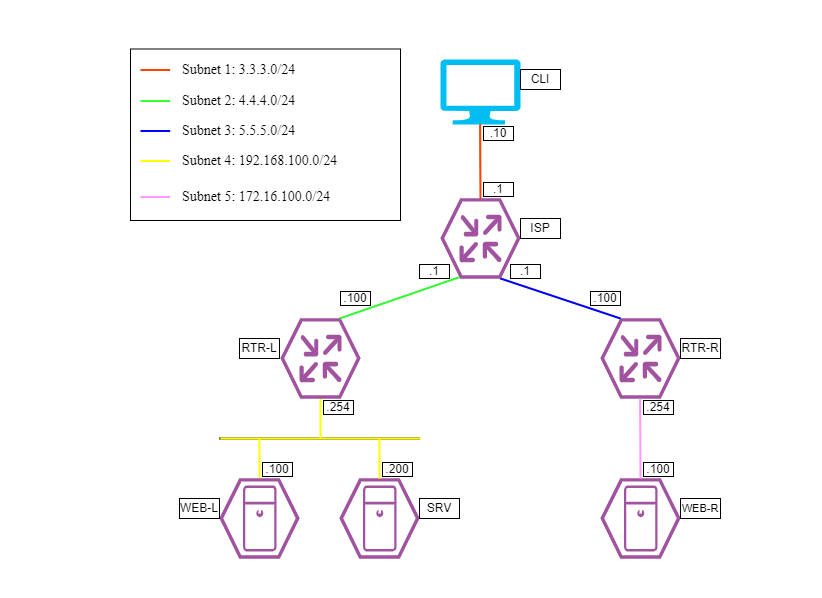
**Модуль 1**

Вариант 1-0 (публичный)

[](https://user-images.githubusercontent.com/79700810/149956179-026c9bba-e6fc-495a-81df-4c6ddb0ec1d6.png)

**Виртуальные машины и коммутация.**

Необходимо выполнить создание и базовую конфигурацию виртуальных машин.

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

**Таблица 1. Характеристики ВМ**

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

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

Убедитесь что все ВМ созданы в соотведствии со схемой

[](https://user-images.githubusercontent.com/79700810/150134013-7ba0f3e5-29cb-4c69-8b6b-3d3c339c99b1.png)

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

**RTR-L**

en

conf t

hostname RTR-L

do wr

**RTR-R**

en

conf t

hostname RTR-R

do wr

**SRV**

Rename-Computer -NewName SRV

**WEB-L**

hostnamectl set-hostname WEB-L

**WEB-R**

hostnamectl set-hostname WEB-R

**ISP**

hostnamectl set-hostname ISP

**CLI**

Rename-Computer -NewName CLI

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

**RTR-L**

int gi 1

ip address 4.4.4.100 255.255.255.0

no sh

int gi 2

ip address 192.168.100.254 255.255.255.0

no sh

end

wr

**RTR-R**

int gi 1

ip address 5.5.5.100 255.255.255.0

no sh

int gi 2

ip address 172.16.100.254 255.255.255.0

no sh

end

wr

**SRV**

$GetIndex = Get-NetAdapter

New-NetIPAddress -InterfaceIndex $GetIndex.ifIndex -IPAddress 192.168.100.200 -PrefixLength 24 -DefaultGateway 192.168.100.254

Set-DnsClientServerAddress -InterfaceIndex $GetIndex.ifIndex -ServerAddresses ("192.168.100.200","4.4.4.1")

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

**WEB-L**

apt-cdrom add

apt install -y network-manager

nmcli connection show

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

**WEB-R**

apt-cdrom add

apt install -y network-manager

nmcli connection show

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

**ISP**

apt-cdrom add

apt install -y network-manager bind9 chrony

nmcli connection show

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

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

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

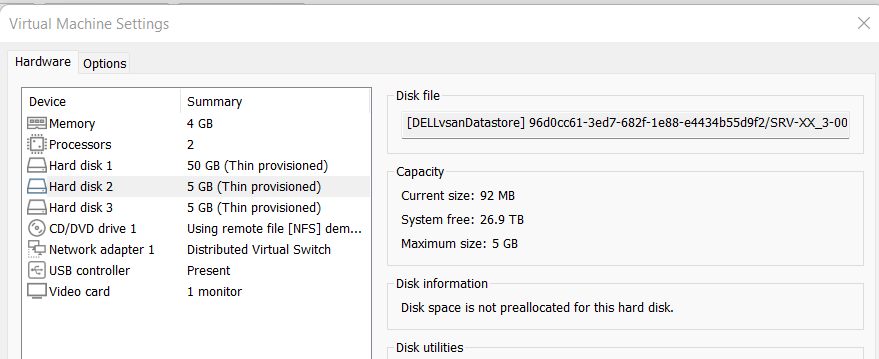
**CLI**

$GetIndex = Get-NetAdapter

New-NetIPAddress -InterfaceIndex $GetIndex.ifIndex -IPAddress 3.3.3.10 -PrefixLength 24 -DefaultGateway 3.3.3.1

Set-DnsClientServerAddress -InterfaceIndex $GetIndex.ifIndex -ServerAddresses ("3.3.3.1")

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

[](https://user-images.githubusercontent.com/79700810/150127140-0285670d-773e-4d61-8739-29d3455a57b1.png)

**Сетевая связность.**

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

1. Сети, подключенные к ISP, считаются внешними:
   * Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;
2. Платформы контроля трафика, установленные на границах регионов, должны выполнять трансляцию трафика, идущего из соответствующих внутренних сетей во внешние сети стенда и в сеть Интернет.
   * Трансляция исходящих адресов производится в адрес платформы,расположенный во внешней сети.
3. Между платформами должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.
   * Трафик, проходящий по данному туннелю, должен быть защищен:
     + Платформа ISP не должна иметь возможности просматривать содержимое пакетов, идущих из одной внутренней сети в другую.
   * Туннель должен позволять защищенное взаимодействие между платформами управления трафиком по их внутренним адресам
     + Взаимодействие по внешним адресам должно происходит без применения туннеля и шифрования
   * Трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.
4. Платформа управления трафиком RTR-L выполняет контроль входящего трафика согласно следующим правилам:
   * Разрешаются подключения к портам DNS, HTTP и HTTPS для всех клиентов;
     + Порты необходимо для работы настраиваемых служб
   * Разрешается работа выбранного протокола организации защищенной связи;
     + Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”
   * Разрешается работа протоколов ICMP;
   * Разрешается работа протокола SSH;
   * Прочие подключения запрещены;
   * Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;
5. Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:
   * Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;
     + Порты необходимо для работы настраиваемых служб
   * Разрешается работа выбранного протокола организации защищенной связи;
     + Разрешение портов должно быть выполнено по принципу необходимо и достаточно”
   * Разрешается работа протоколов ICMP;
   * Разрешается работа протокола SSH;
   * Прочие подключения запрещены;
   * Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;
6. Обеспечьте настройку служб SSH региона Left и Right:
   * Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на ВМ Web-L;
   * Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-R на порт 2244 должны быть перенаправлены на ВМ Web-R;

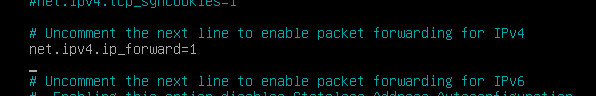
**1. Сети, подключенные к ISP, считаются внешними:**

**ISP forward**

nano /etc/sysctl.conf

net.ipv4.ip\_forward=1

sysctl -p

[](https://user-images.githubusercontent.com/79700810/149896195-71778f11-2e69-4750-b6a0-9424d4dc8890.png)

**RTR-L Gitw**

ip route 0.0.0.0 0.0.0.0 4.4.4.1

**RTR-R gitw**

ip route 0.0.0.0 0.0.0.0 5.5.5.1

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

**RTR-L NAT**

на внутр. интерфейсе - ip nat inside

на внешн. интерфейсе - ip nat outside

int gi 1

ip nat outside

!

int gi 2

ip nat inside

!

access-list 1 permit 192.168.100.0 0.0.0.255

ip nat inside source list 1 interface Gi1 overload

**RTR-R NAT**

int gi 1

ip nat outside

!

int gi 2

ip nat inside

!

access-list 1 permit 172.16.100.0 0.0.0.255

ip nat inside source list 1 interface Gi1 overload

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

**RTR-L GRE**

interface Tunne 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 192.168.100.0 0.0.0.255

network 172.16.1.0 0.0.0.255

**RTR-R**

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

**RTR-L**

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

**RTR-R**

conf t

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

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

**RTR-L ACL**

ip access-list extended Lnew

permit tcp any any established

permit udp host 4.4.4.100 eq 53 any

permit udp host 5.5.5.1 eq 123 any

permit tcp any host 4.4.4.100 eq 80

permit tcp any host 4.4.4.100 eq 443

permit tcp any host 4.4.4.100 eq 2222

permit udp host 5.5.5.100 host 4.4.4.100 eq 500

permit esp any any

permit icmp any any

int gi 1

ip access-group Lnew in

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

**RTR-R ACL**

ip access-list extended Rnew

permit tcp any any established

permit tcp any host 5.5.5.100 eq 80

permit tcp any host 5.5.5.100 eq 443

permit tcp any host 5.5.5.100 eq 2244

permit udp host 4.4.4.100 host 5.5.5.100 eq 500

permit esp any any

permit icmp any any

int gi 1

ip access-group Rnew in

**6. Обеспечьте настройку служб SSH региона Left:**

**RTR-L SSH**

ip nat inside source static tcp 192.168.100.100 22 4.4.4.100 2222

**RTR-R SSH**

ip nat inside source static tcp 172.16.100.100 22 5.5.5.100 2244

**SSH WEB-L**

apt-cdrom add

apt install -y openssh-server ssh

systemctl start sshd

systemctl enable ssh

**SSH WEB-R**

apt-cdrom add

apt install -y openssh-server ssh

systemctl start sshd

systemctl enable ssh

**Инфраструктурные службы**

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

1. Выполните настройку первого уровня DNS-системы стенда:
   * Используется ВМ ISP;
   * Обслуживается зона demo.wsr
     + Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;
   * Сервер делегирует зону int.demo.wsr на SRV;
     + Поскольку SRV находится во внутренней сети западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона.
     + Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV
   * Внешний клиент CLI должен использовать DNS-службу, развернутую на ISP, по умолчанию;
2. Выполните настройку второго уровня DNS-системы стенда;
   * Используется ВМ SRV;
   * Обслуживается зона int.demo.wsr;
     + Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;
   * Обслуживаются обратные зоны для внутренних адресов регионов
     + Имена для разрешения обратных записей следует брать из Таблицы 2;
   * Сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;
     + Обслуживание клиентов(внешних и внутренних), обращающихся к к зоне int.demo.wsr, должно производится без каких либо ограничений по адресу источника;
   * Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен;
3. Выполните настройку первого уровня системы синхронизации времени:
   * Используется сервер ISP.
   * Сервер считает собственный источник времени верным, stratum=4;
   * Сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком;
     + Подразумевается обращение SRV для синхронизации времени;
   * Клиент CLI должен использовать службу времени ISP;
4. Выполните конфигурацию службы второго уровня времени на SRV
   * Сервер синхронизирует время с хостом ISP;
     + Синхронизация с другими источникам запрещена;
   * Сервер должен допускать обращения внутренних хостов регионов, в том числе и платформ управления трафиком, для синхронизации времени;
   * Все внутренние хосты(в том числе и платформы управления трафиком) должны синхронизировать свое время с SRV;
5. Реализуйте файловый SMB-сервер на базе SRV
   * Сервер должен предоставлять доступ для обмена файлами серверам WEB-L и WEB-R;
   * Сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:
     + /mnt/storage для система на базе Linux;
     + Диск R:\ для систем на базе Windows;
   * Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа “Зеркало”;
6. Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:
   * Служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux
     + Разделяемый каталог должен быть смонтирован по адресу /opt/share;
   * Каталог должен позволять удалять и создавать файлы в нем для всех пользователей;
7. Выполните настройку центра сертификации на базе SRV:
   * В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca
   * Выдаваемые сертификаты должны иметь срок жизни не менее 500 дней;
   * Параметры выдаваемых сертификатов:
     + Страна RU;
     + Организация DEMO.WSR;
     + Прочие поля (за исключением CN) должны быть пусты;

**Таблица 2. DNS-записи зон**

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

**1. Выполните настройку первого уровня DNS-системы стенда:**

**ISP**

apt-cdrom add

apt install -y bind9

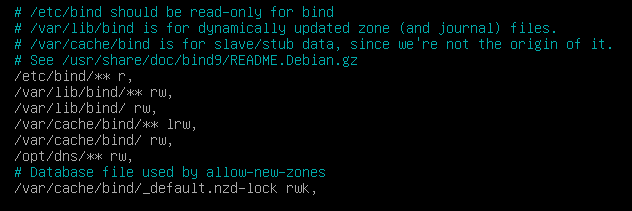
mkdir /opt/dns

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

chown -R bind:bind /opt/dns

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

/opt/dns/\*\* rw,

[](https://user-images.githubusercontent.com/79700810/149896979-a9af8838-dc2a-450b-ac33-efbc1bd98ba8.png)

systemctl restart apparmor.service

nano /etc/bind/named.conf.options

[](https://user-images.githubusercontent.com/79700810/149960943-5fd4702e-a060-4425-ac6b-14cca42e02bf.png)

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

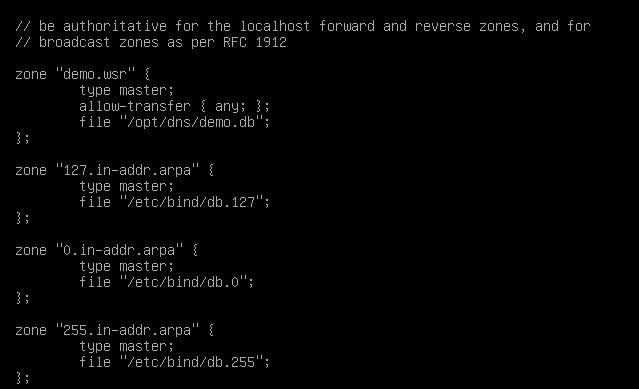
zone "demo.wsr" {

type master;

allow-transfer { any; };

file "/opt/dns/demo.db";

};

[](https://user-images.githubusercontent.com/79700810/149897089-83a29cdb-e5b7-4747-ba0e-e97c600ec2ca.png)

nano /opt/dns/demo.db

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

@ IN NS isp.demo.wsr.

isp IN A 3.3.3.1

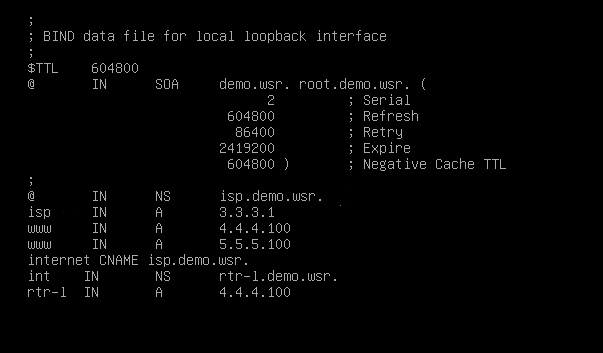
www IN A 4.4.4.100

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

[](https://user-images.githubusercontent.com/79700810/150322909-a9b426ab-9ed2-46e6-bcd2-db39609fe406.png)

systemctl restart bind9

**RTR-L**

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

ip nat inside source static tcp 192.168.100.200 53 4.4.4.100 53

!

ip nat inside source static udp 192.168.100.200 53 4.4.4.100 53

**2. Выполните настройку второго уровня DNS-системы стенда;**

**SRV**

Install-WindowsFeature -Name DNS -IncludeManagementTools

Add-DnsServerPrimaryZone -Name "int.demo.wsr" -ZoneFile "int.demo.wsr.dns"

Add-DnsServerPrimaryZone -NetworkId 192.168.100.0/24 -ZoneFile "int.demo.wsr.dns"

Add-DnsServerPrimaryZone -NetworkId 172.16.100.0/24 -ZoneFile "int.demo.wsr.dns"

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

Add-DnsServerResourceRecordA -Name "web-l" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "192.168.100.100" -CreatePtr

Add-DnsServerResourceRecordA -Name "web-r" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "172.16.100.100" -CreatePtr

Add-DnsServerResourceRecordA -Name "srv" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "192.168.100.200" -CreatePtr

Add-DnsServerResourceRecordA -Name "rtr-l" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "192.168.100.254" -CreatePtr

Add-DnsServerResourceRecordA -Name "rtr-r" -ZoneName "int.demo.wsr" -AllowUpdateAny -IPv4Address "172.16.100.254" -CreatePtr

Add-DnsServerResourceRecordCName -Name "webapp1" -HostNameAlias "web-l.int.demo.wsr" -ZoneName "int.demo.wsr"

Add-DnsServerResourceRecordCName -Name "webapp2" -HostNameAlias "web-r.int.demo.wsr" -ZoneName "int.demo.wsr"

Add-DnsServerResourceRecordCName -Name "ntp" -HostNameAlias "srv.int.demo.wsr" -ZoneName "int.demo.wsr"

Add-DnsServerResourceRecordCName -Name "dns" -HostNameAlias "srv.int.demo.wsr" -ZoneName "int.demo.wsr"

**3. Выполните настройку первого уровня системы синхронизации времени:**

**ISP NTP**

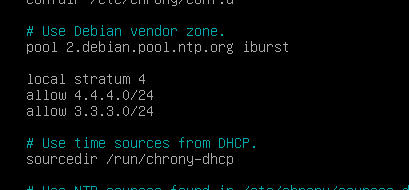
apt install -y chrony

nano /etc/chrony/chrony.conf

local stratum 4

allow 4.4.4.0/24

allow 3.3.3.0/24

[](https://user-images.githubusercontent.com/79700810/149897796-b798dc28-2555-4aa4-9043-9340dda17f57.png)

systemctl restart chronyd

**4. Выполните конфигурацию службы второго уровня времени на SRV**

**SRV NTP**

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

w32tm /query /status

Start-Service W32Time

w32tm /config /manualpeerlist:4.4.4.1 /syncfromflags:manual /reliable:yes /update

Restart-Service W32Time

**CLI NTP**

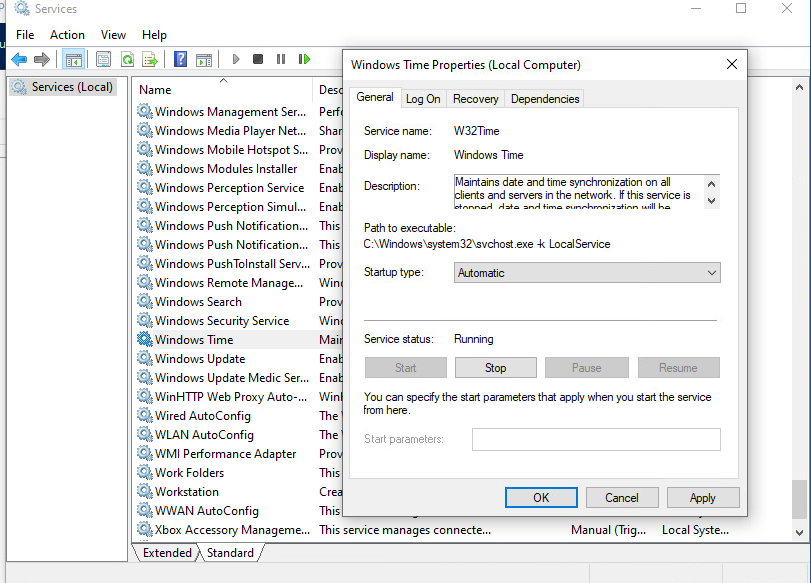
New-NetFirewallRule -DisplayName "NTP" -Direction Inbound -LocalPort 123 -Protocol UDP -Action Allow

Start-Service W32Time

w32tm /config /manualpeerlist:4.4.4.1 /syncfromflags:manual /reliable:yes /update

Restart-Service W32Time

Set-Service -Name W32Time -StartupType Automatic

[](https://user-images.githubusercontent.com/79700810/149523036-1db4eeca-ca6b-491a-9d19-d6c097a7ca80.png)

**RTR-L NTP**

ip domain name int.demo.wsr

ip name-server 192.168.100.200

ntp server ntp.int.demo.wsr

**RTR-R NTP**

ip domain name int.demo.wsr

ip name-server 192.168.100.200

ntp server ntp.int.demo.wsr

**WEB-L NTP**

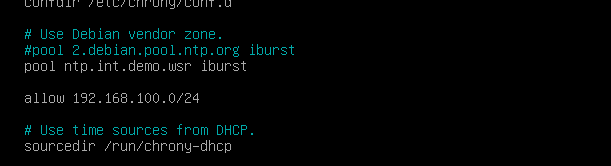
apt-cdrom add

apt install -y chrony

nano /etc/chrony/chrony.conf

pool ntp.int.demo.wsr iburst

allow 192.168.100.0/24

[](https://user-images.githubusercontent.com/79700810/149901162-a912e3d2-fc90-453b-ace0-347e58621ede.png)

systemctl restart chrony

**WEB-R NTP**

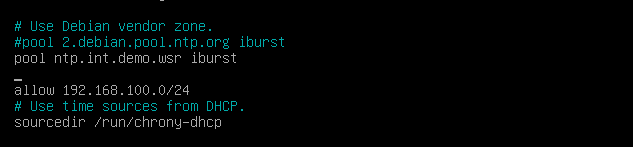
apt-cdrom add

apt install -y chrony

nano /etc/chrony/chrony.conf

pool ntp.int.demo.wsr iburst

allow 192.168.100.0/24

[](https://user-images.githubusercontent.com/79700810/149901302-79e89cb0-27da-44ce-9ac7-9ae2e74bb985.png)

systemctl restart chrony

**5. Реализуйте файловый SMB-сервер на базе SRV**

**SRV RAID1**

get-disk

set-disk -Number 1 -IsOffline $false

set-disk -Number 2 -IsOffline $false

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

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

Initialize-Disk -FriendlyName "RAID1"

New-Partition -DiskNumber 3 -UseMaximumSize -DriveLetter R

Format-Volume -DriveLetter R

**SRV SMB**

Install-WindowsFeature -Name FS-FileServer -IncludeManagementTools

New-Item -Path R:\storage -ItemType Directory

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

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

**WEB-L SMB**

apt-cdrom add

apt install -y cifs-utils

nano /root/.smbclient

username=Administrator

password=Pa$$w0rd

nano /etc/fstab

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

mkdir /opt/share

mount -a

**WEB-R SMB**

apt-cdrom add

apt install -y cifs-utils

nano /root/.smbclient

username=Administrator

password=Pa$$w0rd

nano /etc/fstab

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

mkdir /opt/share

mount -a

**7. Выполните настройку центра сертификации на базе SRV:**

**SRV ADCS**

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

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

Install-AdcsWebEnrollment -Confirm -force

New-SelfSignedCertificate -subject "localhost"

Get-ChildItem cert:\LocalMachine\My

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

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

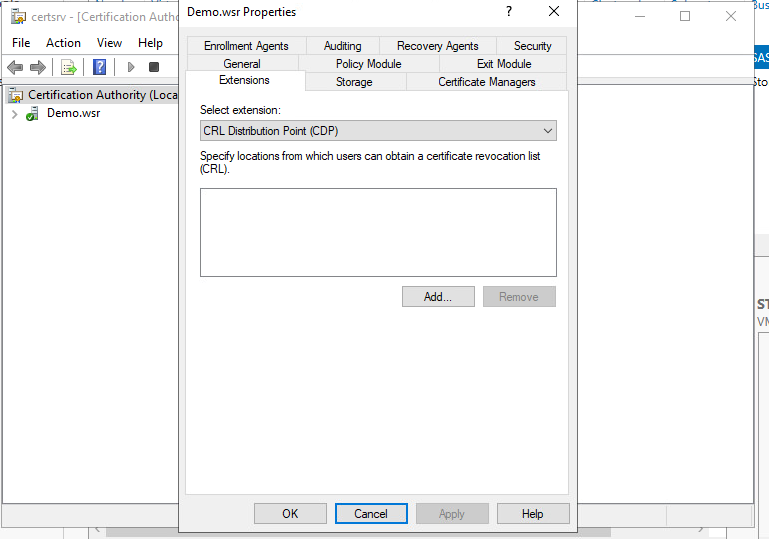
Start-WebSite -Name "Default Web Site"

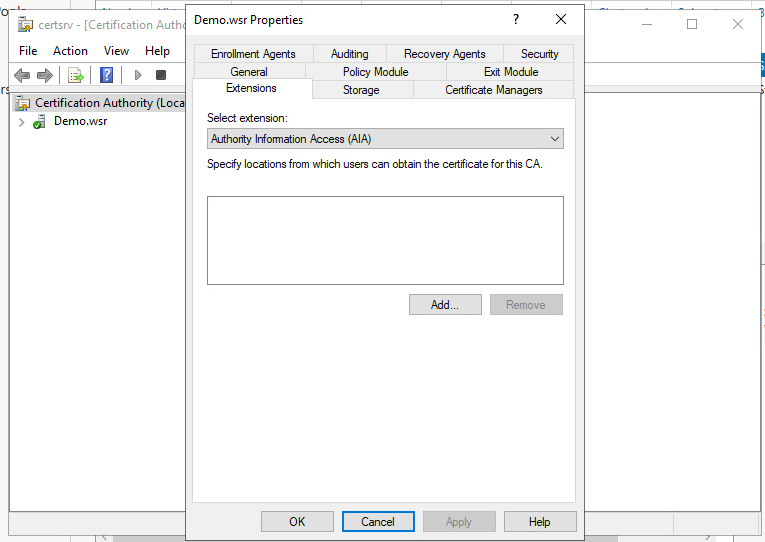
Get-CACrlDistributionPoint | Remove-CACrlDistributionPoint -force

Get-CAAuthorityInformationAccess |Remove-CAAuthorityInformationAccess -force

Get-CAAuthorityInformationAccess |Remove-CAAuthorityInformationAccess -force

Restart-Service CertSrc

[](https://user-images.githubusercontent.com/79700810/149936233-d2a22bf8-037c-4a82-a1f9-a72b24c3843f.png)

[](https://user-images.githubusercontent.com/79700810/149936259-13306942-38d5-4c15-850c-2bf5845968c9.png)

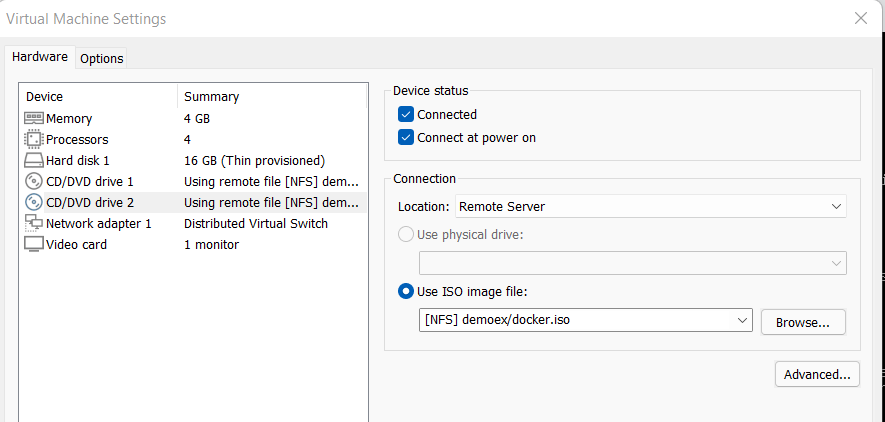
**Инфраструктура веб-приложения.**

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

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

**WEB-L Doc**

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

[](https://user-images.githubusercontent.com/79700810/150127347-b152ce8a-541d-4989-9b3b-dde041f27ccc.png)

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

apt-cdrom add

apt install -y docker-ce

systemctl start docker

systemctl enable docker

mkdir /mnt/app

mount /dev/sr1 /mnt/app

docker load < /mnt/app/app.tar

docker images

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

docker ps

**WEB-R Doc**

apt-cdrom add

apt install -y docker-ce

systemctl start docker

systemctl enable docker

mkdir /mnt/app

mount /dev/sr1 /mnt/app

docker load < /mnt/app/app.tar

docker images

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

docker ps

**RTR-L**

no ip http secure-server

wr

reload

ip nat inside source static tcp 192.168.100.100 80 4.4.4.100 80

ip nat inside source static tcp 192.168.100.100 443 4.4.4.100 443

**RTR-R**

no ip http secure-server

wr

reload

ip nat inside source static tcp 172.16.100.100 80 5.5.5.100 80

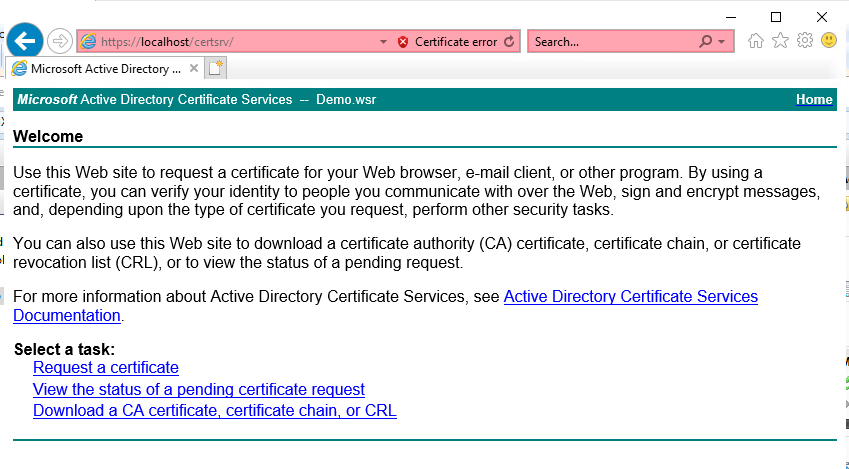
ip nat inside source static tcp 172.16.100.100 443 5.5.5.100 443

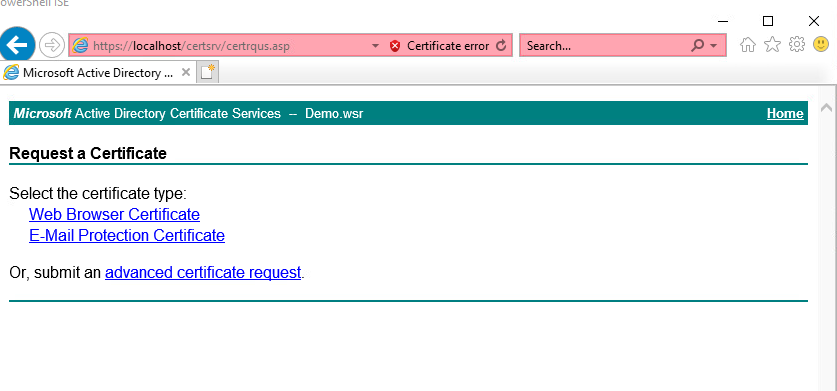
**3. Инструкция по работе с приложением расположена на дополнительном ISO-образе;**

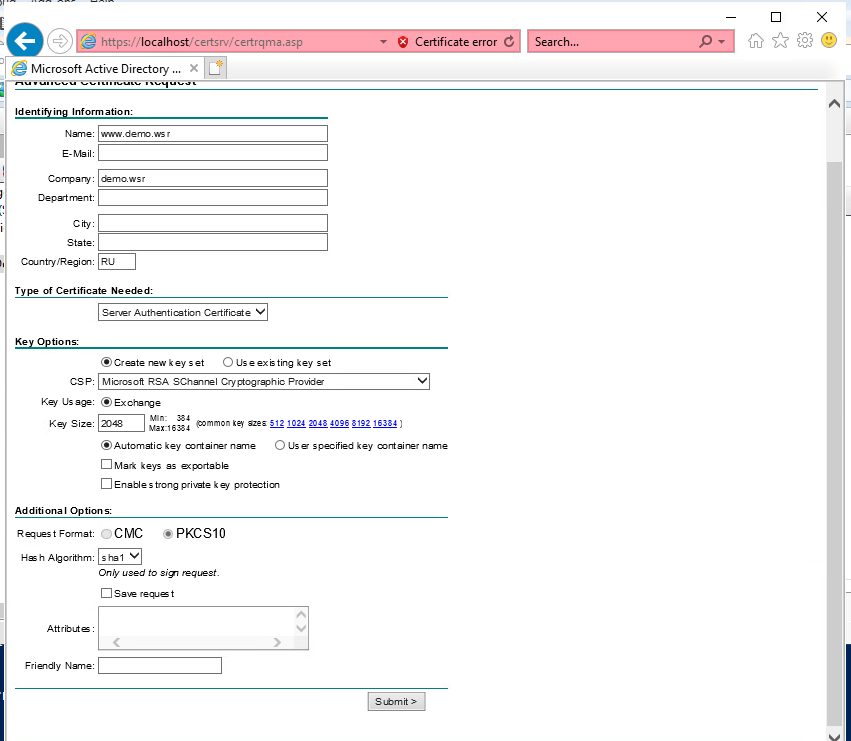
В данной момент инструкции к приложению нет, приложением является однастраничный сайт

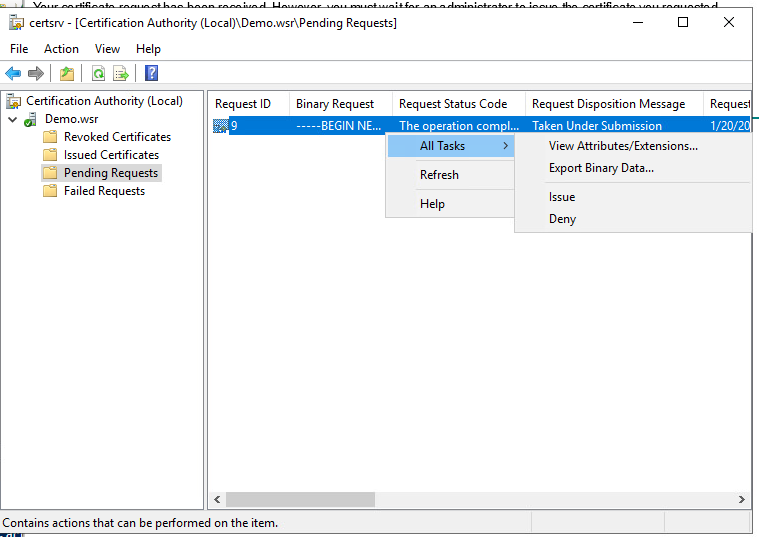
**4. Необходимо реализовать следующую инфраструктуру приложения**

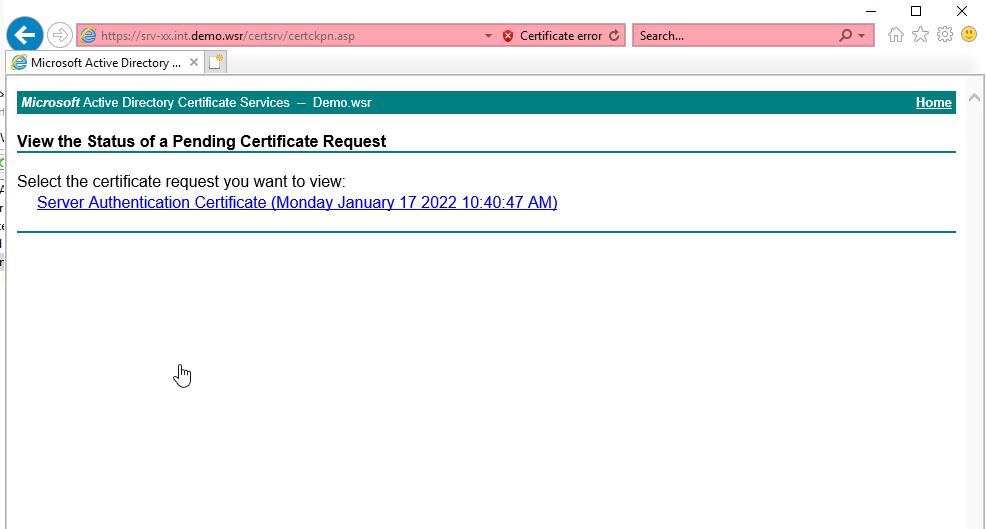
**SRV ssl**

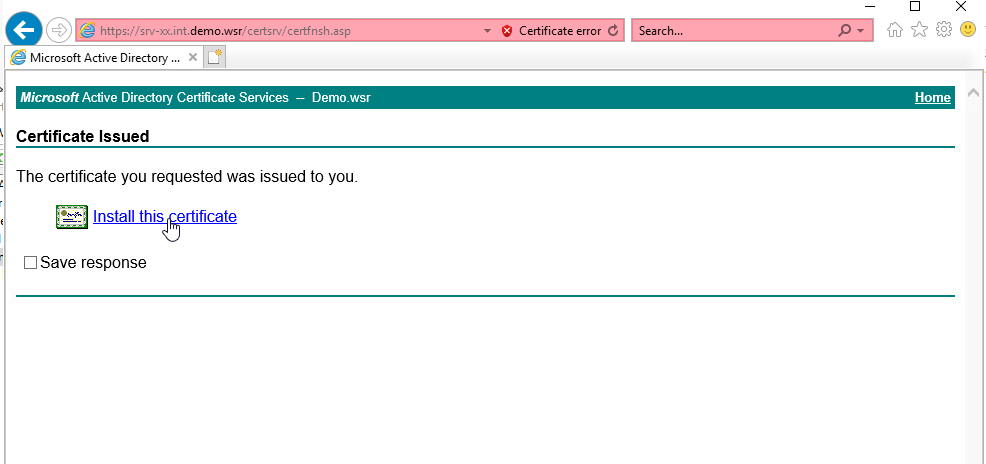
[](https://user-images.githubusercontent.com/79700810/150323908-1e37041d-450f-477e-9f9f-24a5f1313e54.png)

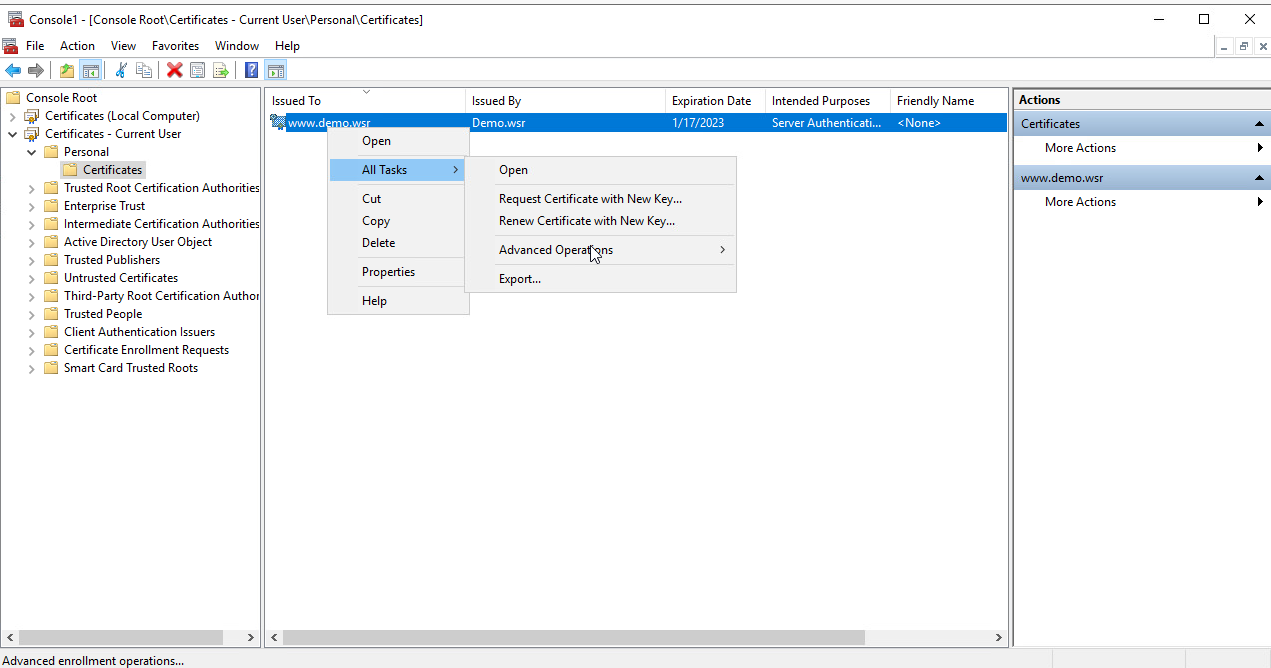
[](https://user-images.githubusercontent.com/79700810/150323973-2b4fd9a8-d934-4a49-8e7d-98e02efd7826.png)

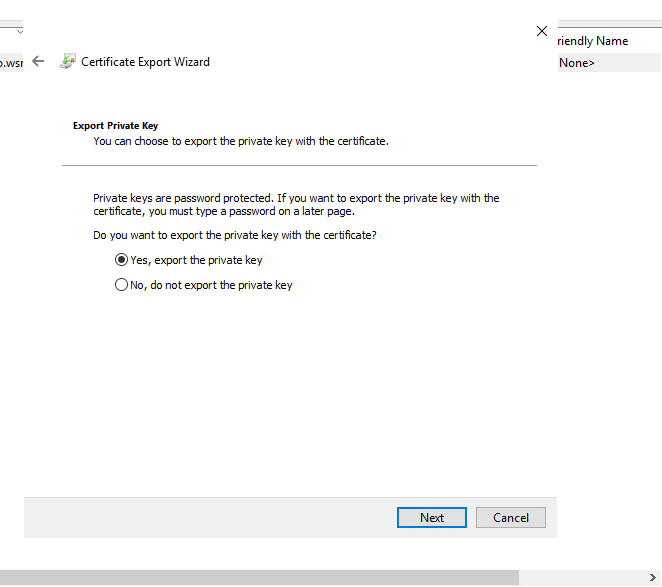
[](https://user-images.githubusercontent.com/79700810/150324325-b67039dc-6d6a-4dd1-9ade-67bbcaa3a6db.png)

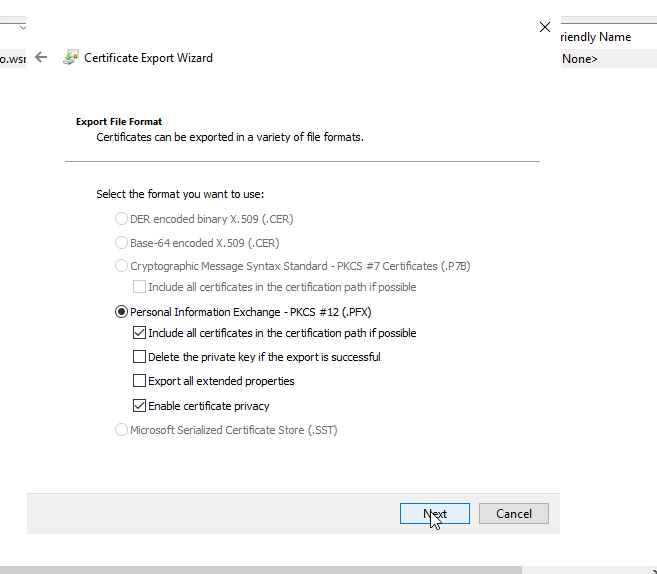
[](https://user-images.githubusercontent.com/79700810/150324402-d9e1c93a-46b0-42ac-83a0-02b97da4829b.png)

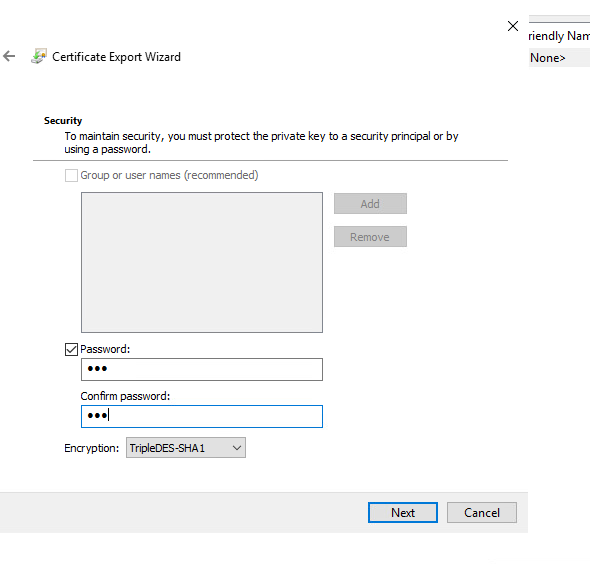
[](https://user-images.githubusercontent.com/79700810/149763513-cb821774-83ce-40f9-a47d-eaa3941504a5.png)

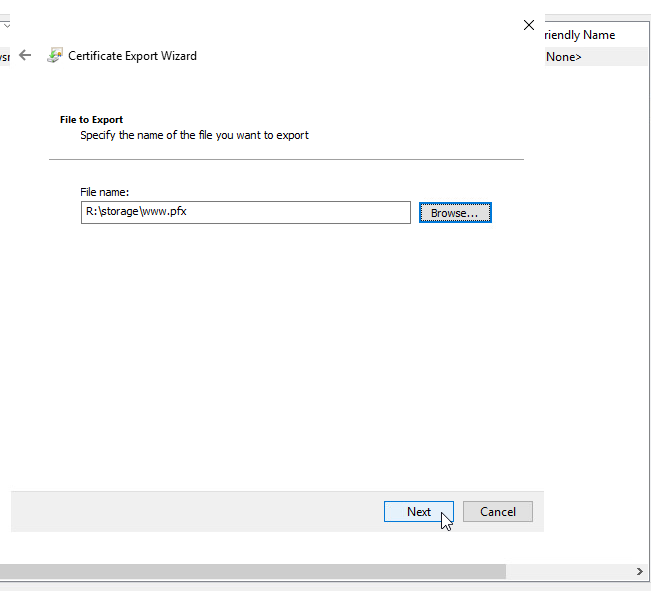
[](https://user-images.githubusercontent.com/79700810/149763553-5a666a1c-6069-4022-9e20-1e3041d345b7.png)

[](https://user-images.githubusercontent.com/79700810/149763685-b0dfb33e-ed50-4de6-937c-1aab86524df9.png)

[](https://user-images.githubusercontent.com/79700810/149763717-75fa754c-4084-4923-acd8-7dc85201fdb1.png)

[](https://user-images.githubusercontent.com/79700810/149763741-0e3281f3-b17b-4101-ad77-8dd21dfc7534.png)

[](https://user-images.githubusercontent.com/79700810/149763772-8f7acb37-379f-455e-9198-1117317d73ed.png)

[](https://user-images.githubusercontent.com/79700810/149763807-f91c2a81-d061-49bd-9b59-b93ae0e30ef3.png)

**5. Необходимо обеспечить отказоустойчивость приложения;**

**WEB-L ssl**

apt install -y nginx

cd /opt/share

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

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

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

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

nano /etc/nginx/snippets/snakeoil.conf

[](https://user-images.githubusercontent.com/79700810/149767553-c42bd433-0ebb-43dd-9256-abcd782c3e47.png)

nano /etc/nginx/sites-available/default

upstream backend {

server 192.168.100.100:8080 fail\_timeout=25;

server 172.16.100.100:8080 fail\_timeout=25;

}

server {

listen 443 ssl default\_server;

include snippers/snakeoil.conf;

server\_name www.demo.wsr;

location / {

proxy\_pass http://backend ;

}

}

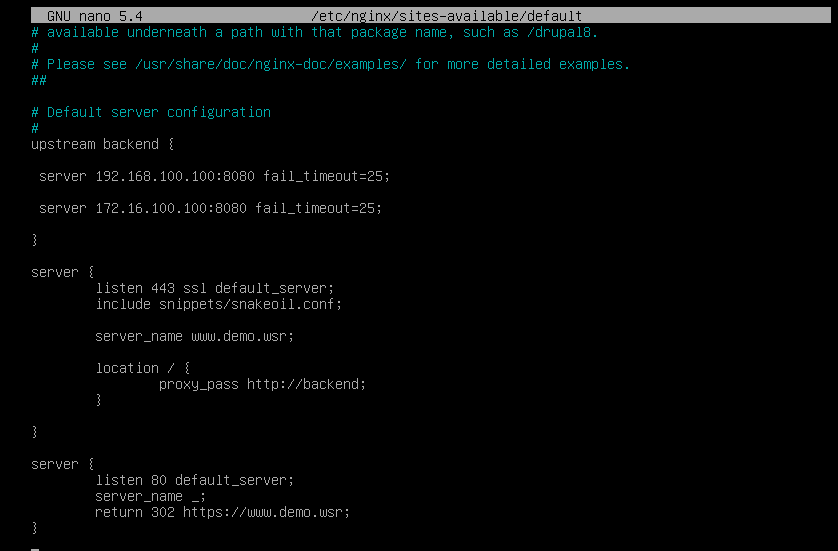
server {

listen 80 default\_server;

server\_name \_;

return 301 https://www.demo.wsr;

}

[](https://user-images.githubusercontent.com/79700810/150126455-0c42a808-bb14-4729-abd8-4f7b66db5554.png)

systemctl reload nginx

**WEB-R ssl**

apt install -y nginx

cd /opt/share

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

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

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

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

nano /etc/nginx/snippets/snakeoil.conf

[](https://user-images.githubusercontent.com/79700810/149767553-c42bd433-0ebb-43dd-9256-abcd782c3e47.png)

nano /etc/nginx/sites-available/default

upstream backend {

server 192.168.100.100:8080 fail\_timeout=25;

server 172.16.100.100:8080 fail\_timeout=25;

}

server {

listen 443 ssl default\_server;

include snippers/snakeoil.conf;

server\_name www.demo.wsr;

location / {

proxy\_pass http://backend ;

}

}

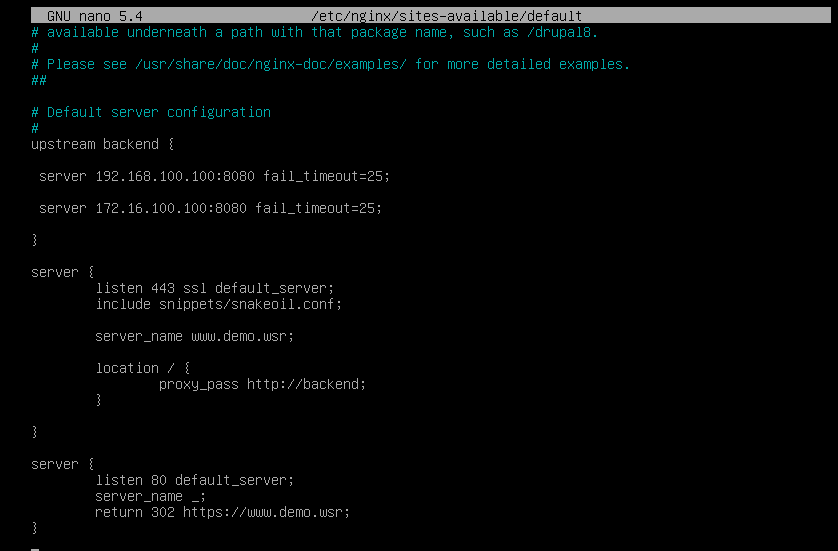
server {

listen 80 default\_server;

server\_name \_;

return 301 https://www.demo.wsr;

}

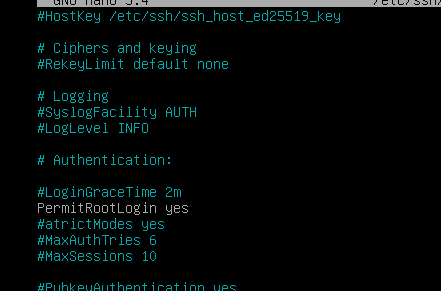
[](https://user-images.githubusercontent.com/79700810/150126411-0bc0538e-3192-421a-a2f7-05901c3d0372.png)

systemctl reload nginx

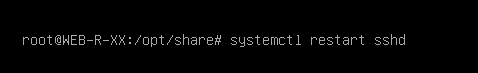
**WEB-R ssl**

ssh

nano /etc/ssh/sshd\_config

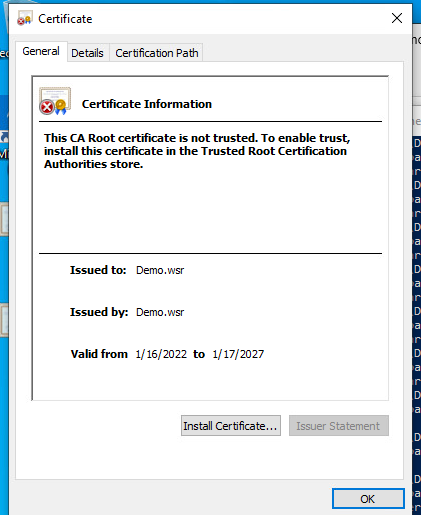
[](https://user-images.githubusercontent.com/79700810/149774137-4c65faa7-a467-4b2f-a2ce-c1f6616f0c54.png)

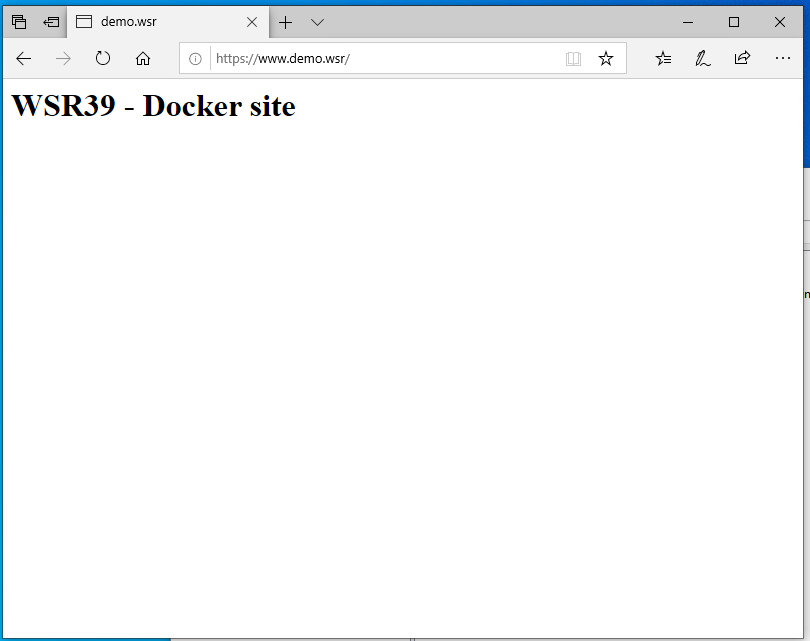
systemctl restart sshd

[](https://user-images.githubusercontent.com/79700810/149774186-c83b7b0a-5f67-41bb-9051-b26897840154.png)

**CLI ssl**

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

[](https://user-images.githubusercontent.com/79700810/149774248-784bebe3-8015-414f-88dc-e96f91dfd395.png)

[](https://user-images.githubusercontent.com/79700810/150135023-996d369c-493e-47c7-b826-6186cc0bf914.png)