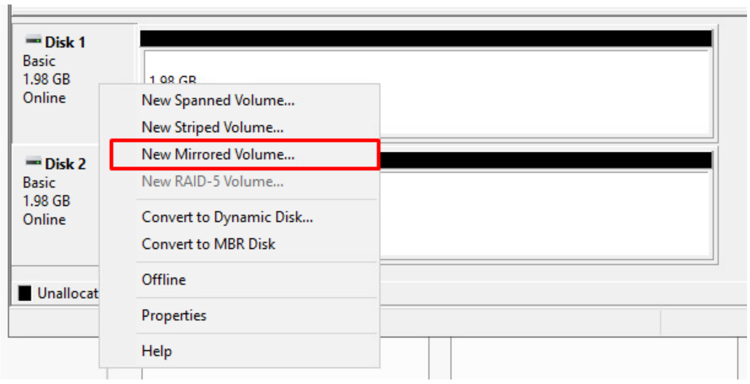
Select disks:

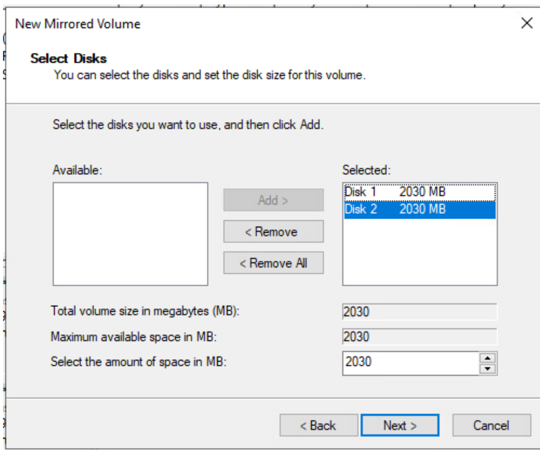
☑ Disk 1
☑ Disk 2

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.





New Mirrored Volume

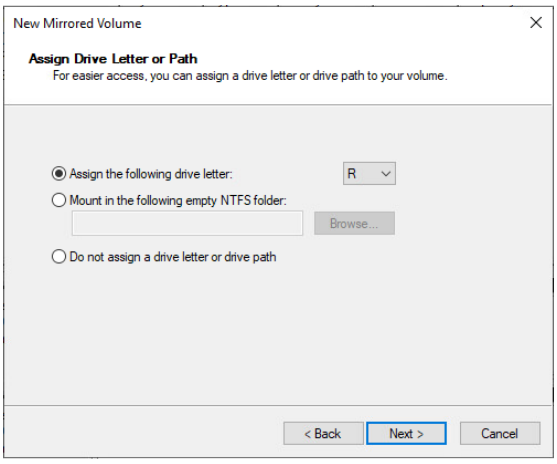
Select Disks
You can select the disks and set the disk size for this volume.

Select the disks you want to use, and then click Add.

Available:

Selected:
Disk 1 2030 MB
Disk 2 2030 MB

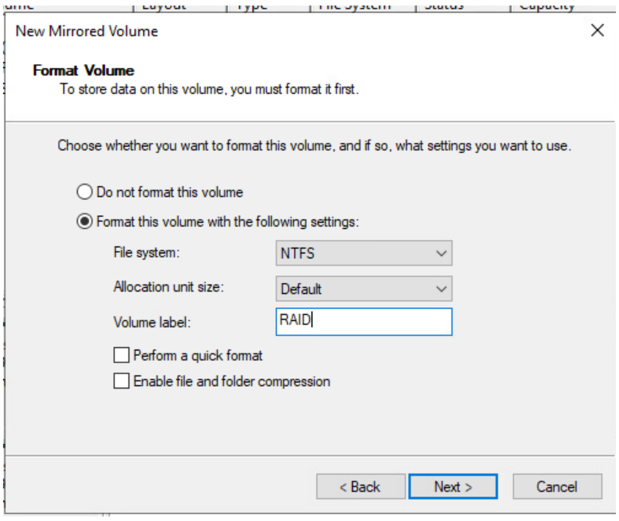
Total volume size in megabytes (MB): 2030
Maximum available space in MB: 2030
Select the amount of space in MB: 2030



New Mirrored Volume

Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your volume.

● Assign the following drive letter: R
○ Mount in the following empty NTFS folder:
○ Do not assign a drive letter or drive path



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

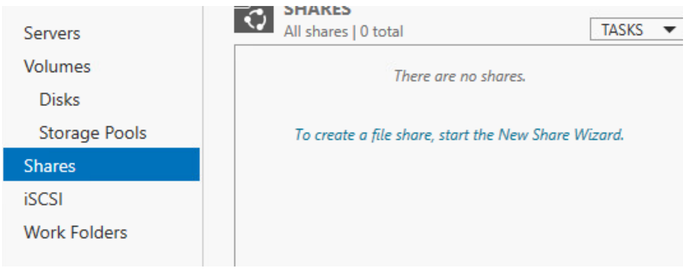
Allocation unit size: Default

Volume label: RAID

□ Perform a quick format

□ Enable file and folder compression

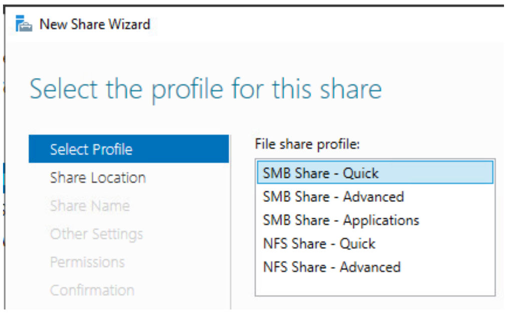
8. Настройка SMB



All shares | 0 total

There are no shares.

To create a file share, start the New Share Wizard.

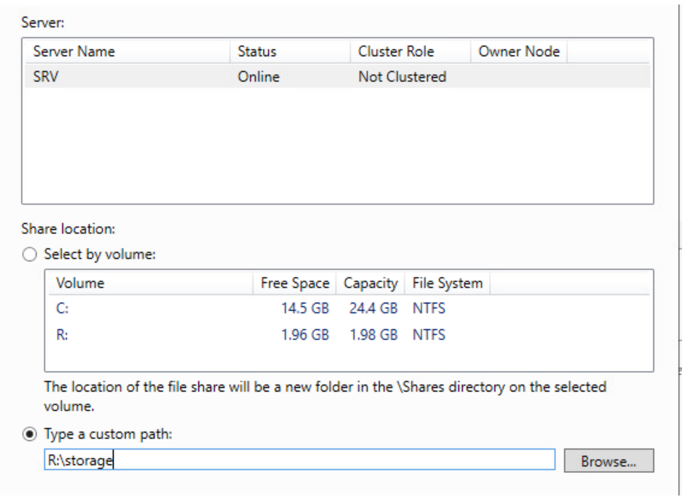


New Share Wizard

Select the profile for this share

File share profile:

SMB Share - Quick
SMB Share - Advanced
SMB Share - Applications
NFS Share - Quick
NFS Share - Advanced



Server:

Server Name	Status	Cluster Role	Owner Node
SRV	Online	Not Clustered	

Share location:

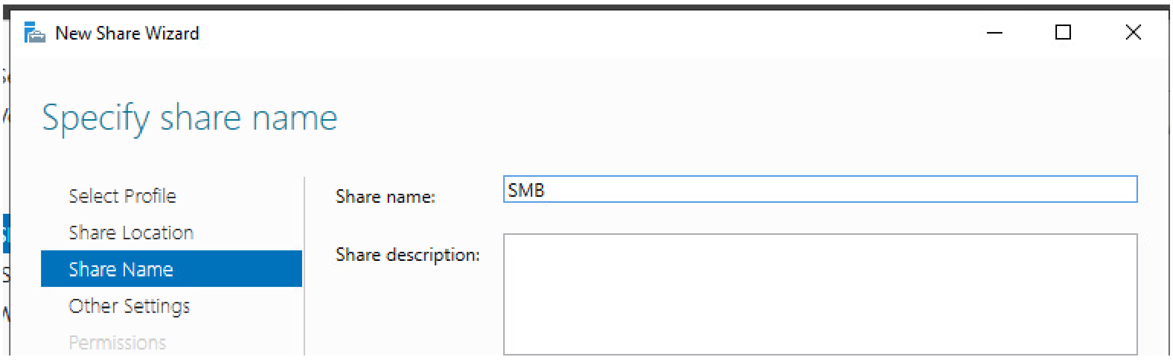
○ Select by volume:

Volume	Free Space	Capacity	File System
C:	14.5 GB	24.4 GB	NTFS
R:	1.96 GB	1.98 GB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

● Type a custom path:

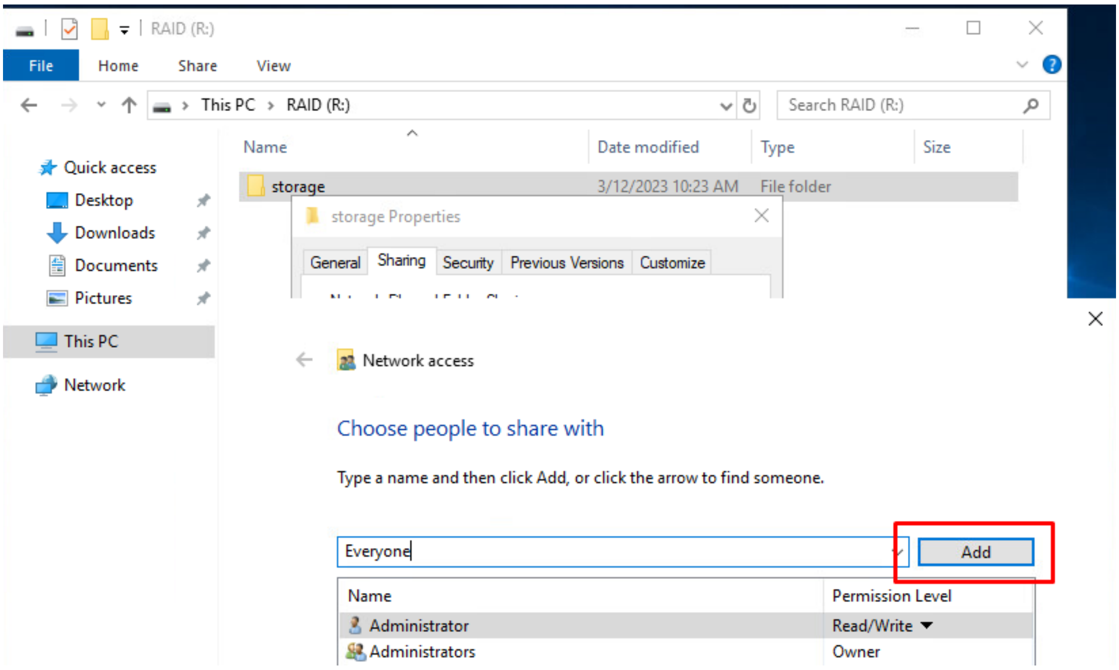
R:\storage



Specify share name

Share name: SMB

Share description:



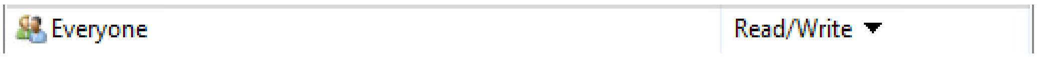
Name	Date modified	Type	Size
storage	3/12/2023 10:23 AM	File folder	

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

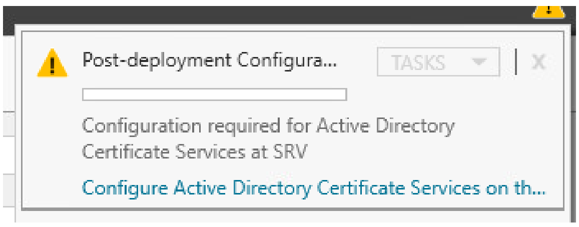
Everyone

Name	Permission Level
Administrator	Read/Write
Administrators	Owner



Everyone	Read/Write

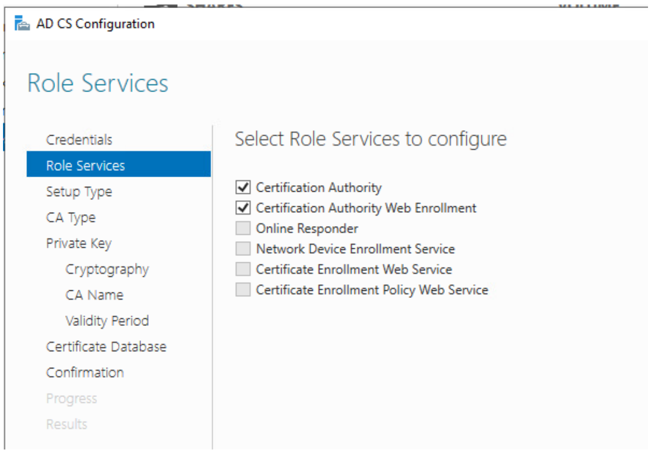
9. Создание сертификатов



Post-deployment Configura...

Configuration required for Active Directory Certificate Services at SRV

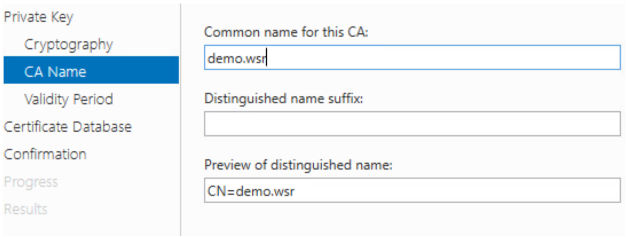
Configure Active Directory Certificate Services on th...



Role Services

Select Role Services to configure

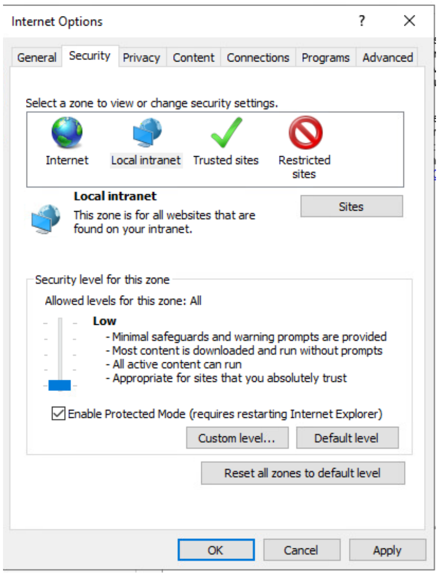
☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service



Common name for this CA: demo.wsr

Distinguished name suffix:

Preview of distinguished name: CN=demo.wsr



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

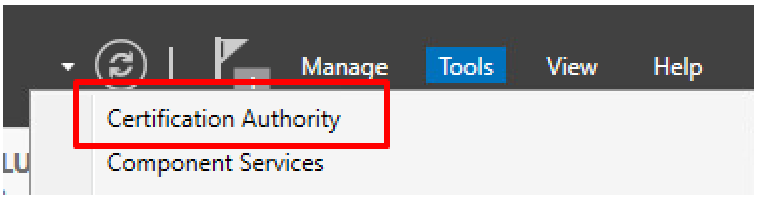
Security level for this zone

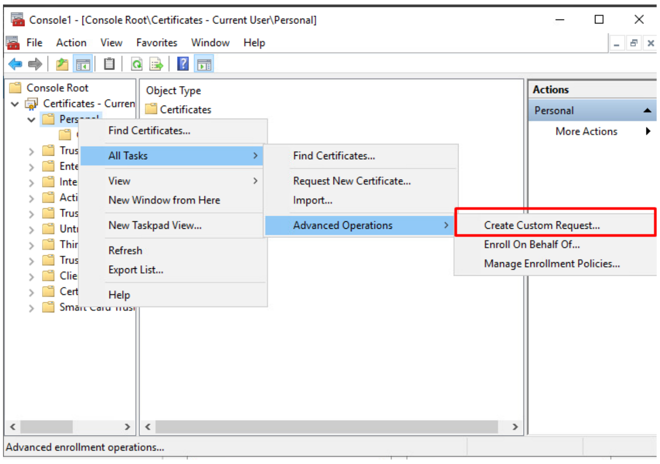
Allowed levels for this zone: All

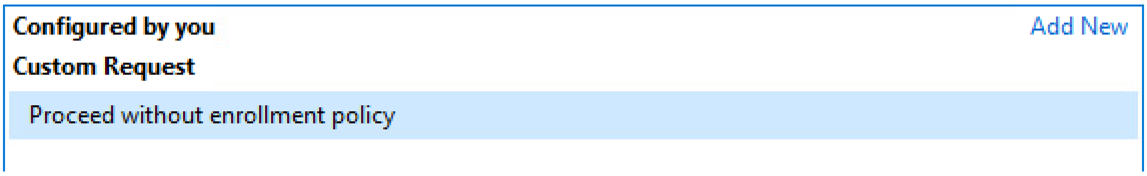
Low

- 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)



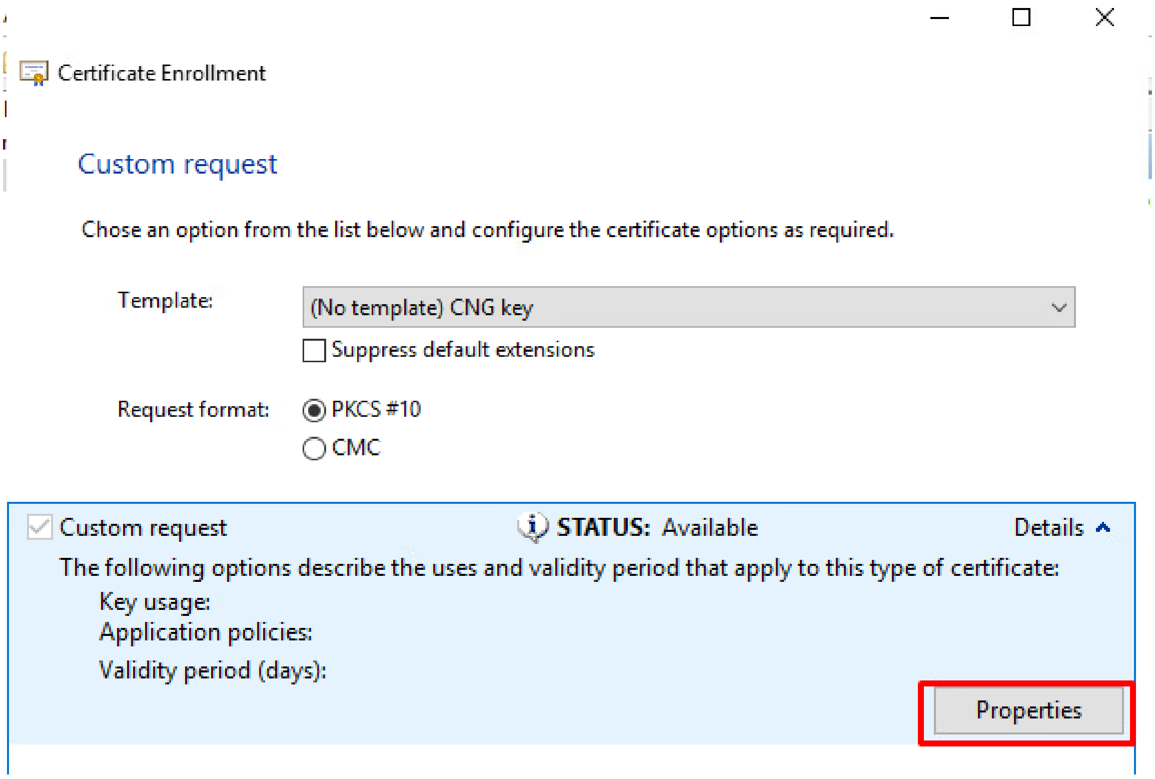




Configured by you

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

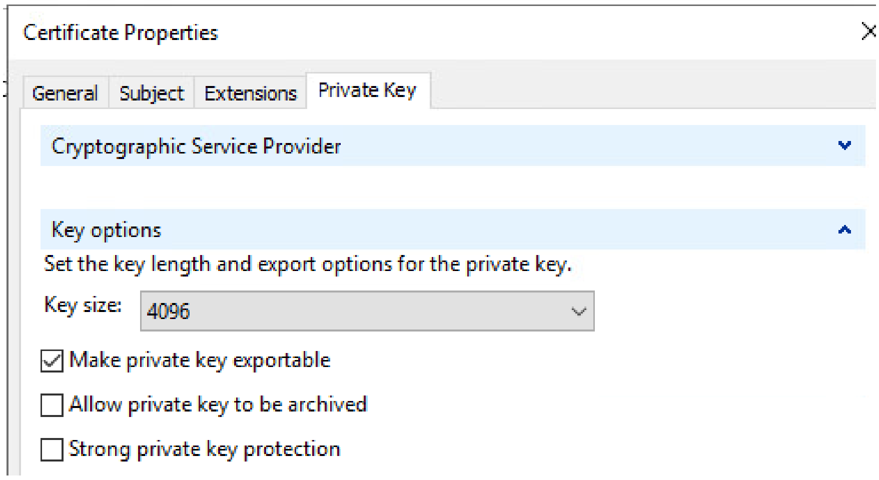
☑ Custom request — STATUS: Available — Details

The following options describe the uses and validity period that apply to this type of certificate:

Key usage:

Application policies:

Validity period (days):



Certificate Properties

Cryptographic Service Provider

Key options

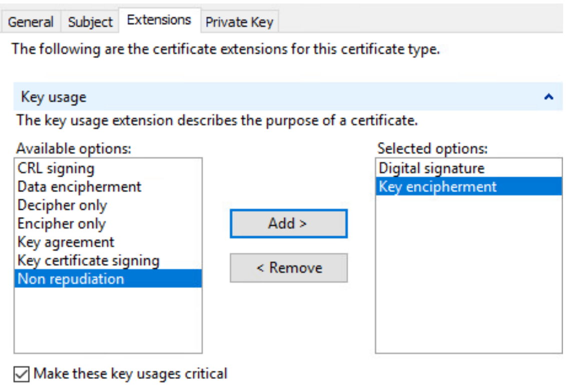
Set the key length and export options for the private key.

Key size: 4096

☑ Make private key exportable

□ Allow private key to be archived

□ Strong private key protection



The following are the certificate extensions for this certificate type.

Key usage

The key usage extension describes the purpose of a certificate.

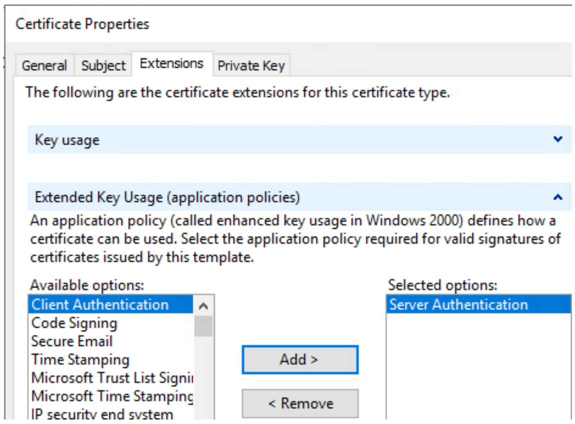
Available options:

CRL signing
Data encipherment
Decipher only
Encipher only
Key agreement
Key certificate signing
Non repudiation

Selected options:

Digital signature
Key encipherment

☑ Make these key usages critical



Certificate Properties

The following are the certificate extensions for this certificate type.

Key usage

Extended Key Usage (application policies)

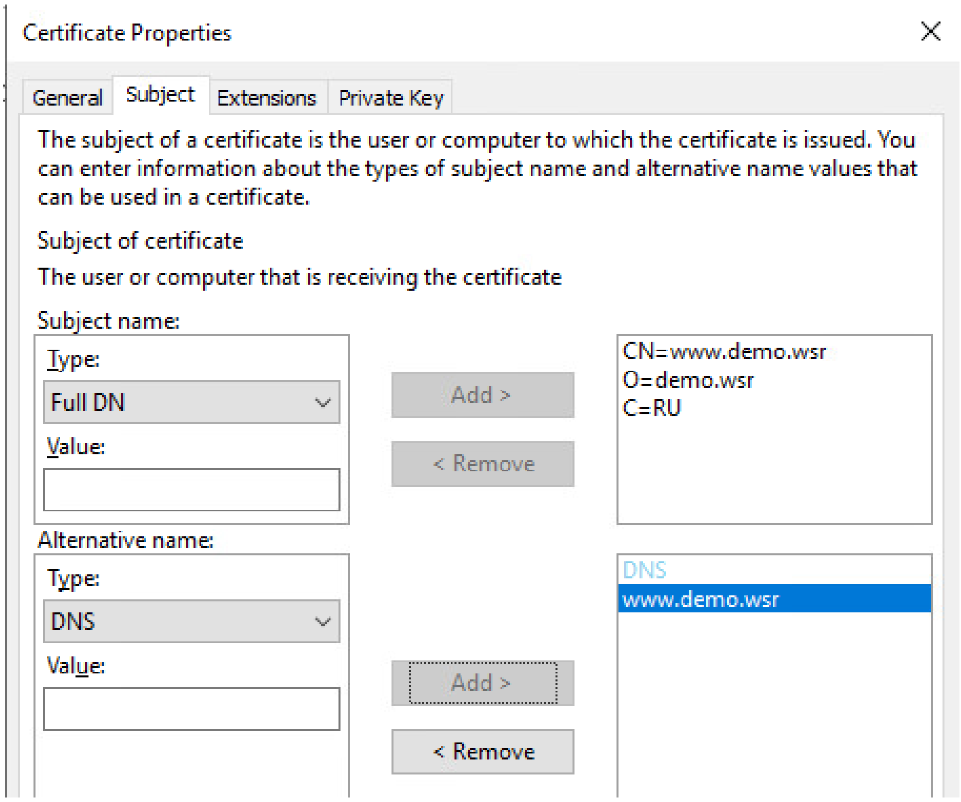
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Available options:

Client Authentication
Code Signing
Secure Email
Time Stamping
Microsoft Trust List Signi
Microsoft Time Stamping
IP security end system

Selected options:

Server Authentication



Certificate Properties

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:

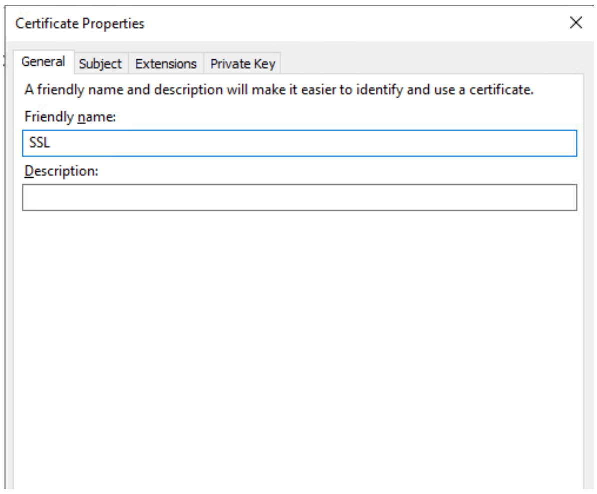
CN=www.demo.wsr
O=demo.wsr
C=RU

Alternative name:

Type: DNS

Value:

DNS
www.demo.wsr

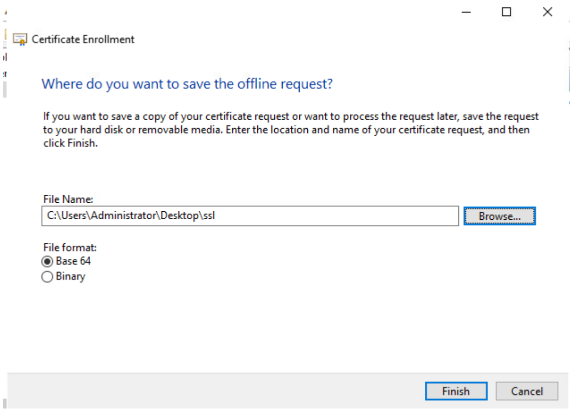


Certificate Properties

A friendly name and description will make it easier to identify and use a certificate.

Friendly name: SSL

Description:



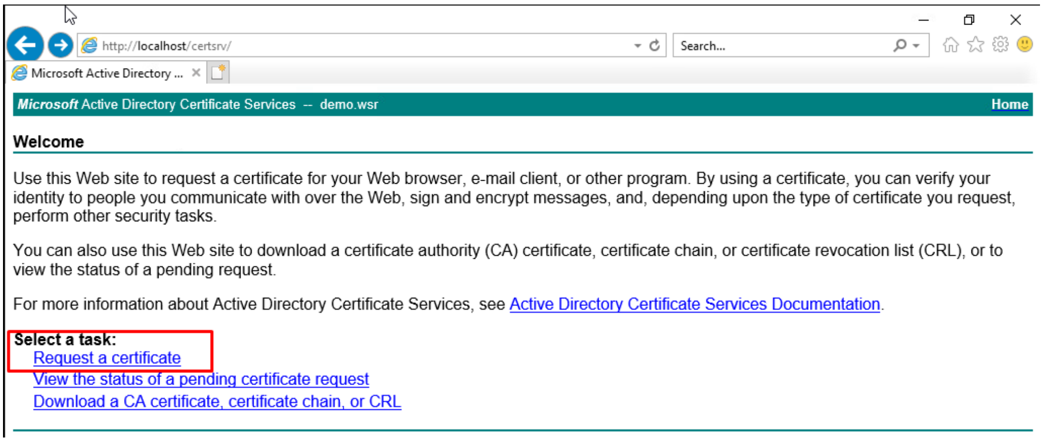
Certificate Enrollment

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

File format:
● Base 64
○ Binary



Microsoft Active Directory Certificate Services -- demo.wsr

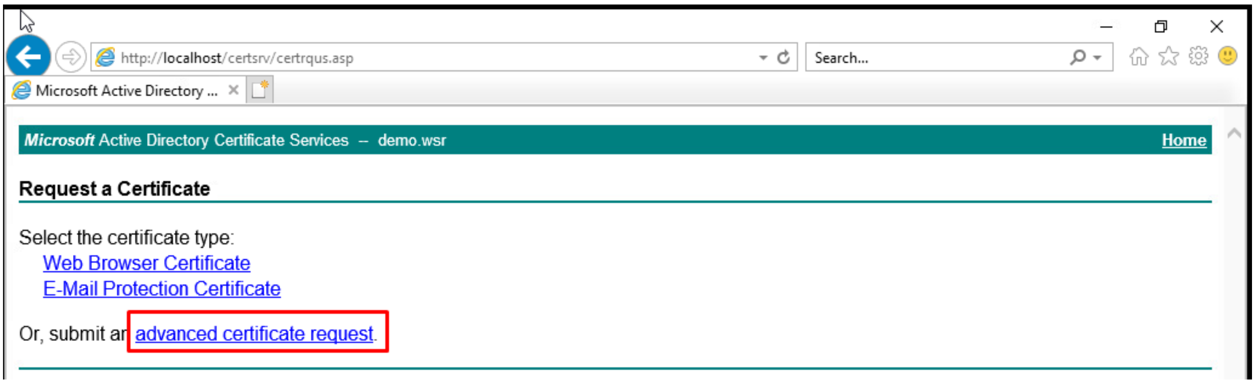
Welcome

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



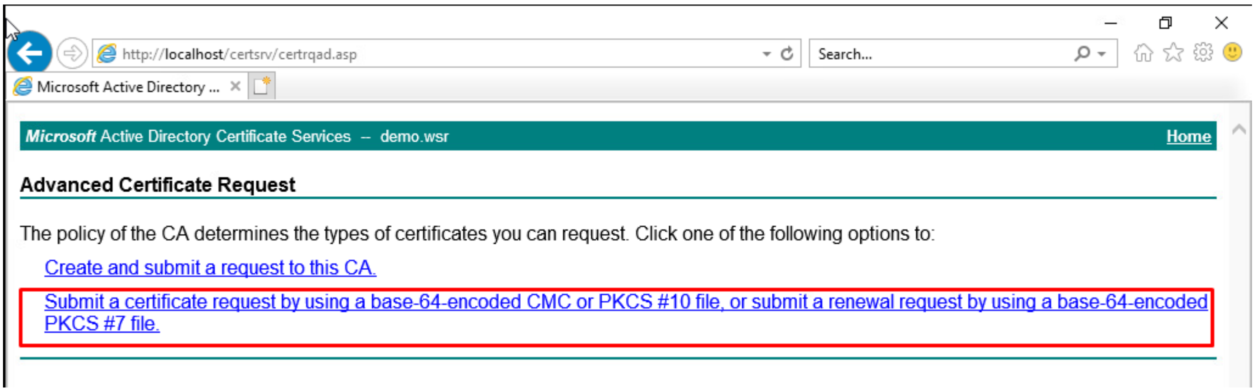
http://localhost/certsrv/certrqus.asp
Search...
Microsoft Active Directory ...

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 ...

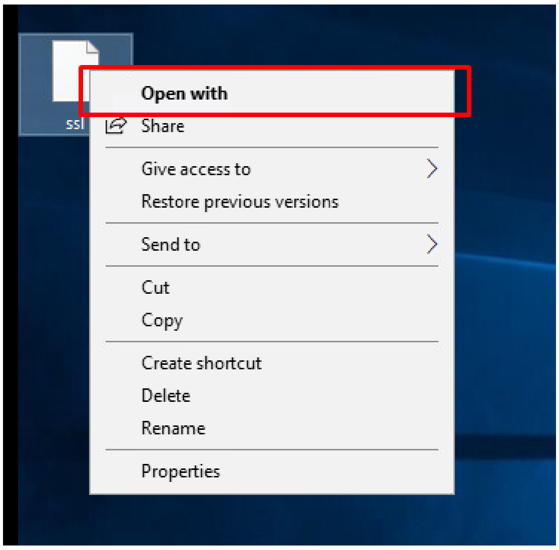
Microsoft Active Directory Certificate Services -- demo.wsr Home

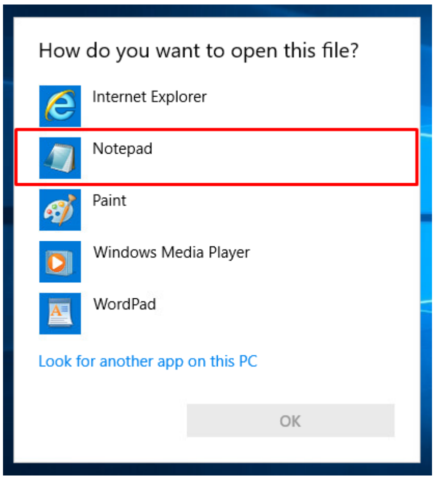
Advanced Certificate Request

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

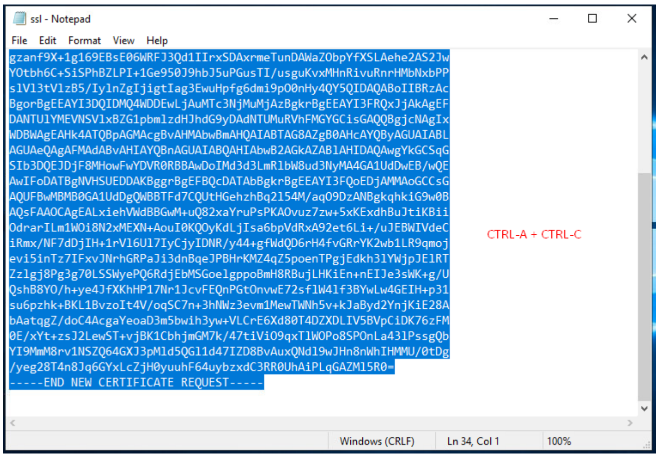
Create and submit a request to this CA.

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.



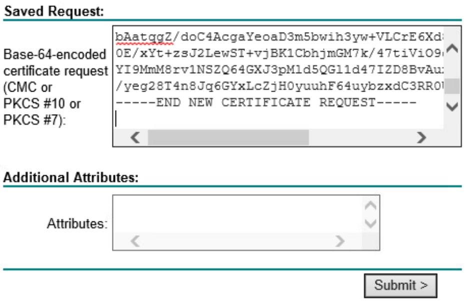


How do you want to open this file?



```
gzanf9X+1g169EBsE06WRFJ3Qd1IIrxSDAxrmeTunDAWaZObpYfXSLAehe2AS2Jw
YOtbh6C+SiSPhBZLPI+1Ge950J9hbJ5uPGusTI/usguKvxMHnRivuRnrHMbNxbPP
slVl3tVlzB5/IylnZgIjigtIag3EwuHpfg6dmi9pO0nHy4QY5QIDAQABoIIBRzAc
BgorBgEEAYI3DQIDMQ4WDDEwLjAuMTc3NjMuMjAzBgkrBgEEAYI3FRQxJjAkAgEF
DANTU1YMEVNSVlxBZG1pbmlzdHJhdG9yDAdNTUMuRVhFMGYGCisGAQQBgjcNAgIx
WDBWAgEAHk4ATQBpAGMAcgBvAHMAbwBmAHQAIABTAG8AZgB0AHcAYQByAGUAIABL
AGUAeQAgAFMAdABvAHIAYQBnAGUAIABQAHIAbwB2AGkAZABlAHIDAQAwgYkGCSqG
SIb3DQEJDjF8MHowFwYDVR0RBBAwDoIMd3d3LmRlbW8ud3NyMA4GA1UdDwEB/wQE
AwIFoDATBgNVHSUEDDAKBggrBgEFBQcDATAbBgkrBgEEAYI3FQoEDjAMMAoGCCsG
AQUFBwMBMB0GA1UdDgQWBBTFd7CQUtHGehzhBq2l54M/aqO9DzANBgkqhkiG9w0B
AQsFAAOCAgEALxiehVWdBBGwM+uQ82xaYruPsPKAOvuz7zw+5xKExdhBuJtiKBii
OdrarILm1WOi8N2xMEXN+AouI0KQOyKdLjIsa6bpVdRxA92et6Li+/uJEBWIVdeC
iRmx/NF7dDjIH+1rVl6Ul7IyCjyIDNR/y44+gfWdQD6rH4fvGRrYK2wb1LR9qmoj
evi5inTz7IFxvJNrhGRPaJi3dnBqeJPBHrKMZ4qZ5poenTPgjEdkh3lYWjpJElRT
Zzlgj8Pg3g70LSSWyePQ6RdjEbMSGoelgppoBmH8RBujLHKiEn+nEIJe3sWK+g/U
QshB8YO/h+ye4JfXKhHP17Nr1JcvFEQnPGtOnvwE72sflW4lf3BYwLw4GEIH+p31
su6pzhk+BKL1BvzoIt4V/oqSC7n+3hNWz3evm1MewTWNh5v+kJaByd2YnjKiE28A
bAatqgZ/doC4AcgaYeoaD3m5bwih3yw+VLCrE6Xd80T4DZXDLIV5BVpCiDK76zFM
0E/xYt+zsJ2LewST+vjBK1CbhjmGM7k/47tiViO9qxTlWOPo8SPOnLa43lPssgQb
YI9MmM8rv1NSZQ64GXJ3pMld5QGl1d47IZD8BvAuxQNdl9wJHn8nWhIHMMU/0tDg
/yeg28T4n8Jq6GYxLcZjH0yuuhF64uybzxdC3RR0UhAiPLqGAZMl5R0=
-----END NEW CERTIFICATE REQUEST-----
```

CTRL-A + CTRL-C



Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

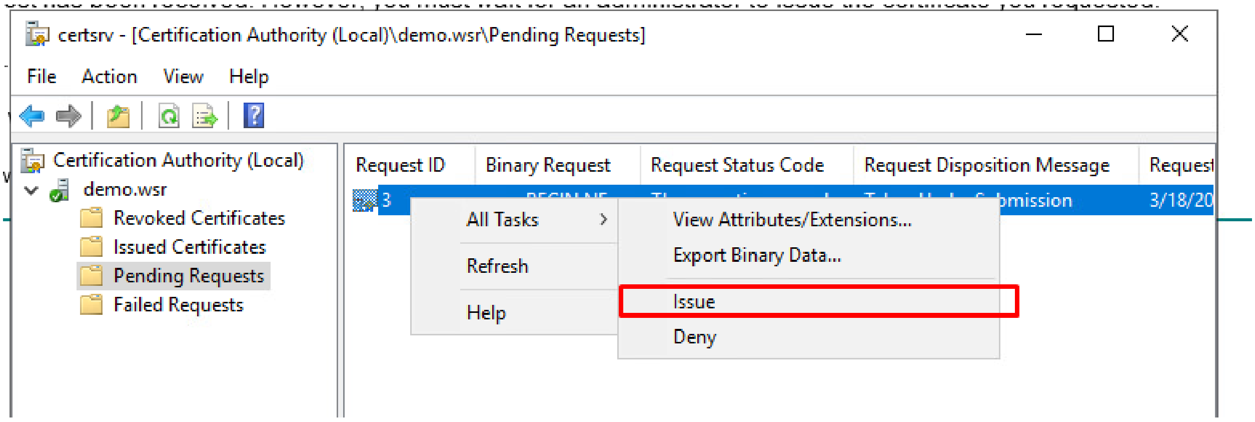
```
bAatqgZ/doC4AcgaYeoaD3m5bwih3yw+VLCrE6Xd
0E/xYt+zsJ2LewST+vjBK1CbhjmGM7k/47tiViO9
YI9MmM8rv1NSZQ64GXJ3pMld5QGl1d47IZD8BvAu
/yeg28T4n8Jq6GYxLcZjH0yuuhF64uybzxdC3RR0
-----END NEW CERTIFICATE REQUEST-----
```

Additional Attributes:

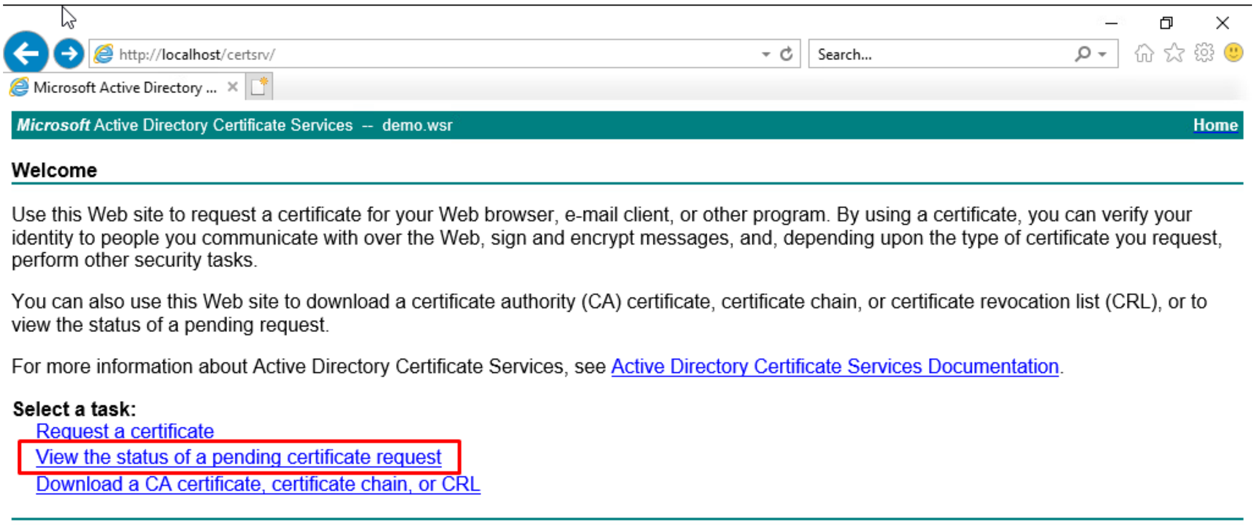
Attributes:

Submit >

...est has been received. However, you must wait for an administrator to issue the certificate you requested.



certsrv - [Certification Authority (Local)\demo.wsr\Pending Requests]



Microsoft Active Directory Certificate Services -- demo.wsr **Home**

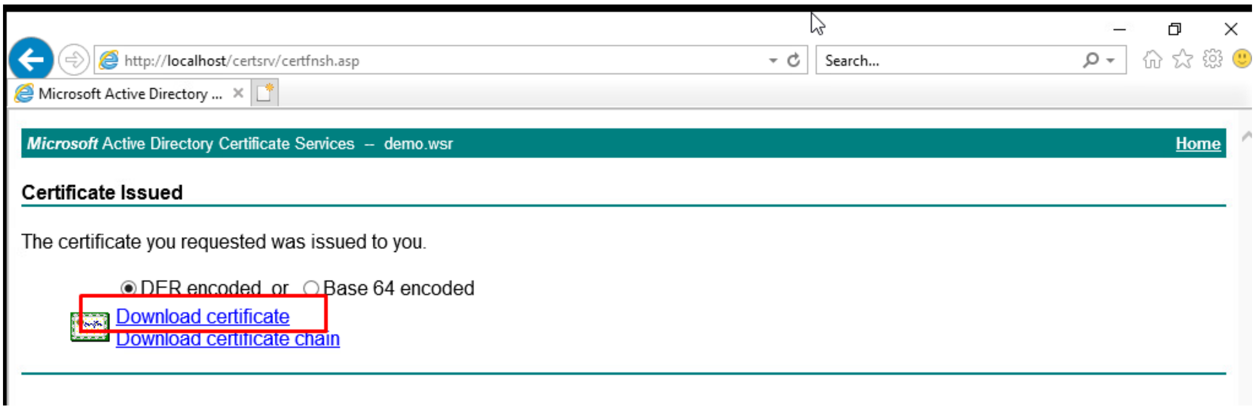
Welcome

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



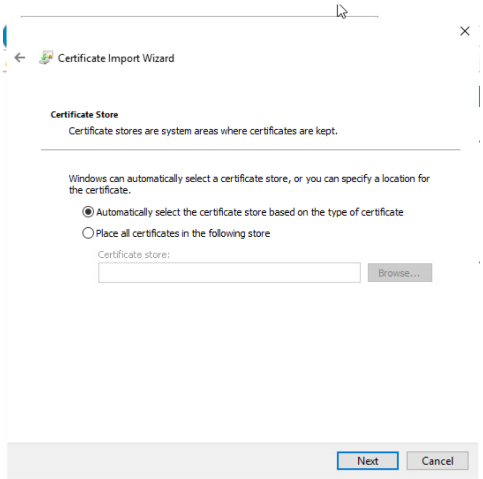
http://localhost/certsrv/certfnsh.asp
Search...
Microsoft Active Directory ...

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

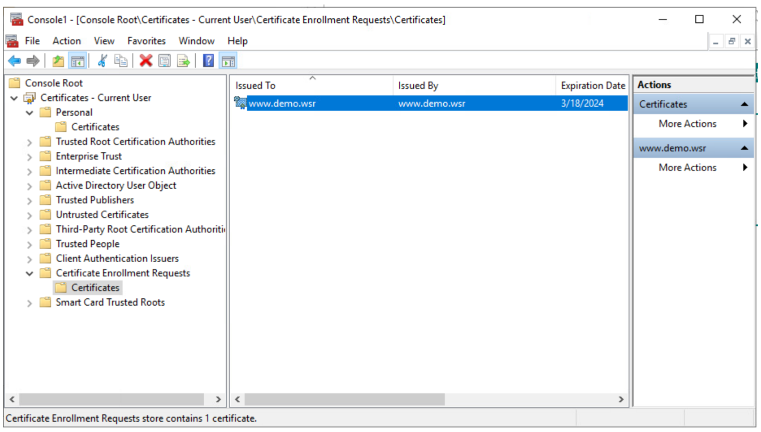


Certificate Import Wizard

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:

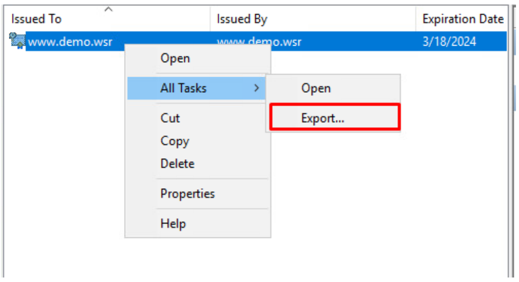


Console1 - [Console Root\Certificates - Current User\Certificate Enrollment Requests\Certificates]

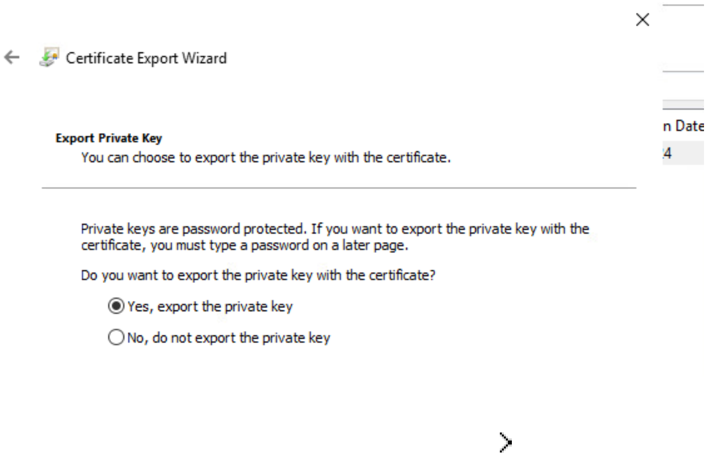
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Certificates
Smart Card Trusted Roots
Actions
Certificates
More Actions
www.demo.wsr
More Actions

Issued To	Issued By	Expiration Date
www.demo.wsr	www.demo.wsr	3/18/2024

Certificate Enrollment Requests store contains 1 certificate.



Issued To	Issued By	Expiration Date
www.demo.wsr	www.demo.wsr	3/18/2024



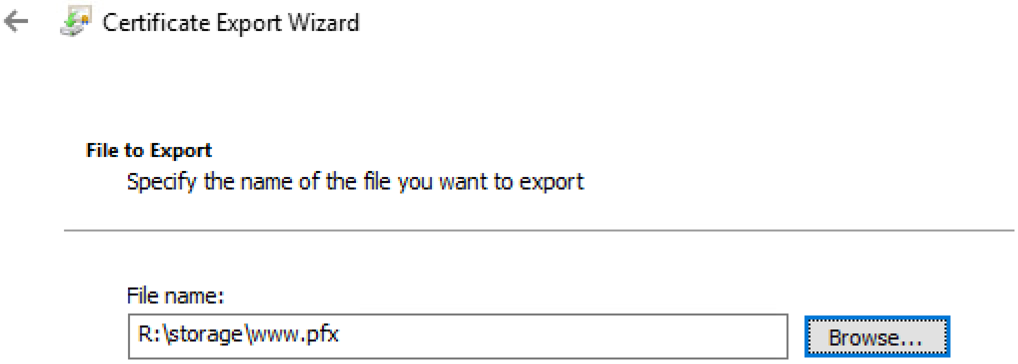
Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key



File to Export
Specify the name of the file you want to export

File name:
R:\storage\www.pfx

RTR-L (NTP)

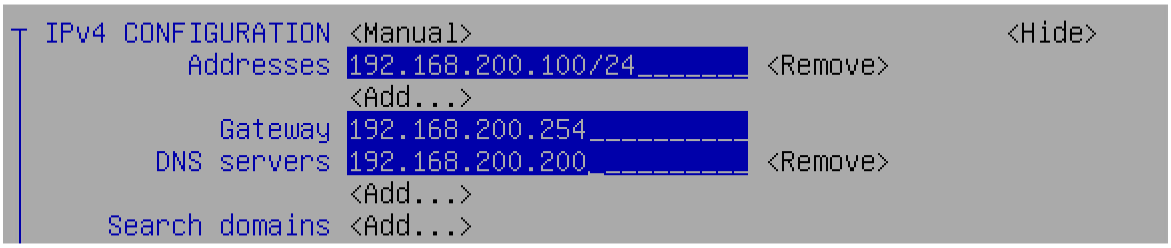
```
ip domain name int.demo.wsr
ip name-server 192.168.200.200
ntp server ntp.int.demo.wsr
```

RTR-R (NTP)

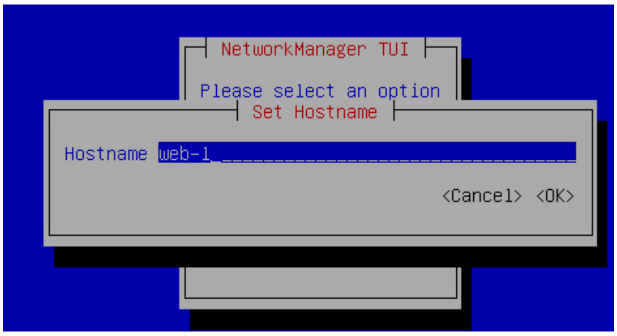
```
ip domain name int.demo.wsr
ip name-server 192.168.200.200
ntp server ntp.int.demo.wsr
```

WEB-L

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

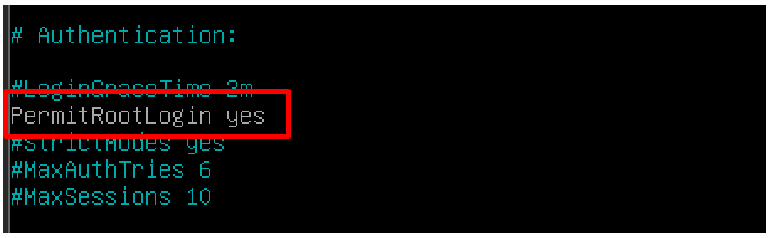


```
┬ IPv4 CONFIGURATION <Manual>                                    <Hide>
│          Addresses 192.168.200.100/24_______ <Remove>
│                    <Add...>
│            Gateway 192.168.200.254__________
│        DNS servers 192.168.200.200__________ <Remove>
│                    <Add...>
│     Search domains <Add...>
```



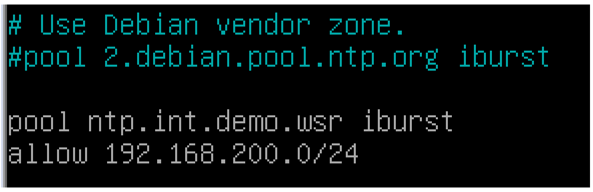
```
Hostname web-1
```

Reboot
Nano /etc/ssh/sshd_config

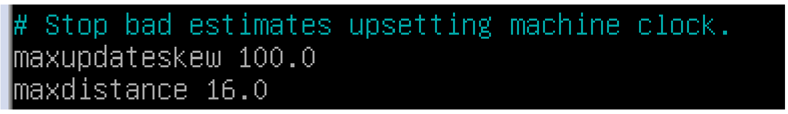


```
# Authentication:

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

systemctl restart sshd
systemctl enable ssh
nano /etc/chrony/chrony.conf

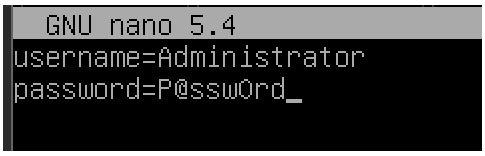


```
# Use Debian vendor zone.
#pool 2.debian.pool.ntp.org iburst

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



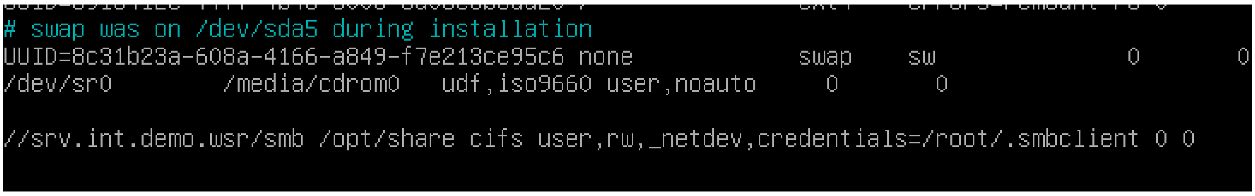
```
# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0
maxdistance 16.0
```

timedatectl set-timezone UTC
systemctl restart chrony
nano /root/.smbclient



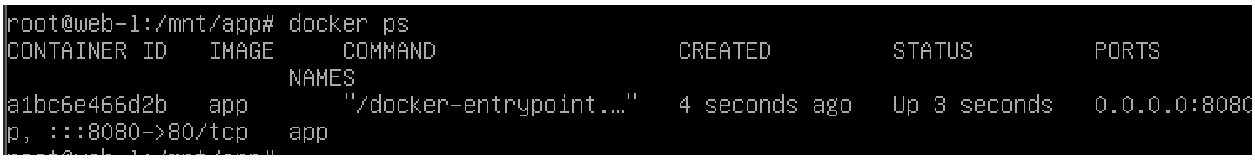
```
  GNU nano 5.4
username=Administrator
password=P@ssw0rd_
```

mkdir /opt/share
nano /etc/fstab



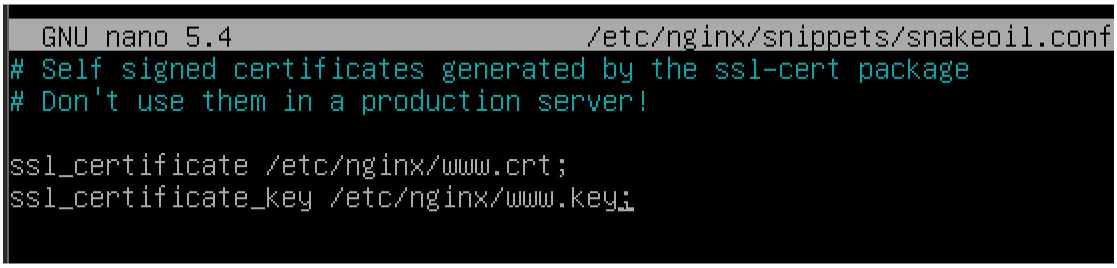
```
# swap was on /dev/sda5 during installation
UUID=8c31b23a-608a-4166-a849-f7e213ce95c6 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

//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



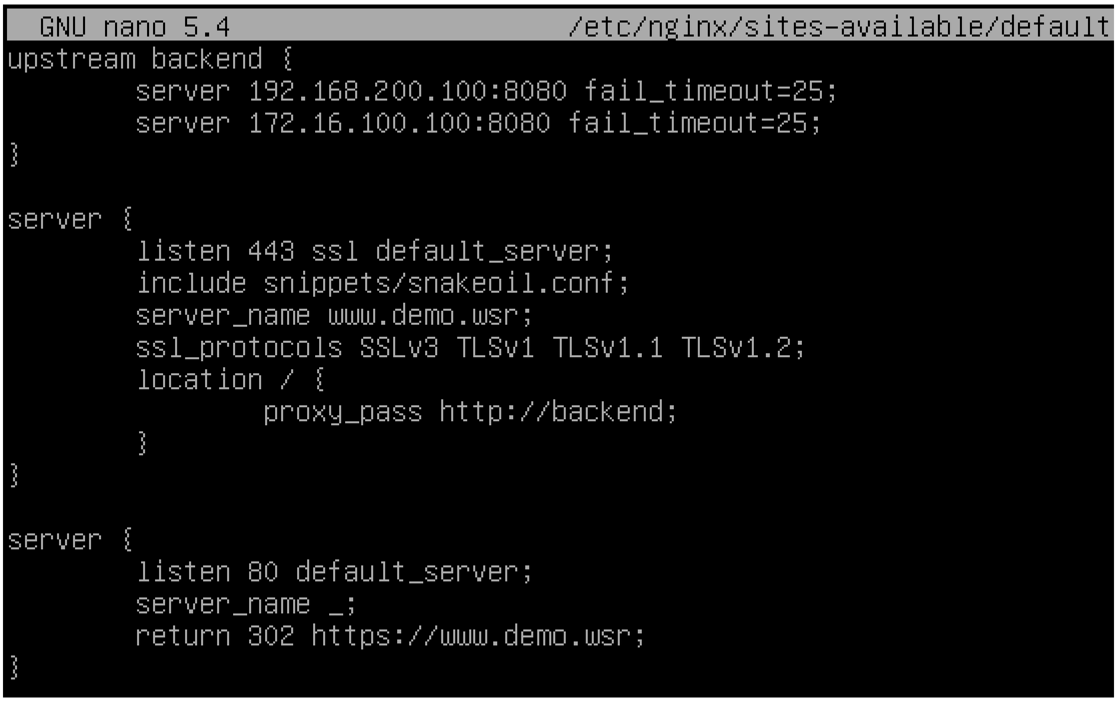
```
root@web-1:/mnt/app# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS          PORTS
                NAMES
a1bc6e466d2b   app       "/docker-entrypoint.…"   4 seconds ago    Up 3 seconds    0.0.0.0:8080
p, :::8080->80/tcp   app
```

```
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;
```

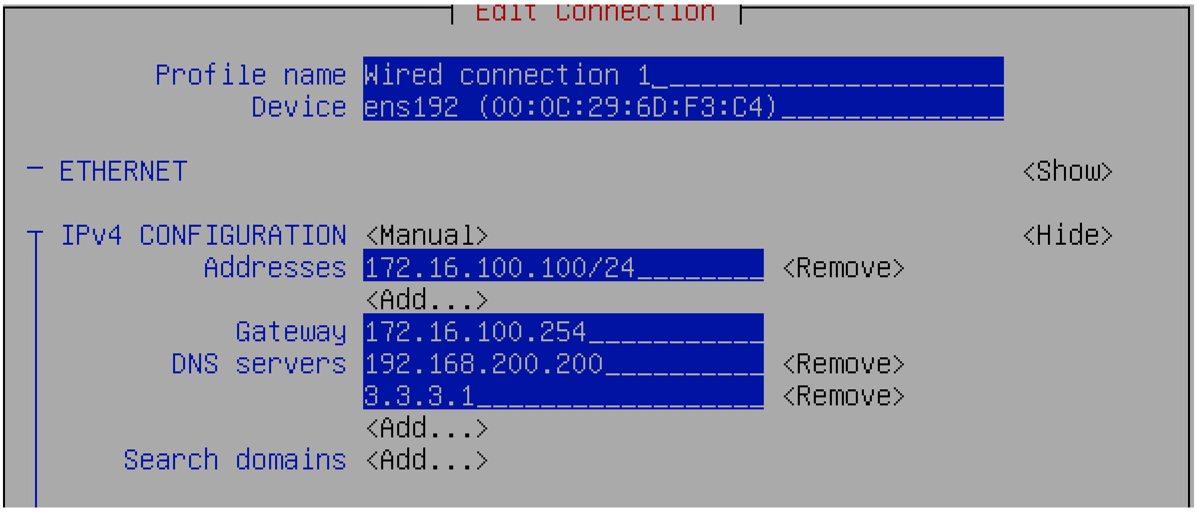
```
rm /etc/nginx/sites-available/default
nano /etc/nginx/sites-available/default
```



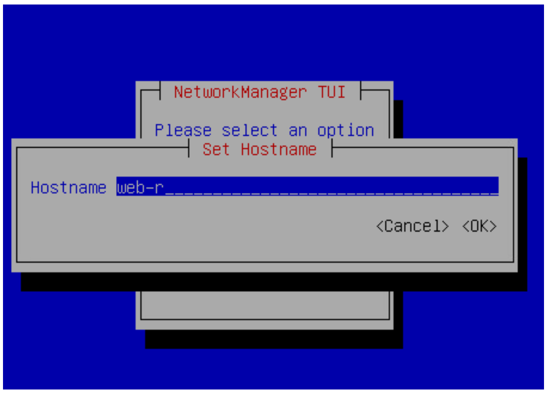
```
  GNU nano 5.4                        /etc/nginx/sites-available/default
upstream backend {
        server 192.168.200.100:8080 fail_timeout=25;
        server 172.16.100.100:8080 fail_timeout=25;
}

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 open-sshserver chrony cifs-utils
nginx
nmtui
```



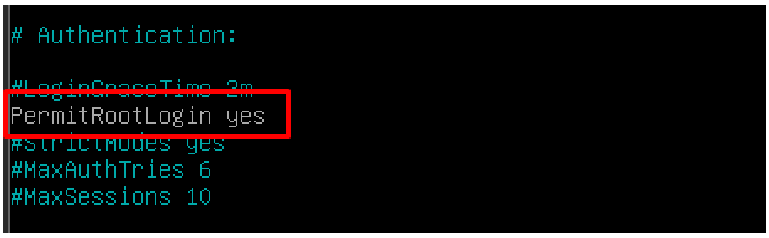
```
Edit Connection

     Profile name Wired connection 1_______________________
           Device ens192 (00:0C:29:6D:F3:C4)______________

─ ETHERNET                                                  <Show>

┬ IPv4 CONFIGURATION <Manual>                               <Hide>
│          Addresses 172.16.100.100/24________ <Remove>
│                    <Add...>
│            Gateway 172.16.100.254___________
│        DNS servers 192.168.200.200__________ <Remove>
│                    3.3.3.1__________________ <Remove>
│                    <Add...>
│     Search domains <Add...>
```



```
NetworkManager TUI
Please select an option
Set Hostname

Hostname web-r_________________________________

                                  <Cancel> <OK>
```

Reboot

Nano /etc/ssh/sshd_config

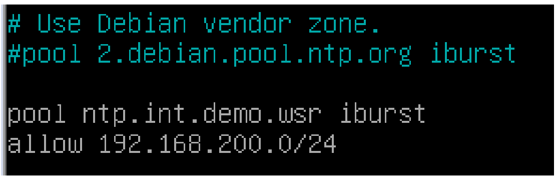


```
# Authentication:

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

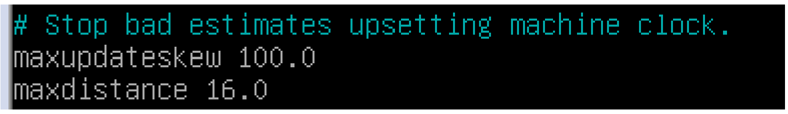
systemctl restart sshd

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
```

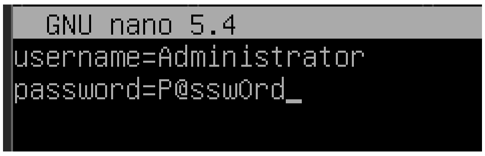


```
# Stop bad estimates upsetting machine clock.
maxupdateskew 100.0
maxdistance 16.0
```

timedatectl set-timezone UTC

systemctl restart chrony

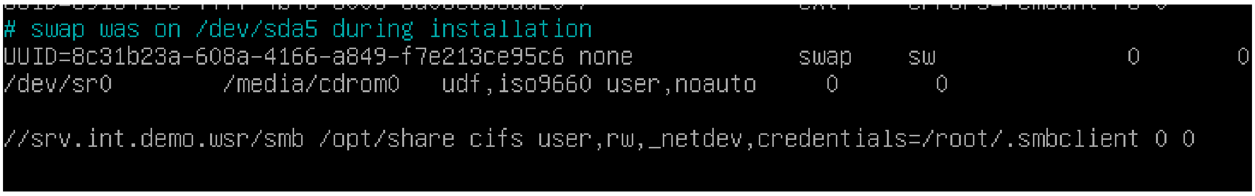
nano /root/.smbclient



```
  GNU nano 5.4
username=Administrator
password=P@ssw0rd_
```

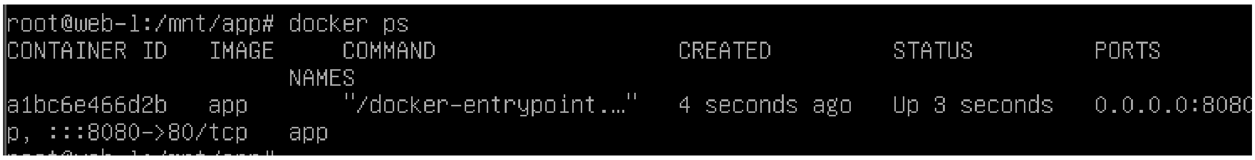
mkdir /opt/share

```
nano /etc/fstab
```



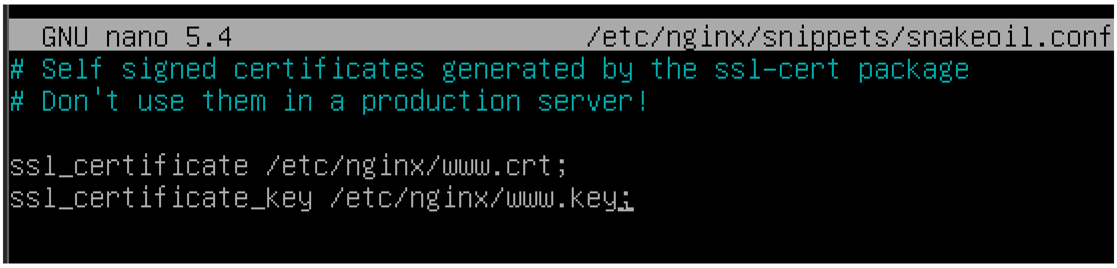
```
# swap was on /dev/sda5 during installation
UUID=8c31b23a-608a-4166-a849-f7e213ce95c6 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

//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
```



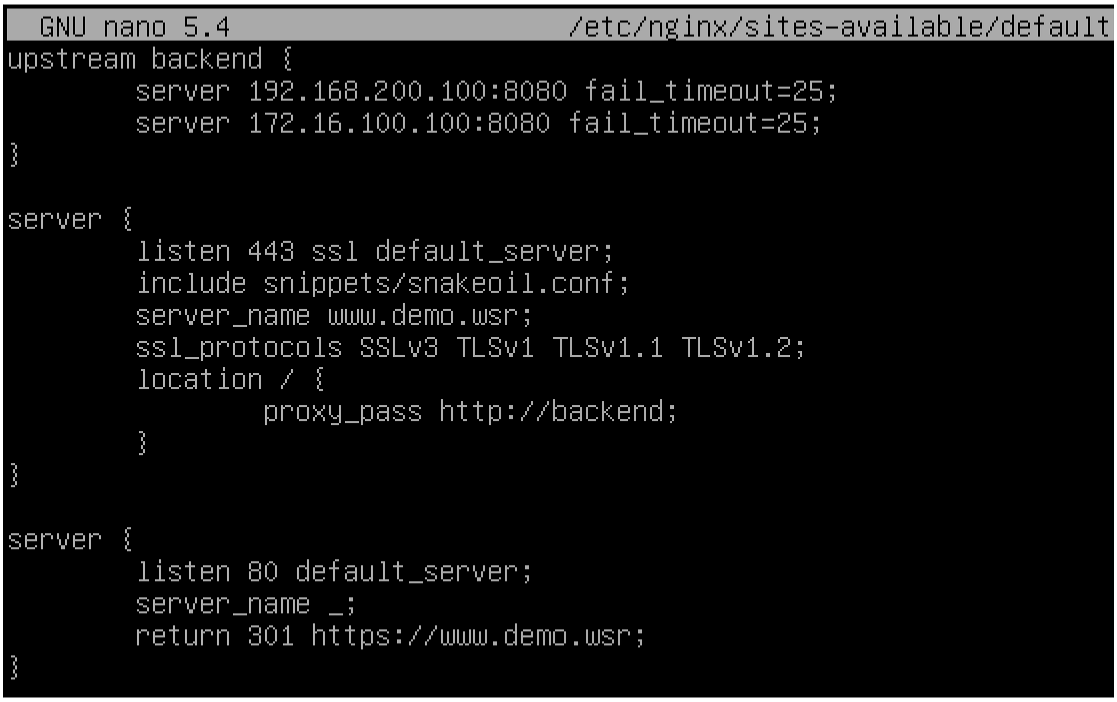
```
root@web-1:/mnt/app# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED         STATUS         PORTS
               NAMES
a1bc6e466d2b   app       "/docker-entrypoint.…"   4 seconds ago   Up 3 seconds   0.0.0.0:8080
p, :::8080->80/tcp   app
```

```
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;
```

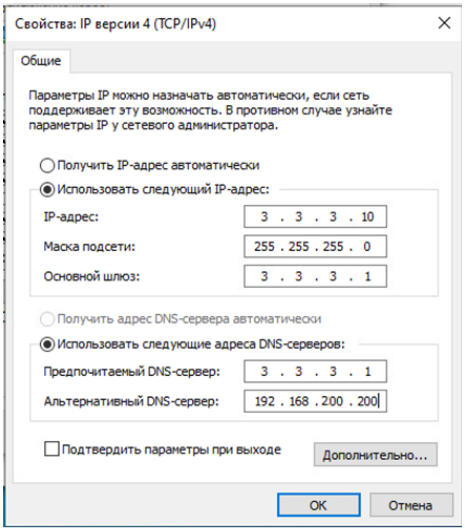
```
rm /etc/nginx/sites-available/default
nano /etc/nginx/sites-available/default
```



```
  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



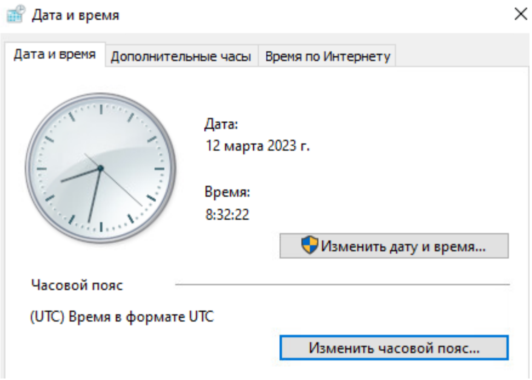
Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

○ Получить IP-адрес автоматически
● Использовать следующий IP-адрес:
IP-адрес: 3 . 3 . 3 . 10
Маска подсети: 255 . 255 . 255 . 0
Основной шлюз: 3 . 3 . 3 . 1

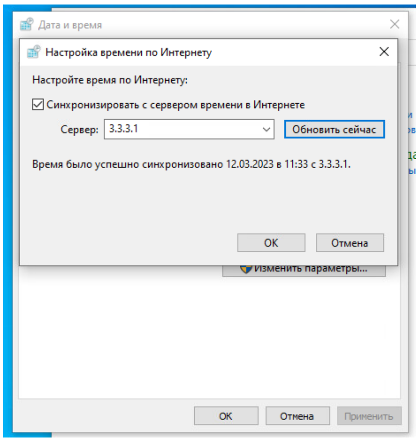
○ Получить адрес DNS-сервера автоматически
● Использовать следующие адреса DNS-серверов:
Предпочитаемый DNS-сервер: 3 . 3 . 3 . 1
Альтернативный DNS-сервер: 192 . 168 . 200 . 200

□ Подтвердить параметры при выходе

2. Присваиваем имя
3. Настраиваем NTP



Дата:
12 марта 2023 г.
Время:
8:32:22
Часовой пояс
(UTC) Время в формате UTC



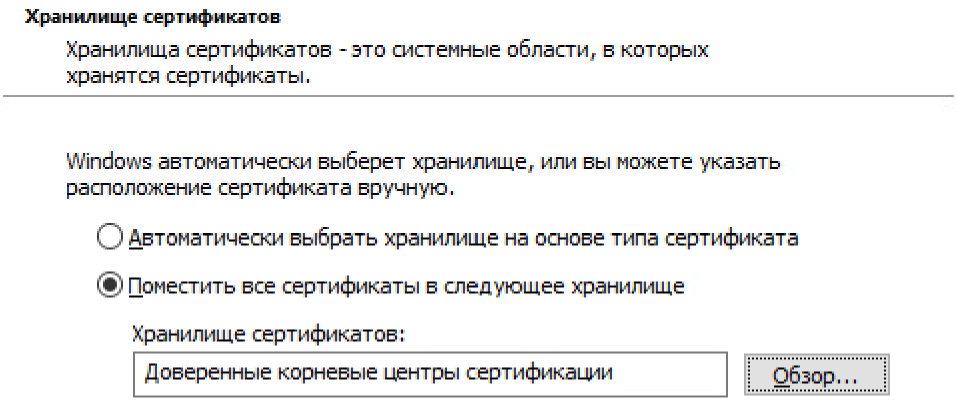
Настройте время по Интернету:
☑ Синхронизировать с сервером времени в Интернете
Сервер: 3.3.3.1
Время было успешно синхронизировано 12.03.2023 в 11:33 с 3.3.3.1.

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

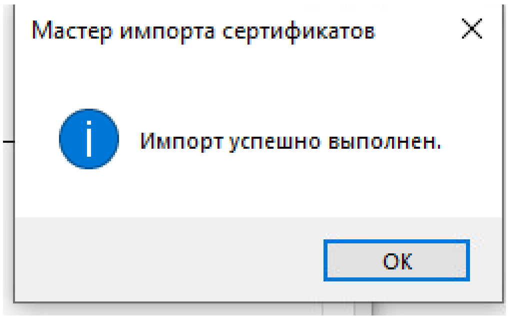


Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

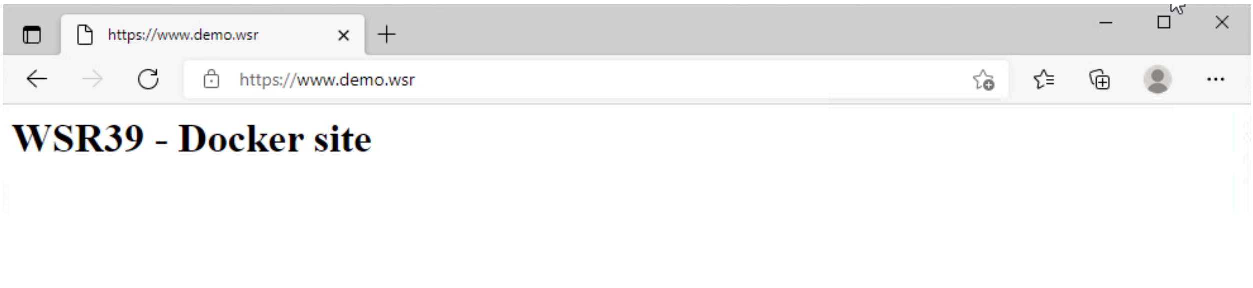
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

○ Автоматически выбрать хранилище на основе типа сертификата
● Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:
Доверенные корневые центры сертификации


Мастер импорта сертификатов

Импорт успешно выполнен.



WSR39 - Docker site

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
```